

Documents for the Record
Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade
Legislative Solutions to Protect Children and Teens Online
December 2, 2025

Submitted by the Majority

1. Compilation of letters in support of H.R. 3149, App Store Accountability Act, submitted by Rep. James.
2. Letter from Concerned Women for America in support of H.R. 3149, App Store Accountability Act.
3. Letter from the Dignity Defense Institute in support of H.R. 3149, App Store Accountability Act.
4. Letter from ACT the App Association regarding the hearing.
5. Letter from the International Union of Police Associations in support of H.R. 3149, App Store Accountability Act.
6. Letter from Engine regarding the hearing.
7. Letter from undersigned Utah organizations in support of H.R. 3149, App Store Accountability Act.
8. Letter from the Center for Innovation and Free Enterprise in support of H.R. 3149, App Store Accountability Act.
9. Letter from the Suicide Awareness Voices of Education (SAVE) regarding the hearing.
10. Memorandum of poll data conducted by Digital Childhood Alliance via Fabrizio Ward.
11. Letter from Indiana University College Republicans in support of H.R. 3149, App Store Accountability Act.
12. Letter from Latinos for Tennessee in support of H.R. 3149, App Store Accountability Act.
13. Letter from the Main Street Privacy Coalition in support of H.R. 6291, Children and Teens Online Privacy Protection Act.
14. Letter from Apple regarding parental tools and the hearing.
15. Letter from OpenAI in support of H.R. 6289, Promoting a Safe Internet for Minors Act, the Assessing Safety Tools for Parents Act, and H.R. 5360, the AWARE Act.
16. Statement for the record from NetChoice regarding legislative solutions to protect kids online.
17. Letter from Cloaked regarding the hearing.
18. Letter from undersigned organizations regarding the Kids Online Safety Act.
19. Compiled information sourced from the Federal Trade Commission related to app stores.
20. Letter from undersigned child advocacy organizations in support of H.R. 3149, App Store Accountability Act.
21. Letter from the Alabama Policy Institute in support of H.R. 3149, App Store Accountability Act.
22. Letter from the Livingston County Office of the Sheriff in support of H.R. 3149, App Store Accountability Act.

Minority

1. Letter from AAJ in opposition to KOSA and COPPA.
2. Letter from Apple to Chairman Bilirakis and Ranking Member Schakowsky.
3. Letter from California Privacy Protection Agency to Chairman Guthrie, Ranking Member Pallone, Chairman Bilirakis, Ranking Member Schakowsky.
4. Letter from various parents to Speaker Johnson, Minority Leader Jeffries, Chairman Guthrie, Ranking Member Pallone.
5. Letter from various organizations to Chairman Guthrie and Ranking Member Pallone.
6. Letter from 408 organizations to Majority Leader Thune, Speaker Johnson, Minority Leader Schumer, Minority Leader Jeffries, Chairman Cruz, Chairman Guthrie, Ranking Member Cantwell, Ranking Member Pallone in support of KOSA.
7. Letter from Common Sense Media regarding COPPA 2.0.
8. Letter from ParentsSOS regarding KOSA.
9. Advisory from U.S. Surgeon General regarding Social Media and Youth Mental Health (2023).
10. Advisory from American Psychological Association regarding Social Media Use in Adolescence.
11. Report from Pew Research Center titled “Teens, Social Media, and Mental Health”.
12. Testimony from Cayce Savage to Senate Judiciary Committee, Subcommittee on Privacy, Technology and the Law.
13. Responses to Questions for the Record from Cayce Savage to Senate Judiciary Committee.
14. Testimony from Jason Sattizahn to Senate Judiciary Committee, Subcommittee on Privacy, Technology and the Law.
15. Responses to Questions for the Record from Jason Sattizahn to Senate Judiciary Committee.
16. Report from various organizations titled “Teen Accounts, Broken Promises: How Instagram is Failing to Protect Minors”.

The Honorable Brett Guthrie
2161 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Gus Bilirakis
2306 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Frank Pallone
2107 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Jan Schakowsky
2408 Rayburn House Office Building
Washington, D.C. 20515

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

As the House Energy & Commerce Committee reviews ways to improve children's online safety, I wanted to voice my support for the [App Store Accountability Act](#) (H.R. 3149 / S. 1586). This legislation, which is [widely supported by parents](#), deserves your prompt consideration as it moves through the House.

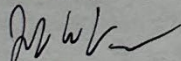
Today, Apple and Google's app stores have near-complete market share and virtually no responsibility for the platforms they advertise. Apple and Google routinely promote apps to young users that may be [inaccurately labeled or outright inappropriate](#), all while denying parents effective tools to understand or prevent those downloads. Following the money, their motive is clear: because app stores profit each time a child downloads a new platform, they have no meaningful incentive to prioritize safety over engagement.

That's why Congress must step in and pass the App Store Accountability Act. The bill requires app stores to present parents with accurate and transparent age ratings and mandates parental consent before minors can install apps or make in-app transactions. These provisions give parents the power app stores, up until now, have hoarded for themselves, ensuring moms and dads are the ones with final say over what their children engage with online.

What makes this proposal especially practical is that it does not force app stores to overhaul their systems. They already collect and securely store user age information, and their user-friendly systems allow parents to oversee kids' digital consumption without having to learn a whole new interface. With the groundwork already laid, app stores could implement these protections at the drop of a hat – but they won't act without a push from Congress.

At its core, this legislation brings digital oversight in line with the expectations we already place on parents in the real world. Just as families look out for kids' wellbeing at schools and in communities, parents deserve a meaningful say over the digital environments occupying increasing amounts of their kids' time. The App Store Accountability Act advances that goal, and I urge the Committee to give it the attention and support it deserves.

Sincerely,



Jeff Varner

The Honorable Brett Guthrie
2161 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Gus Bilirakis
2306 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Frank Pallone
2107 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Jan Schakowsky
2408 Rayburn House Office Building
Washington, D.C. 20515

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

As a father of five daughters, the thought of what my young girls might one day experience online – from dieting apps and beauty filters to manipulative chatbots and child predators – deeply troubles me. Like any dad, I do my best to protect them; but like all parents, I can't possibly oversee every second they spend on their devices.

I was encouraged to learn that the House Energy & Commerce Committee's Commerce, Manufacturing, and Trade Subcommittee will soon consider the [App Store Accountability Act](#) (H.R. 3149 / S. 1586). This bill delivers the common-sense digital safeguards [88% of parents support](#): a way for us to review, block, and approve all apps on our kids' devices before they're ever installed on one seamless interface.

With five girls to think about, managing a patchwork of inconsistent, opt-in parental controls that change from app to app is an impossible burden. The App Store Accountability Act ensures all platforms play by the same rules and gives parents a chance to review every app – whether it's a calculator, photo editor, or social media platform – within a single secure and familiar system.

Having tried (and failed) to stay on top of each trending app my girls ask about, I'm also supportive of the App Store Accountability Act's push to standardize age categories across the app store and provide accurate, transparent age-rating information. This way, whether it's Candy Crush or Roblox they're attempting to download, I can get a clear picture of the content and privacy risks associated.

Unlike other solutions that attempt to ban or restrict access to certain platforms, the App Store Accountability Act recognizes that parents know their kids best and places them in the driver's seat. All my daughters are different, and the apps that are appropriate for some are unthinkable for others – policies like the App Store Accountability Act acknowledge that different approaches work for different kids and leave it up to parents to determine the best level of exposure.

I also appreciate that the App Store Accountability Act is narrowly targeted and technically feasible. We've already seen this bill signed into law in several states, and we know that app stores already collect and securely store the age data needed to implement its requirements.

I humbly ask you and your colleagues to support the App Store Accountability Act during the upcoming hearing and work to pass this long-overdue bill into law this session.

Sincerely,

Scott Carr





December 1, 2025

Re: Hold App Stores Accountable to Keep Kids Safe

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

In my more than twenty years in elected office, I've witnessed two troubling trends: an increase in the time kids spend on digital devices and an uptick in online exploitation. As a parent, grandparent and citizen, I urge you and the rest of the House Energy & Commerce Committee to help make the digital world safer for kids by supporting the [App Store](#)

[Accountability Act](#) (H.R. 3149 / S. 1586) in the upcoming Subcommittee on Commerce, Manufacturing, and Trade hearing.

The current digital universe, dominated by Apple and Google, is designed to sideline parents and enable child predators, scam artists and bad actors to exploit impressionable kids. The system has no meaningful guardrails — developers can publish their applications with minimal oversight and kids can download any one of these platforms in just a few taps.

Not only does allowing kids to agree to binding terms and conditions violate contract law, but it also opens the door for kids to access features like sexualized AI chatbots, anonymous messages, nudifying filters and more that allow cybercrime to fester. Kids' parents are in the dark the entire time.

The App Store Accountability Act finally holds Apple and Google accountable for the harm they enable by demanding safety and transparency. The bill, which requires app stores to verify users' ages during account set-up and ask a parent's permission before a minor can download any platform, will prevent countless cybercrimes before they occur by giving parents better oversight into their kids' online experiences.

Today, with more and more crimes happening behind screens and out-of-sight, parents, lawmakers and law enforcement must work together to protect kids online. The App Store Accountability Act, supported by [88% of parents across the country](#), is a solution we should all get behind.

I thank you for your consideration and urge your support to pass this crucial child safety bill into law.

Sincerely,

A handwritten signature in black ink that reads "Beverly K. Burger". The signature is written in a cursive style with a large, stylized 'B' and 'B'.

Beverly K. Burger Alderman – Ward I

City of Franklin, Tennessee

bev@aldermanburger.com 615-498-4794

cc: House Energy & Commerce Committee

House Energy & Commerce Committee on Commerce, Manufacturing, & Trade

ManageHealthCareCost.com

Re: Pass the App Store Accountability Act to Protect Kids' Digital Health

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

As a health care advocate, I am encouraged to see that the House Energy & Commerce Committee Subcommittee on Commerce, Manufacturing, and Trade will consider a package of proposals aimed at creating safe and healthy digital spaces for kids. Ahead of this important hearing, I am particularly excited about and wish to call the Committee's attention to a desperately needed solution for parents: the [App Store Accountability Act](#) (H.R. 3149 / S. 1586).

The App Store Accountability Act is exactly the pro-family, privacy-preserving child safety solution parents are asking for. The bill's premise is simple: just like parents give consent for kids to see rated-R movies or attend school field trips, they ought to sign off on the platforms available on their kids' devices. The App Store Accountability Act extends this common-sense standard from the physical world to the digital sphere by requiring app stores to verify users' age and obtain a parent's permission before allowing a minor to download an app or make an in-app purchase.

Unlike other approaches that target specific platforms or restrict content, the App Store Accountability Act applies a consistent standard to all applications without picking favorites. Plus, the bill focuses on commercial conduct, not user speech, therefore respecting the constitutional principles American families cherish.

Most importantly, the bill puts the power to shape kids' online experiences back where it belongs: with parents. The only way to put a stop to the app store's misleading, exploitative practices is for force Big Tech's hand and demand accountability. Apple and Google have proven that they won't enact these protections voluntarily, and parents are counting on Congress to act.

I urge you to stand with the [88% of parents nationwide](#) who support the App Store Accountability Act and work to carry this long-overdue child safety bill into law.

Thank you for your consideration. Sincerely



Patsy Writesman

Owner, ManageHealthCareCosts.com

cc: House Energy & Commerce Committee

House Energy & Commerce Committee on Commerce, Manufacturing, & Trade

The Honorable Brett Guthrie
2161 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Gus Bilirakis
2306 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Frank Pallone
2107 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Jan Schakowsky
2408 Rayburn House Office Building
Washington, D.C. 20515

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

Ahead of the House Energy & Commerce Committee's upcoming child safety hearing, I wanted to voice my support for the [App Store Accountability Act](#) (H.R. 3149 / S. 1586).

Among the 19 bills to be considered, I believe this proposal offers the best solution. Unlike other heavy-handed attempts to restrict online speech or outright ban certain digital platforms, the App Store Accountability Act is constitutional and privacy preserving. The bill echoes a conviction many parents share: the power to decide which apps are available to kids and at what age they gain access must rest with parents, not politicians.

The App Store Accountability Act is an equal parts child safety and parents' right bill. Using data Apple and Google already collect and securely store, the bill would require app stores to verify users' age and ask parental permission for minors' app purchases and downloads. In practice, this grants parents the power to review, block, and approve each of the millions of platforms app stores advertise to their children, creating a needed barrier between kids and tech companies.

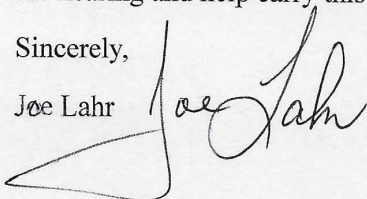
By targeting app stores' commercial conduct and applying equal, across-the-board standards to all platforms – no carveouts for popular apps like TikTok, Snapchat, and Instagram – the App Store Accountability Act respects the core constitutional principles Americans hold dear. Instead of allowing the government to determine which speech is appropriate for kids of certain ages, the App Store Accountability Act gives parents final say, leaving citizens' First Amendment freedoms intact.

Unsurprisingly, parents overwhelmingly support the App Store Accountability Act. According to a [national poll](#), 88% of parents, including overwhelming majorities of Republicans, Democrats, and Independents, support requiring app stores to verify age and ask parental permission for minors' app downloads.

I urge you and your colleagues to listen to parents and prioritize policies that protect kids while strengthening parents' rights. I hope you will support the App Store Accountability Act during the hearing and help carry this important bill to passage this session.

Sincerely,

Joe Lahr

A handwritten signature in black ink, appearing to read "Joe Lahr", is written over a large, stylized, handwritten letter "J" that serves as a decorative flourish or part of the signature.

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

Today, the online ecosystem is full of AI chatbots, anonymous messaging platforms, pornographic content, and violent video games that I never could have imagined growing up. As the digital world evolves, parents, now more than ever, need the tools to protect children online. As leaders on the House Energy & Commerce Committee, you all have the power to help make

online spaces more navigable for kids and parents by supporting the App Store Accountability Act (H.R. 3149 / S. 1586).

This bill does exactly what 88% of parents nationwide are asking for: create a one-stop shop for parents to review and approve all apps before they are downloaded on their children's devices. As any parent knows, raising kids is hard enough without having to navigate a complicated web of contradictory, unreliable parental controls that change between apps. By verifying users' age and obtaining parents' consent at the app store level, the bill gives parents full oversight of kids' digital consumption from one easy-to-use interface.

The App Store Accountability Act also ends the alarming practice of kids agreeing to binding contracts with developers. It's unthinkable that a child would ever open a bank account or sign a lease, but they enter equally binding contracts every day on the app store when they agree to developers' terms and conditions. According to contract law, these transactions should not take place without a parent's consent – the App Store Accountability Act ensures they don't.

Importantly, the App Store Accountability Act doesn't play favorites – it applies consistent rules so that all apps, from Roblox to the Bible app, receive the same treatment. Too many parents have learned the hard way that seemingly harmless platforms rated safe for teens are more dangerous than they look. The App Store Accountability Act uniquely addresses this risk and avoids carve outs for the multi-billion dollar tech giants like TikTok, Instagram, and Snapchat. Families like mine are counting on our representatives to make child safety a priority. The upcoming Subcommittee on Commerce, Manufacturing, and Trade meeting is a strong first step

– I urge you all to seize this opportunity to advance the App Store Accountability Act.

Sincerely,

Cristi Waltz

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

For too many parents, it seems like the worst-case scenario has come true for kids online. Devastating headlines of teens driven to suicide by AI chatbots and gaining premature exposure to violent, explicit content on platforms like Roblox make clear that Congress must step in to protect kids online.

Online, as in real life, we know that kids benefit from parental supervision. We wouldn't dream of letting our young child wander unattended through a busy city; but kids do just that online every day. Left to their own devices, kids are unequipped to navigate the unregulated and ever-changing digital world without a parent by their side.

That's why we urge you and your colleagues to support the App Store Accountability Act (H.R. 3149/S. 1586). The bill, supported by [88% of parents](#) across the country, gives parents the tools they need to supervise kids online and take action before potentially dangerous apps are ever installed.

Today, Apple and Google's app stores advertise millions of platforms to minors. Not only do parents struggle to keep up with the sheer volume of platforms available, but these app stores further complicate our jobs by misrepresenting each platform's appropriateness for kids. As the [Wall Street Journal](#) reported, hundreds of apps rated safe for children on the app store include inappropriate features like dieting tips, tools to circumvent banned sites, beauty filters, and anonymous chat functions.

The App Store Accountability Act addresses both concerns – it requires app stores to ask a parent's permission before a minor can download any app and makes available the accurate, transparent content rating information parents need to fully understand the risks associated.

The good news is, Apple and Google already have all the information they need to implement this simple-age gate, delivering added protection at no extra hassle for parents. Plus, by working within the app store's existing interface, parents don't have to learn a new system – they can simply, review, block, and/or approve all downloads in one place.

As parents, we're relieved to see that the House Energy & Commerce Committee will consider the App Store Accountability Act during an upcoming Subcommittee on Commerce, Manufacturing, and Trade hearing. As you debate the bills, we urge you to keep this pro-family, privacy-preserving solution in mind.

Sincerely,

Chris Shadle & Ben Becker

Catasaqua, PA

Dear Chairman,

Please support the App Store Accountability Act, supported by 88% of parents across the country, to put parents back in control.

Every parent I know worries about what their kids are exposed to online. We are told to set rules and monitor, but none of that matters when app stores quietly allow children to download anything they want and agree to terms they cannot possibly understand. Parents are locked out while our kids are left unprotected.

The App Store Accountability Act gives families a way forward. It requires companies to tell the truth about what's in their apps, verify ages so protections actually work, and make sure parents have the final say before kids gain access. That's not asking for too much – it's asking for the basic ability to parent.

Sincerely,

Mischalina Bishop

Dear Chairman,

I'm writing to urge you to support HR 3149, the App Store Accountability Act at the upcoming committee hearing.

I have always believed that raising children in a digital world meant learning new tools and setting new rules, but what I have discovered is that those tools are broken by design. Parents cannot compete with app stores that deliberately cut us out of the process, making it easier for kids to slip into contracts and content that should never be on their screens.

Almost 90% of parents support the App Store Accountability Act, which is constitutional and puts parents back in the driver's seat instead of Big Tech or the government.

The App Store Accountability Act restores the role of parents by requiring our approval, demanding truthful ratings, and ensuring companies stop pretending unsafe apps are harmless.

Congress has the power to empower parents with tools to help keep their kids safe online. **VOTE YES ON THE APP STORE ACCOUNTABILITY ACT!**

Sincerely,

Patricia Blake

Dear Chairman,

On behalf of parents in your district, please support the App Store Accountability Act.

Parents are expected to supervise their kids online, but the system is stacked against us. App stores present themselves as safe for kids while pushing apps with hidden risks, contracts no child should be signing, and content no parent would allow. We are left powerless while Big Tech profits off our children.

The App Store Accountability Act gives parents oversight before kids can download apps on their iPhone or iPad and ensures real protections are in place.

Families deserve better than the status quo. I urge you to support the App Store Accountability Act!

Sincerely,

Arthur Miller

Dear Chairman,

On behalf of parents in your district, please support the App Store Accountability Act.

Parents are expected to supervise their kids online, but the system is stacked against us. App stores present themselves as safe for kids while pushing apps with hidden risks, contracts no child should be signing, and content no parent would allow. We are left powerless while Big Tech profits off our children.

The App Store Accountability Act gives parents oversight before kids can download apps on their iPhone or iPad and ensures real protections are in place.

Families deserve better than the status quo. I urge you to support the App Store Accountability Act!

Sincerely,

Phil Zeitler

Dear Chairman,

I'm writing to urge you to support HR 3149, the App Store Accountability Act at the upcoming committee hearing.

I have always believed that raising children in a digital world meant learning new tools and setting new rules, but what I have discovered is that those tools are broken by design. Parents cannot compete with app stores that deliberately cut us out of the process, making it easier for kids to slip into contracts and content that should never be on their screens.

Almost 90% of parents support the App Store Accountability Act, which is constitutional and puts parents back in the driver's seat instead of Big Tech or the government.

The App Store Accountability Act restores the role of parents by requiring our approval, demanding truthful ratings, and ensuring companies stop pretending unsafe apps are harmless.

Congress has the power to empower parents with tools to help keep their kids safe online. VOTE YES ON THE APP STORE ACCOUNTABILITY ACT!

Sincerely,

troy vonk

Dear Chairman,

Please stand up for parental rights and co-sponsor the App Store Accountability Act. Parents are doing our part, but we need Congress to step in and give us the tools to keep our kids safe.

We all agree that parents should be guiding and protecting their children online. But the reality is, the system was designed to work around us, not with us.

App stores let kids download apps, enter into binding contracts, and expose personal data without any parental oversight. The ratings we see are misleading – making apps appear safer than they truly are.

Parents are not asking anyone to replace us. We are asking for the chance to do our job. And that requires real accountability.

The App Store Accountability Act is supported by 88% of parents with broad, bipartisan support.

This is not a partisan issue. It is about restoring parents' role in their kids' digital lives and making sure trillion-dollar corporations do not get to decide what is safe.

Please support the App Store Accountability Act during the upcoming Energy & Commerce Committee hearing.

Sincerely,

Holly Sahmel

Dear Chairman,

Please support the App Store Accountability Act, supported by 88% of parents across the country, to put parents back in control.

Every parent I know worries about what their kids are exposed to online. We are told to set rules and monitor, but none of that matters when app stores quietly allow children to download anything they want and agree to terms they cannot possibly understand. Parents are locked out while our kids are left unprotected.

The App Store Accountability Act gives families a way forward. It requires companies to tell the truth about what's in their apps, verify ages so protections actually work, and make sure parents have the final say before kids gain access. That's not asking for too much – it's asking for the basic ability to parent.

Sincerely,

Joseph Joyce

Dear Chairman,

I'm writing to urge you to support HR 3149, the App Store Accountability Act at the upcoming committee hearing.

I have always believed that raising children in a digital world meant learning new tools and setting new rules, but what I have discovered is that those tools are broken by design. Parents cannot compete with app stores that deliberately cut us out of the process, making it easier for kids to slip into contracts and content that should never be on their screens.

Almost 90% of parents support the App Store Accountability Act, which is constitutional and puts parents back in the driver's seat instead of Big Tech or the government.

The App Store Accountability Act restores the role of parents by requiring our approval, demanding truthful ratings, and ensuring companies stop pretending unsafe apps are harmless.

Congress has the power to empower parents with tools to help keep their kids safe online. **VOTE YES ON THE APP STORE ACCOUNTABILITY ACT!**

Sincerely,

James Van Zandt

Dear Chairman,

On behalf of parents in your district, please support the App Store Accountability Act.

Parents are expected to supervise their kids online, but the system is stacked against us. App stores present themselves as safe for kids while pushing apps with hidden risks, contracts no

child should be signing, and content no parent would allow. We are left powerless while Big Tech profits off our children.

The App Store Accountability Act gives parents oversight before kids can download apps on their iPhone or iPad and ensures real protections are in place.

Families deserve better than the status quo. I urge you to support the App Store Accountability Act!

Sincerely,

Stephen Garrison

Dear Chairman,

Please support the App Store Accountability Act during the upcoming hearing in the House Energy & Commerce Committee.

The App Store Accountability Act, which is supported by 88% of parents, will empower parents and finally hold big tech accountable. I believe parents should be responsible for guiding and protecting their kids online. But today's system makes that nearly impossible.

The App Store Accountability Act is constitutional and common sense.

App stores were built to keep parents out, leaving kids vulnerable to exploitative contracts and harmful content. And when parents try to exercise oversight, we're shown misleading app ratings that make it seem like apps are safe when, in fact, they are not.

The App Store Accountability Act changes that and has already been signed into law in three states.

Please co-sponsor and VOTE YES on the App Store Accountability Act so families across the country will have the tools they need to protect their children online.

Sincerely,

Steve Spurlock

Dear Chairman,

On behalf of parents in your district, please support the App Store Accountability Act.

Parents are expected to supervise their kids online, but the system is stacked against us. App stores present themselves as safe for kids while pushing apps with hidden risks, contracts no

child should be signing, and content no parent would allow. We are left powerless while Big Tech profits off our children.

The App Store Accountability Act gives parents oversight before kids can download apps on their iPhone or iPad and ensures real protections are in place.

Families deserve better than the status quo. I urge you to support the App Store Accountability Act!

Sincerely,

Robin Roberts

Dear Chairman,

I'm asking you to support the App Store Accountability Act – a commonsense bill that empowers parents and finally holds Big Tech accountable - during the upcoming committee hearing.

Parents want to take responsibility for guiding their kids' digital lives. But the truth is, the system was not built for us. App stores lock parents out, letting kids download apps, sign contracts, and share personal data without our knowledge. And when we do try to step in, we are given misleading app ratings that downplay the risks.

The App Store Accountability Act gives parents the tools we have been missing by ensuring:

- 1) Parental consent before kids can download or purchase apps.
- 2) Accurate, transparent ratings parents can trust.
- 3) Privacy-preserving age verification so protections actually work.

The App Store Accountability Act restores what parents have always wanted – the chance to actually parent.

Please vote YES and support this bill so it can be signed into law!

Sincerely,

Dottie Indihar

Dear Chairman,

On behalf of parents in your district, please support the App Store Accountability Act.

Parents are expected to supervise their kids online, but the system is stacked against us. App stores present themselves as safe for kids while pushing apps with hidden risks, contracts no

child should be signing, and content no parent would allow. We are left powerless while Big Tech profits off our children.

The App Store Accountability Act gives parents oversight before kids can download apps on their iPhone or iPad and ensures real protections are in place.

Families deserve better than the status quo. I urge you to support the App Store Accountability Act!

Sincerely,

Denise Fuentes

Dear Chairman,

Please support the App Store Accountability Act, supported by 88% of parents across the country, to put parents back in control.

Every parent I know worries about what their kids are exposed to online. We are told to set rules and monitor, but none of that matters when app stores quietly allow children to download anything they want and agree to terms they cannot possibly understand. Parents are locked out while our kids are left unprotected.

The App Store Accountability Act gives families a way forward. It requires companies to tell the truth about what's in their apps, verify ages so protections actually work, and make sure parents have the final say before kids gain access. That's not asking for too much – it's asking for the basic ability to parent.

Sincerely,

Matt Capozzoli

Dear Chairman,

Please support the App Store Accountability Act during the upcoming hearing in the House Energy & Commerce Committee.

The App Store Accountability Act, which is supported by 88% of parents, will empower parents and finally hold big tech accountable. I believe parents should be responsible for guiding and protecting their kids online. But today's system makes that nearly impossible.

The App Store Accountability Act is constitutional and common sense.

App stores were built to keep parents out, leaving kids vulnerable to exploitative contracts and harmful content. And when parents try to exercise oversight, we're shown misleading app ratings that make it seem like apps are safe when, in fact, they are not.

The App Store Accountability Act changes that and has already been signed into law in three states.

Please co-sponsor and VOTE YES on the App Store Accountability Act so families across the country will have the tools they need to protect their children online.

Sincerely,

George Kendrick

Dear Chairman,

I'm writing to urge you to support HR 3149, the App Store Accountability Act at the upcoming committee hearing.

I have always believed that raising children in a digital world meant learning new tools and setting new rules, but what I have discovered is that those tools are broken by design. Parents cannot compete with app stores that deliberately cut us out of the process, making it easier for kids to slip into contracts and content that should never be on their screens.

Almost 90% of parents support the App Store Accountability Act, which is constitutional and puts parents back in the driver's seat instead of Big Tech or the government.

The App Store Accountability Act restores the role of parents by requiring our approval, demanding truthful ratings, and ensuring companies stop pretending unsafe apps are harmless.

Congress has the power to empower parents with tools to help keep their kids safe online. **VOTE YES ON THE APP STORE ACCOUNTABILITY ACT!**

Sincerely,

Donna White

Dear Chairman,

Please support the App Store Accountability Act during the upcoming hearing in the House Energy & Commerce Committee.

The App Store Accountability Act, which is supported by 88% of parents, will empower parents and finally hold big tech accountable. I believe parents should be responsible for guiding and protecting their kids online. But today's system makes that nearly impossible.

The App Store Accountability Act is constitutional and common sense.

App stores were built to keep parents out, leaving kids vulnerable to exploitative contracts and harmful content. And when parents try to exercise oversight, we're shown misleading app ratings that make it seem like apps are safe when, in fact, they are not.

The App Store Accountability Act changes that and has already been signed into law in three states.

Please co-sponsor and VOTE YES on the App Store Accountability Act so families across the country will have the tools they need to protect their children online.

Sincerely,

Steve Herndon

Dear Chairman,

I'm writing to urge you to support HR 3149, the App Store Accountability Act at the upcoming committee hearing.

I have always believed that raising children in a digital world meant learning new tools and setting new rules, but what I have discovered is that those tools are broken by design. Parents cannot compete with app stores that deliberately cut us out of the process, making it easier for kids to slip into contracts and content that should never be on their screens.

Almost 90% of parents support the App Store Accountability Act, which is constitutional and puts parents back in the driver's seat instead of Big Tech or the government.

The App Store Accountability Act restores the role of parents by requiring our approval, demanding truthful ratings, and ensuring companies stop pretending unsafe apps are harmless.

Congress has the power to empower parents with tools to help keep their kids safe online. VOTE YES ON THE APP STORE ACCOUNTABILITY ACT!

Sincerely,

Blair Burton

Dear Chairman,

I'm asking you to support the App Store Accountability Act – a commonsense bill that empowers parents and finally holds Big Tech accountable - during the upcoming committee hearing.

Parents want to take responsibility for guiding their kids' digital lives. But the truth is, the system was not built for us. App stores lock parents out, letting kids download apps, sign contracts, and share personal data without our knowledge. And when we do try to step in, we are given misleading app ratings that downplay the risks.

The App Store Accountability Act gives parents the tools we have been missing by ensuring:

- 1) Parental consent before kids can download or purchase apps.
- 2) Accurate, transparent ratings parents can trust.
- 3) Privacy-preserving age verification so protections actually work.

The App Store Accountability Act restores what parents have always wanted – the chance to actually parent.

Please vote YES and support this bill so it can be signed into law!

Sincerely,

Darlene Nowery

Dear Chairman,

Please stand up for parental rights and co-sponsor the App Store Accountability Act. Parents are doing our part, but we need Congress to step in and give us the tools to keep our kids safe.

We all agree that parents should be guiding and protecting their children online. But the reality is, the system was designed to work around us, not with us.

App stores let kids download apps, enter into binding contracts, and expose personal data without any parental oversight. The ratings we see are misleading – making apps appear safer than they truly are.

Parents are not asking anyone to replace us. We are asking for the chance to do our job. And that requires real accountability.

The App Store Accountability Act is supported by 88% of parents with broad, bipartisan support.

This is not a partisan issue. It is about restoring parents' role in their kids' digital lives and making sure trillion-dollar corporations do not get to decide what is safe.

Please support the App Store Accountability Act during the upcoming Energy & Commerce Committee hearing.

Sincerely,

Luke Lynn

Dear Chairman,

Please support the App Store Accountability Act during the upcoming hearing in the House Energy & Commerce Committee.

The App Store Accountability Act, which is supported by 88% of parents, will empower parents and finally hold big tech accountable. I believe parents should be responsible for guiding and protecting their kids online. But today's system makes that nearly impossible.

The App Store Accountability Act is constitutional and common sense.

App stores were built to keep parents out, leaving kids vulnerable to exploitative contracts and harmful content. And when parents try to exercise oversight, we're shown misleading app ratings that make it seem like apps are safe when, in fact, they are not.

The App Store Accountability Act changes that and has already been signed into law in three states.

Please co-sponsor and VOTE YES on the App Store Accountability Act so families across the country will have the tools they need to protect their children online.

Sincerely,

Valerie Jateff

Dear Chairman,

Please stand up for parental rights and co-sponsor the App Store Accountability Act. Parents are doing our part, but we need Congress to step in and give us the tools to keep our kids safe.

We all agree that parents should be guiding and protecting their children online. But the reality is, the system was designed to work around us, not with us.

App stores let kids download apps, enter into binding contracts, and expose personal data without any parental oversight. The ratings we see are misleading – making apps appear safer than they truly are.

Parents are not asking anyone to replace us. We are asking for the chance to do our job. And that requires real accountability.

The App Store Accountability Act is supported by 88% of parents with broad, bipartisan support.

This is not a partisan issue. It is about restoring parents' role in their kids' digital lives and making sure trillion-dollar corporations do not get to decide what is safe.

Please support the App Store Accountability Act during the upcoming Energy & Commerce Committee hearing.

Sincerely,

Carol Meeks

Dear Chairman,

Please stand up for parental rights and co-sponsor the App Store Accountability Act. Parents are doing our part, but we need Congress to step in and give us the tools to keep our kids safe.

We all agree that parents should be guiding and protecting their children online. But the reality is, the system was designed to work around us, not with us.

App stores let kids download apps, enter into binding contracts, and expose personal data without any parental oversight. The ratings we see are misleading – making apps appear safer than they truly are.

Parents are not asking anyone to replace us. We are asking for the chance to do our job. And that requires real accountability.

The App Store Accountability Act is supported by 88% of parents with broad, bipartisan support.

This is not a partisan issue. It is about restoring parents' role in their kids' digital lives and making sure trillion-dollar corporations do not get to decide what is safe.

Please support the App Store Accountability Act during the upcoming Energy & Commerce Committee hearing.

Sincerely,

Danielle Coatney

Dear Chairman,

Please stand up for parental rights and co-sponsor the App Store Accountability Act. Parents are doing our part, but we need Congress to step in and give us the tools to keep our kids safe.

We all agree that parents should be guiding and protecting their children online. But the reality is, the system was designed to work around us, not with us.

App stores let kids download apps, enter into binding contracts, and expose personal data without any parental oversight. The ratings we see are misleading – making apps appear safer than they truly are.

Parents are not asking anyone to replace us. We are asking for the chance to do our job. And that requires real accountability.

The App Store Accountability Act is supported by 88% of parents with broad, bipartisan support.

This is not a partisan issue. It is about restoring parents' role in their kids' digital lives and making sure trillion-dollar corporations do not get to decide what is safe.

Please support the App Store Accountability Act during the upcoming Energy & Commerce Committee hearing.

Sincerely,

Mark Finney

Dear Chairman,

I'm asking you to support the App Store Accountability Act, a bill nearly 90 percent of parents across the country - including in your district, support.

Even the best parents who set boundaries, check devices, and have tough conversations need better tools because we're fighting against a system that was never meant to include parents. App stores make decisions for our children without our knowledge, and we're left powerless after the damage is done to our children.

The App Store Accountability Act would finally ensure PARENTS are informed, that app ratings reflect reality, and that app stores receive parental consent before a child can download apps on their devices.

Please give families the chance to truly protect our kids online and vote YES on the App Store Accountability Act

Sincerely,

Kenneth Parchinski

Dear Chairman,

Please stand up for parental rights and co-sponsor the App Store Accountability Act. Parents are doing our part, but we need Congress to step in and give us the tools to keep our kids safe.

We all agree that parents should be guiding and protecting their children online. But the reality is, the system was designed to work around us, not with us.

App stores let kids download apps, enter into binding contracts, and expose personal data without any parental oversight. The ratings we see are misleading – making apps appear safer than they truly are.

Parents are not asking anyone to replace us. We are asking for the chance to do our job. And that requires real accountability.

The App Store Accountability Act is supported by 88% of parents with broad, bipartisan support.

This is not a partisan issue. It is about restoring parents' role in their kids' digital lives and making sure trillion-dollar corporations do not get to decide what is safe.

Please support the App Store Accountability Act during the upcoming Energy & Commerce Committee hearing.

Sincerely,

Phillip Porter

Dear Chairman,

Please support the App Store Accountability Act, supported by 88% of parents across the country, to put parents back in control.

Every parent I know worries about what their kids are exposed to online. We are told to set rules and monitor, but none of that matters when app stores quietly allow children to download anything they want and agree to terms they cannot possibly understand. Parents are locked out while our kids are left unprotected.

The App Store Accountability Act gives families a way forward. It requires companies to tell the truth about what's in their apps, verify ages so protections actually work, and make sure parents have the final say before kids gain access. That's not asking for too much – it's asking for the basic ability to parent.

Sincerely,

Melanie Coats

Dear Chairman,

Please support the App Store Accountability Act during the upcoming hearing in the House Energy & Commerce Committee.

The App Store Accountability Act, which is supported by 88% of parents, will empower parents and finally hold big tech accountable. I believe parents should be responsible for guiding and protecting their kids online. But today's system makes that nearly impossible.

The App Store Accountability Act is constitutional and common sense.

App stores were built to keep parents out, leaving kids vulnerable to exploitative contracts and harmful content. And when parents try to exercise oversight, we're shown misleading app ratings that make it seem like apps are safe when, in fact, they are not.

The App Store Accountability Act changes that and has already been signed into law in three states.

Please co-sponsor and VOTE YES on the App Store Accountability Act so families across the country will have the tools they need to protect their children online.

Sincerely,

Leonides Pimienta

Dear Chairman,

Please support the App Store Accountability Act, supported by 88% of parents across the country, to put parents back in control.

Every parent I know worries about what their kids are exposed to online. We are told to set rules and monitor, but none of that matters when app stores quietly allow children to download anything they want and agree to terms they cannot possibly understand. Parents are locked out while our kids are left unprotected.

The App Store Accountability Act gives families a way forward. It requires companies to tell the truth about what's in their apps, verify ages so protections actually work, and make sure parents have the final say before kids gain access. That's not asking for too much – it's asking for the basic ability to parent.

Sincerely,

Jason Pappas

Dear Chairman,

I'm writing to urge you to support HR 3149, the App Store Accountability Act at the upcoming committee hearing.

I have always believed that raising children in a digital world meant learning new tools and setting new rules, but what I have discovered is that those tools are broken by design. Parents cannot compete with app stores that deliberately cut us out of the process, making it easier for kids to slip into contracts and content that should never be on their screens.

Almost 90% of parents support the App Store Accountability Act, which is constitutional and puts parents back in the driver's seat instead of Big Tech or the government.

The App Store Accountability Act restores the role of parents by requiring our approval, demanding truthful ratings, and ensuring companies stop pretending unsafe apps are harmless.

Congress has the power to empower parents with tools to help keep their kids safe online. VOTE YES ON THE APP STORE ACCOUNTABILITY ACT!

Sincerely,

Dawn James

Dear Chairman,

Please support the App Store Accountability Act during the upcoming hearing in the House Energy & Commerce Committee.

The App Store Accountability Act, which is supported by 88% of parents, will empower parents and finally hold big tech accountable. I believe parents should be responsible for guiding and protecting their kids online. But today's system makes that nearly impossible.

The App Store Accountability Act is constitutional and common sense.

App stores were built to keep parents out, leaving kids vulnerable to exploitative contracts and harmful content. And when parents try to exercise oversight, we're shown misleading app ratings that make it seem like apps are safe when, in fact, they are not.

The App Store Accountability Act changes that and has already been signed into law in three states.

Please co-sponsor and VOTE YES on the App Store Accountability Act so families across the country will have the tools they need to protect their children online.

Sincerely,

Jennifer Mitchell

Dear Chairman,

Please support the App Store Accountability Act during the upcoming hearing in the House Energy & Commerce Committee.

The App Store Accountability Act, which is supported by 88% of parents, will empower parents and finally hold big tech accountable. I believe parents should be responsible for guiding and protecting their kids online. But today's system makes that nearly impossible.

The App Store Accountability Act is constitutional and common sense.

App stores were built to keep parents out, leaving kids vulnerable to exploitative contracts and harmful content. And when parents try to exercise oversight, we're shown misleading app ratings that make it seem like apps are safe when, in fact, they are not.

The App Store Accountability Act changes that and has already been signed into law in three states.

Please co-sponsor and VOTE YES on the App Store Accountability Act so families across the country will have the tools they need to protect their children online.

Sincerely,

Jennifer Mitchell

Dear Chairman,

On behalf of parents in your district, please support the App Store Accountability Act.

Parents are expected to supervise their kids online, but the system is stacked against us. App stores present themselves as safe for kids while pushing apps with hidden risks, contracts no child should be signing, and content no parent would allow. We are left powerless while Big Tech profits off our children.

The App Store Accountability Act gives parents oversight before kids can download apps on their iPhone or iPad and ensures real protections are in place.

Families deserve better than the status quo. I urge you to support the App Store Accountability Act!

Sincerely,

Henry Rutledge

Dear Chairman,

Please support the App Store Accountability Act during the upcoming hearing in the House Energy & Commerce Committee.

The App Store Accountability Act, which is supported by 88% of parents, will empower parents and finally hold big tech accountable. I believe parents should be responsible for guiding and protecting their kids online. But today's system makes that nearly impossible.

The App Store Accountability Act is constitutional and common sense.

App stores were built to keep parents out, leaving kids vulnerable to exploitative contracts and harmful content. And when parents try to exercise oversight, we're shown misleading app ratings that make it seem like apps are safe when, in fact, they are not.

The App Store Accountability Act changes that and has already been signed into law in three states.

Please co-sponsor and VOTE YES on the App Store Accountability Act so families across the country will have the tools they need to protect their children online.

Sincerely,

Robert Ausburn

Dear Chairman,

Please stand up for parental rights and co-sponsor the App Store Accountability Act. Parents are doing our part, but we need Congress to step in and give us the tools to keep our kids safe.

We all agree that parents should be guiding and protecting their children online. But the reality is, the system was designed to work around us, not with us.

App stores let kids download apps, enter into binding contracts, and expose personal data without any parental oversight. The ratings we see are misleading – making apps appear safer than they truly are.

Parents are not asking anyone to replace us. We are asking for the chance to do our job. And that requires real accountability.

The App Store Accountability Act is supported by 88% of parents with broad, bipartisan support.

This is not a partisan issue. It is about restoring parents' role in their kids' digital lives and making sure trillion-dollar corporations do not get to decide what is safe.

Please support the App Store Accountability Act during the upcoming Energy & Commerce Committee hearing.

Sincerely,

Bryan Love

Dear Chairman,

Please support the App Store Accountability Act during the upcoming hearing in the House Energy & Commerce Committee.

The App Store Accountability Act, which is supported by 88% of parents, will empower parents and finally hold big tech accountable. I believe parents should be responsible for guiding and protecting their kids online. But today's system makes that nearly impossible.

The App Store Accountability Act is constitutional and common sense.

App stores were built to keep parents out, leaving kids vulnerable to exploitative contracts and harmful content. And when parents try to exercise oversight, we're shown misleading app ratings that make it seem like apps are safe when, in fact, they are not.

The App Store Accountability Act changes that and has already been signed into law in three states.

Please co-sponsor and VOTE YES on the App Store Accountability Act so families across the country will have the tools they need to protect their children online.

Sincerely,

Stewart Jamison

Dear Chairman,

I'm writing to urge you to support HR 3149, the App Store Accountability Act at the upcoming committee hearing.

I have always believed that raising children in a digital world meant learning new tools and setting new rules, but what I have discovered is that those tools are broken by design. Parents cannot compete with app stores that deliberately cut us out of the process, making it easier for kids to slip into contracts and content that should never be on their screens.

Almost 90% of parents support the App Store Accountability Act, which is constitutional and puts parents back in the driver's seat instead of Big Tech or the government.

The App Store Accountability Act restores the role of parents by requiring our approval, demanding truthful ratings, and ensuring companies stop pretending unsafe apps are harmless.

Congress has the power to empower parents with tools to help keep their kids safe online. VOTE YES ON THE APP STORE ACCOUNTABILITY ACT!

Sincerely,

Susan Boone

Dear Chairman,

Please stand up for parental rights and co-sponsor the App Store Accountability Act. Parents are doing our part, but we need Congress to step in and give us the tools to keep our kids safe.

We all agree that parents should be guiding and protecting their children online. But the reality is, the system was designed to work around us, not with us.

App stores let kids download apps, enter into binding contracts, and expose personal data without any parental oversight. The ratings we see are misleading – making apps appear safer than they truly are.

Parents are not asking anyone to replace us. We are asking for the chance to do our job. And that requires real accountability.

The App Store Accountability Act is supported by 88% of parents with broad, bipartisan support.

This is not a partisan issue. It is about restoring parents' role in their kids' digital lives and making sure trillion-dollar corporations do not get to decide what is safe.

Please support the App Store Accountability Act during the upcoming Energy & Commerce Committee hearing.

Sincerely,

Michelle Jenkins

Dear Chairman,

Please support the App Store Accountability Act during the upcoming hearing in the House Energy & Commerce Committee.

The App Store Accountability Act, which is supported by 88% of parents, will empower parents and finally hold big tech accountable. I believe parents should be responsible for guiding and protecting their kids online. But today's system makes that nearly impossible.

The App Store Accountability Act is constitutional and common sense.

App stores were built to keep parents out, leaving kids vulnerable to exploitative contracts and harmful content. And when parents try to exercise oversight, we're shown misleading app ratings that make it seem like apps are safe when, in fact, they are not.

The App Store Accountability Act changes that and has already been signed into law in three states.

Please co-sponsor and VOTE YES on the App Store Accountability Act so families across the country will have the tools they need to protect their children online.

Sincerely,

Charles Cecil

Dear Chairman,

I'm asking you to support the App Store Accountability Act – a commonsense bill that empowers parents and finally holds Big Tech accountable - during the upcoming committee hearing.

Parents want to take responsibility for guiding their kids' digital lives. But the truth is, the system was not built for us. App stores lock parents out, letting kids download apps, sign contracts, and share personal data without our knowledge. And when we do try to step in, we are given misleading app ratings that downplay the risks.

The App Store Accountability Act gives parents the tools we have been missing by ensuring:

- 1) Parental consent before kids can download or purchase apps.
- 2) Accurate, transparent ratings parents can trust.
- 3) Privacy-preserving age verification so protections actually work.

The App Store Accountability Act restores what parents have always wanted – the chance to actually parent.

Please vote YES and support this bill so it can be signed into law!

Sincerely,

Matt Sawyer

Dear Chairman,

I'm writing to urge you to support HR 3149, the App Store Accountability Act at the upcoming committee hearing.

I have always believed that raising children in a digital world meant learning new tools and setting new rules, but what I have discovered is that those tools are broken by design. Parents cannot compete with app stores that deliberately cut us out of the process, making it easier for kids to slip into contracts and content that should never be on their screens.

Almost 90% of parents support the App Store Accountability Act, which is constitutional and puts parents back in the driver's seat instead of Big Tech or the government.

The App Store Accountability Act restores the role of parents by requiring our approval, demanding truthful ratings, and ensuring companies stop pretending unsafe apps are harmless.

Congress has the power to empower parents with tools to help keep their kids safe online. VOTE YES ON THE APP STORE ACCOUNTABILITY ACT!

Sincerely,

David Parkerson

Dear Chairman,

I'm asking you to support the App Store Accountability Act, a bill nearly 90 percent of parents across the country - including in your district, support.

Even the best parents who set boundaries, check devices, and have tough conversations need better tools because we're fighting against a system that was never meant to include parents. App stores make decisions for our children without our knowledge, and we're left powerless after the damage is done to our children.

The App Store Accountability Act would finally ensure PARENTS are informed, that app ratings reflect reality, and that app stores receive parental consent before a child can download apps on their devices.

Please give families the chance to truly protect our kids online and vote YES on the App Store Accountability Act

Sincerely,

Clara Chapman

Dear Chairman,

On behalf of parents in your district, please support the App Store Accountability Act.

Parents are expected to supervise their kids online, but the system is stacked against us. App stores present themselves as safe for kids while pushing apps with hidden risks, contracts no child should be signing, and content no parent would allow. We are left powerless while Big Tech profits off our children.

The App Store Accountability Act gives parents oversight before kids can download apps on their iPhone or iPad and ensures real protections are in place.

Families deserve better than the status quo. I urge you to support the App Store Accountability Act!

Sincerely,

Toby Sweets

Dear Chairman,

I'm asking you to support the App Store Accountability Act – a commonsense bill that empowers parents and finally holds Big Tech accountable - during the upcoming committee hearing.

Parents want to take responsibility for guiding their kids' digital lives. But the truth is, the system was not built for us. App stores lock parents out, letting kids download apps, sign contracts, and share personal data without our knowledge. And when we do try to step in, we are given misleading app ratings that downplay the risks.

The App Store Accountability Act gives parents the tools we have been missing by ensuring:

- 1) Parental consent before kids can download or purchase apps.
- 2) Accurate, transparent ratings parents can trust.
- 3) Privacy-preserving age verification so protections actually work.

The App Store Accountability Act restores what parents have always wanted – the chance to actually parent.

Please vote YES and support this bill so it can be signed into law!

Sincerely,

Todd Thayer

Dear Chairman,

I'm writing to urge you to support HR 3149, the App Store Accountability Act at the upcoming committee hearing.

I have always believed that raising children in a digital world meant learning new tools and setting new rules, but what I have discovered is that those tools are broken by design. Parents cannot compete with app stores that deliberately cut us out of the process, making it easier for kids to slip into contracts and content that should never be on their screens.

Almost 90% of parents support the App Store Accountability Act, which is constitutional and puts parents back in the driver's seat instead of Big Tech or the government.

The App Store Accountability Act restores the role of parents by requiring our approval, demanding truthful ratings, and ensuring companies stop pretending unsafe apps are harmless.

Congress has the power to empower parents with tools to help keep their kids safe online. VOTE YES ON THE APP STORE ACCOUNTABILITY ACT!

Sincerely,

Karyl Kaufmann

Dear Chairman,

On behalf of parents in your district, please support the App Store Accountability Act.

Parents are expected to supervise their kids online, but the system is stacked against us. App stores present themselves as safe for kids while pushing apps with hidden risks, contracts no child should be signing, and content no parent would allow. We are left powerless while Big Tech profits off our children.

The App Store Accountability Act gives parents oversight before kids can download apps on their iPhone or iPad and ensures real protections are in place.

Families deserve better than the status quo. I urge you to support the App Store Accountability Act!

Sincerely,

Betty Robey

Dear Chairman,

Please support the App Store Accountability Act during the upcoming hearing in the House Energy & Commerce Committee.

The App Store Accountability Act, which is supported by 88% of parents, will empower parents and finally hold big tech accountable. I believe parents should be responsible for guiding and protecting their kids online. But today's system makes that nearly impossible.

The App Store Accountability Act is constitutional and common sense.

App stores were built to keep parents out, leaving kids vulnerable to exploitative contracts and harmful content. And when parents try to exercise oversight, we're shown misleading app ratings that make it seem like apps are safe when, in fact, they are not.

The App Store Accountability Act changes that and has already been signed into law in three states.

Please co-sponsor and VOTE YES on the App Store Accountability Act so families across the country will have the tools they need to protect their children online.

Sincerely,

James Thieneman

Dear Chairman,

Please support the App Store Accountability Act during the upcoming hearing in the House Energy & Commerce Committee.

The App Store Accountability Act, which is supported by 88% of parents, will empower parents and finally hold big tech accountable. I believe parents should be responsible for guiding and protecting their kids online. But today's system makes that nearly impossible.

The App Store Accountability Act is constitutional and common sense.

App stores were built to keep parents out, leaving kids vulnerable to exploitative contracts and harmful content. And when parents try to exercise oversight, we're shown misleading app ratings that make it seem like apps are safe when, in fact, they are not.

The App Store Accountability Act changes that and has already been signed into law in three states.

Please co-sponsor and VOTE YES on the App Store Accountability Act so families across the country will have the tools they need to protect their children online.

Sincerely,

Paul Baskis

Dear Chairman,

On behalf of parents in your district, please support the App Store Accountability Act.

Parents are expected to supervise their kids online, but the system is stacked against us. App stores present themselves as safe for kids while pushing apps with hidden risks, contracts no child should be signing, and content no parent would allow. We are left powerless while Big Tech profits off our children.

The App Store Accountability Act gives parents oversight before kids can download apps on their iPhone or iPad and ensures real protections are in place.

Families deserve better than the status quo. I urge you to support the App Store Accountability Act!

Sincerely,

Toby Sweets

Dear Chairman,

Please support the App Store Accountability Act, supported by 88% of parents across the country, to put parents back in control.

Every parent I know worries about what their kids are exposed to online. We are told to set rules and monitor, but none of that matters when app stores quietly allow children to download anything they want and agree to terms they cannot possibly understand. Parents are locked out while our kids are left unprotected.

The App Store Accountability Act gives families a way forward. It requires companies to tell the truth about what's in their apps, verify ages so protections actually work, and make sure parents have the final say before kids gain access. That's not asking for too much – it's asking for the basic ability to parent.

Sincerely,

Sharon Foley

Dear Chairman,

I'm asking you to support the App Store Accountability Act, a bill nearly 90 percent of parents across the country - including in your district, support.

Even the best parents who set boundaries, check devices, and have tough conversations need better tools because we're fighting against a system that was never meant to include parents. App stores make decisions for our children without our knowledge, and we're left powerless after the damage is done to our children.

The App Store Accountability Act would finally ensure PARENTS are informed, that app ratings reflect reality, and that app stores receive parental consent before a child can download apps on their devices.

Please give families the chance to truly protect our kids online and vote YES on the App Store Accountability Act

Sincerely,

Janice Williams

Dear Chairman,

Please support the App Store Accountability Act during the upcoming hearing in the House Energy & Commerce Committee.

The App Store Accountability Act, which is supported by 88% of parents, will empower parents and finally hold big tech accountable. I believe parents should be responsible for guiding and protecting their kids online. But today's system makes that nearly impossible.

The App Store Accountability Act is constitutional and common sense.

App stores were built to keep parents out, leaving kids vulnerable to exploitative contracts and harmful content. And when parents try to exercise oversight, we're shown misleading app ratings that make it seem like apps are safe when, in fact, they are not.

The App Store Accountability Act changes that and has already been signed into law in three states.

Please co-sponsor and VOTE YES on the App Store Accountability Act so families across the country will have the tools they need to protect their children online.

Sincerely,

Dawn Lawrence

Dear Chairman,

Please support the App Store Accountability Act during the upcoming hearing in the House Energy & Commerce Committee.

The App Store Accountability Act, which is supported by 88% of parents, will empower parents and finally hold big tech accountable. I believe parents should be responsible for guiding and protecting their kids online. But today's system makes that nearly impossible.

The App Store Accountability Act is constitutional and common sense.

App stores were built to keep parents out, leaving kids vulnerable to exploitative contracts and harmful content. And when parents try to exercise oversight, we're shown misleading app ratings that make it seem like apps are safe when, in fact, they are not.

The App Store Accountability Act changes that and has already been signed into law in three states.

Please co-sponsor and VOTE YES on the App Store Accountability Act so families across the country will have the tools they need to protect their children online.

Sincerely,

Paula Hinman

Dear Chairman,

I'm asking you to support the App Store Accountability Act, a bill nearly 90 percent of parents across the country - including in your district, support.

Even the best parents who set boundaries, check devices, and have tough conversations need better tools because we're fighting against a system that was never meant to include parents. App stores make decisions for our children without our knowledge, and we're left powerless after the damage is done to our children.

The App Store Accountability Act would finally ensure PARENTS are informed, that app ratings reflect reality, and that app stores receive parental consent before a child can download apps on their devices.

Please give families the chance to truly protect our kids online and vote YES on the App Store Accountability Act

Sincerely,

Janice Williams

Dear Chairman,

Please stand up for parental rights and co-sponsor the App Store Accountability Act. Parents are doing our part, but we need Congress to step in and give us the tools to keep our kids safe.

We all agree that parents should be guiding and protecting their children online. But the reality is, the system was designed to work around us, not with us.

App stores let kids download apps, enter into binding contracts, and expose personal data without any parental oversight. The ratings we see are misleading – making apps appear safer than they truly are.

Parents are not asking anyone to replace us. We are asking for the chance to do our job. And that requires real accountability.

The App Store Accountability Act is supported by 88% of parents with broad, bipartisan support.

This is not a partisan issue. It is about restoring parents' role in their kids' digital lives and making sure trillion-dollar corporations do not get to decide what is safe.

Please support the App Store Accountability Act during the upcoming Energy & Commerce Committee hearing.

Sincerely,

Tatiana pryor

Dear Chairman,

I'm asking you to support the App Store Accountability Act – a commonsense bill that empowers parents and finally holds Big Tech accountable - during the upcoming committee hearing.

Parents want to take responsibility for guiding their kids' digital lives. But the truth is, the system was not built for us. App stores lock parents out, letting kids download apps, sign contracts, and share personal data without our knowledge. And when we do try to step in, we are given misleading app ratings that downplay the risks.

The App Store Accountability Act gives parents the tools we have been missing by ensuring:

- 1) Parental consent before kids can download or purchase apps.
- 2) Accurate, transparent ratings parents can trust.
- 3) Privacy-preserving age verification so protections actually work.

The App Store Accountability Act restores what parents have always wanted – the chance to actually parent.

Please vote YES and support this bill so it can be signed into law!

Sincerely,

Brittany Stallwood

Dear Chairman,

Please support the App Store Accountability Act during the upcoming hearing in the House Energy & Commerce Committee.

The App Store Accountability Act, which is supported by 88% of parents, will empower parents and finally hold big tech accountable. I believe parents should be responsible for guiding and protecting their kids online. But today's system makes that nearly impossible.

The App Store Accountability Act is constitutional and common sense.

App stores were built to keep parents out, leaving kids vulnerable to exploitative contracts and harmful content. And when parents try to exercise oversight, we're shown misleading app ratings that make it seem like apps are safe when, in fact, they are not.

The App Store Accountability Act changes that and has already been signed into law in three states.

Please co-sponsor and VOTE YES on the App Store Accountability Act so families across the country will have the tools they need to protect their children online.

Sincerely,

Bobby Deacon

Dear Chairman,

Please support the App Store Accountability Act during the upcoming hearing in the House Energy & Commerce Committee.

The App Store Accountability Act, which is supported by 88% of parents, will empower parents and finally hold big tech accountable. I believe parents should be responsible for guiding and protecting their kids online. But today's system makes that nearly impossible.

The App Store Accountability Act is constitutional and common sense.

App stores were built to keep parents out, leaving kids vulnerable to exploitative contracts and harmful content. And when parents try to exercise oversight, we're shown misleading app ratings that make it seem like apps are safe when, in fact, they are not.

The App Store Accountability Act changes that and has already been signed into law in three states.

Please co-sponsor and VOTE YES on the App Store Accountability Act so families across the country will have the tools they need to protect their children online.

Sincerely,

Kristy Wasinger

Dear Chairman,

I'm asking you to support the App Store Accountability Act, a bill nearly 90 percent of parents across the country - including in your district, support.

Even the best parents who set boundaries, check devices, and have tough conversations need better tools because we're fighting against a system that was never meant to include parents. App stores make decisions for our children without our knowledge, and we're left powerless after the damage is done to our children.

The App Store Accountability Act would finally ensure PARENTS are informed, that app ratings reflect reality, and that app stores receive parental consent before a child can download apps on their devices.

Please give families the chance to truly protect our kids online and vote YES on the App Store Accountability Act

Sincerely,

Janice Richard

Dear Chairman,

I'm writing to urge you to support HR 3149, the App Store Accountability Act at the upcoming committee hearing.

I have always believed that raising children in a digital world meant learning new tools and setting new rules, but what I have discovered is that those tools are broken by design. Parents cannot compete with app stores that deliberately cut us out of the process, making it easier for kids to slip into contracts and content that should never be on their screens.

Almost 90% of parents support the App Store Accountability Act, which is constitutional and puts parents back in the driver's seat instead of Big Tech or the government.

The App Store Accountability Act restores the role of parents by requiring our approval, demanding truthful ratings, and ensuring companies stop pretending unsafe apps are harmless.

Congress has the power to empower parents with tools to help keep their kids safe online. VOTE YES ON THE APP STORE ACCOUNTABILITY ACT!

Sincerely,

Sherry Gaston

Dear Chairman,

On behalf of parents in your district, please support the App Store Accountability Act.

Parents are expected to supervise their kids online, but the system is stacked against us. App stores present themselves as safe for kids while pushing apps with hidden risks, contracts no child should be signing, and content no parent would allow. We are left powerless while Big Tech profits off our children.

The App Store Accountability Act gives parents oversight before kids can download apps on their iPhone or iPad and ensures real protections are in place.

Families deserve better than the status quo. I urge you to support the App Store Accountability Act!

Sincerely,

Christopher Theisen

Dear Chairman,

Please support the App Store Accountability Act during the upcoming hearing in the House Energy & Commerce Committee.

The App Store Accountability Act, which is supported by 88% of parents, will empower parents and finally hold big tech accountable. I believe parents should be responsible for guiding and protecting their kids online. But today's system makes that nearly impossible.

The App Store Accountability Act is constitutional and common sense.

App stores were built to keep parents out, leaving kids vulnerable to exploitative contracts and harmful content. And when parents try to exercise oversight, we're shown misleading app ratings that make it seem like apps are safe when, in fact, they are not.

The App Store Accountability Act changes that and has already been signed into law in three states.

Please co-sponsor and VOTE YES on the App Store Accountability Act so families across the country will have the tools they need to protect their children online.

Sincerely,

Pam Jordan

Dear Chairman,

Please support the App Store Accountability Act during the upcoming hearing in the House Energy & Commerce Committee.

The App Store Accountability Act, which is supported by 88% of parents, will empower parents and finally hold big tech accountable. I believe parents should be responsible for guiding and protecting their kids online. But today's system makes that nearly impossible.

The App Store Accountability Act is constitutional and common sense.

App stores were built to keep parents out, leaving kids vulnerable to exploitative contracts and harmful content. And when parents try to exercise oversight, we're shown misleading app ratings that make it seem like apps are safe when, in fact, they are not.

The App Store Accountability Act changes that and has already been signed into law in three states.

Please co-sponsor and VOTE YES on the App Store Accountability Act so families across the country will have the tools they need to protect their children online.

Sincerely,

Anthony Goff

Dear Chairman,

Please support the App Store Accountability Act during the upcoming hearing in the House Energy & Commerce Committee.

The App Store Accountability Act, which is supported by 88% of parents, will empower parents and finally hold big tech accountable. I believe parents should be responsible for guiding and protecting their kids online. But today's system makes that nearly impossible.

The App Store Accountability Act is constitutional and common sense.

App stores were built to keep parents out, leaving kids vulnerable to exploitative contracts and harmful content. And when parents try to exercise oversight, we're shown misleading app ratings that make it seem like apps are safe when, in fact, they are not.

The App Store Accountability Act changes that and has already been signed into law in three states.

Please co-sponsor and VOTE YES on the App Store Accountability Act so families across the country will have the tools they need to protect their children online.

Sincerely,

Jessica Alicna

Dear Chairman,

On behalf of parents in your district, please support the App Store Accountability Act.

Parents are expected to supervise their kids online, but the system is stacked against us. App stores present themselves as safe for kids while pushing apps with hidden risks, contracts no child should be signing, and content no parent would allow. We are left powerless while Big Tech profits off our children.

The App Store Accountability Act gives parents oversight before kids can download apps on their iPhone or iPad and ensures real protections are in place.

Families deserve better than the status quo. I urge you to support the App Store Accountability Act!

Sincerely,

Liza Crall

Dear Chairman,

I'm asking you to support the App Store Accountability Act, a bill nearly 90 percent of parents across the country - including in your district, support.

Even the best parents who set boundaries, check devices, and have tough conversations need better tools because we're fighting against a system that was never meant to include parents. App stores make decisions for our children without our knowledge, and we're left powerless after the damage is done to our children.

The App Store Accountability Act would finally ensure PARENTS are informed, that app ratings reflect reality, and that app stores receive parental consent before a child can download apps on their devices.

Please give families the chance to truly protect our kids online and vote YES on the App Store Accountability Act

Sincerely,

Maegan Bennett

Dear Chairman,

Please support the App Store Accountability Act, supported by 88% of parents across the country, to put parents back in control.

Every parent I know worries about what their kids are exposed to online. We are told to set rules and monitor, but none of that matters when app stores quietly allow children to download anything they want and agree to terms they cannot possibly understand. Parents are locked out while our kids are left unprotected.

The App Store Accountability Act gives families a way forward. It requires companies to tell the truth about what's in their apps, verify ages so protections actually work, and make sure parents have the final say before kids gain access. That's not asking for too much – it's asking for the basic ability to parent.

Sincerely,

Donald Carman

Dear Chairman,

I'm writing to urge you to support HR 3149, the App Store Accountability Act at the upcoming committee hearing.

I have always believed that raising children in a digital world meant learning new tools and setting new rules, but what I have discovered is that those tools are broken by design. Parents cannot compete with app stores that deliberately cut us out of the process, making it easier for kids to slip into contracts and content that should never be on their screens.

Almost 90% of parents support the App Store Accountability Act, which is constitutional and puts parents back in the driver's seat instead of Big Tech or the government.

The App Store Accountability Act restores the role of parents by requiring our approval, demanding truthful ratings, and ensuring companies stop pretending unsafe apps are harmless.

Congress has the power to empower parents with tools to help keep their kids safe online. **VOTE YES ON THE APP STORE ACCOUNTABILITY ACT!**

Sincerely,

Katie Dendy

Dear Chairman,

I'm asking you to support the App Store Accountability Act – a commonsense bill that empowers parents and finally holds Big Tech accountable - during the upcoming committee hearing.

Parents want to take responsibility for guiding their kids' digital lives. But the truth is, the system was not built for us. App stores lock parents out, letting kids download apps, sign contracts, and share personal data without our knowledge. And when we do try to step in, we are given misleading app ratings that downplay the risks.

The App Store Accountability Act gives parents the tools we have been missing by ensuring:

- 1) Parental consent before kids can download or purchase apps.
- 2) Accurate, transparent ratings parents can trust.
- 3) Privacy-preserving age verification so protections actually work.

The App Store Accountability Act restores what parents have always wanted – the chance to actually parent.

Please vote YES and support this bill so it can be signed into law!

Sincerely,

Virgil Willoughby

Dear Chairman,

Please support the App Store Accountability Act during the upcoming hearing in the House Energy & Commerce Committee.

The App Store Accountability Act, which is supported by 88% of parents, will empower parents and finally hold big tech accountable. I believe parents should be responsible for guiding and protecting their kids online. But today's system makes that nearly impossible.

The App Store Accountability Act is constitutional and common sense.

App stores were built to keep parents out, leaving kids vulnerable to exploitative contracts and harmful content. And when parents try to exercise oversight, we're shown misleading app ratings that make it seem like apps are safe when, in fact, they are not.

The App Store Accountability Act changes that and has already been signed into law in three states.

Please co-sponsor and VOTE YES on the App Store Accountability Act so families across the country will have the tools they need to protect their children online.

Sincerely,

Darrell Watson

Dear Chairman,

I'm asking you to support the App Store Accountability Act, a bill nearly 90 percent of parents across the country - including in your district, support.

Even the best parents who set boundaries, check devices, and have tough conversations need better tools because we're fighting against a system that was never meant to include parents. App stores make decisions for our children without our knowledge, and we're left powerless after the damage is done to our children.

The App Store Accountability Act would finally ensure PARENTS are informed, that app ratings reflect reality, and that app stores receive parental consent before a child can download apps on their devices.

Please give families the chance to truly protect our kids online and vote YES on the App Store Accountability Act

Sincerely,

Maegan Bennett

Dear Chairman,

I'm asking you to support the App Store Accountability Act, a bill nearly 90 percent of parents across the country - including in your district, support.

Even the best parents who set boundaries, check devices, and have tough conversations need better tools because we're fighting against a system that was never meant to include parents. App stores make decisions for our children without our knowledge, and we're left powerless after the damage is done to our children.

The App Store Accountability Act would finally ensure PARENTS are informed, that app ratings reflect reality, and that app stores receive parental consent before a child can download apps on their devices.

Please give families the chance to truly protect our kids online and vote YES on the App Store Accountability Act

Sincerely,

Billee Bridges

Dear Chairman,

Please support the App Store Accountability Act during the upcoming hearing in the House Energy & Commerce Committee.

The App Store Accountability Act, which is supported by 88% of parents, will empower parents and finally hold big tech accountable. I believe parents should be responsible for guiding and protecting their kids online. But today's system makes that nearly impossible.

The App Store Accountability Act is constitutional and common sense.

App stores were built to keep parents out, leaving kids vulnerable to exploitative contracts and harmful content. And when parents try to exercise oversight, we're shown misleading app ratings that make it seem like apps are safe when, in fact, they are not.

The App Store Accountability Act changes that and has already been signed into law in three states.

Please co-sponsor and VOTE YES on the App Store Accountability Act so families across the country will have the tools they need to protect their children online.

Sincerely,

Karen Foree

Dear Chairman,

On behalf of parents in your district, please support the App Store Accountability Act.

Parents are expected to supervise their kids online, but the system is stacked against us. App stores present themselves as safe for kids while pushing apps with hidden risks, contracts no child should be signing, and content no parent would allow. We are left powerless while Big Tech profits off our children.

The App Store Accountability Act gives parents oversight before kids can download apps on their iPhone or iPad and ensures real protections are in place.

Families deserve better than the status quo. I urge you to support the App Store Accountability Act!

Sincerely,

Jennifer Kerouac

Dear Chairman,

Please stand up for parental rights and co-sponsor the App Store Accountability Act. Parents are doing our part, but we need Congress to step in and give us the tools to keep our kids safe.

We all agree that parents should be guiding and protecting their children online. But the reality is, the system was designed to work around us, not with us.

App stores let kids download apps, enter into binding contracts, and expose personal data without any parental oversight. The ratings we see are misleading – making apps appear safer than they truly are.

Parents are not asking anyone to replace us. We are asking for the chance to do our job. And that requires real accountability.

The App Store Accountability Act is supported by 88% of parents with broad, bipartisan support.

This is not a partisan issue. It is about restoring parents' role in their kids' digital lives and making sure trillion-dollar corporations do not get to decide what is safe.

Please support the App Store Accountability Act during the upcoming Energy & Commerce Committee hearing.

Sincerely,

Dawn Fehl

Dear Chairman,

I'm asking you to support the App Store Accountability Act, a bill nearly 90 percent of parents across the country - including in your district, support.

Even the best parents who set boundaries, check devices, and have tough conversations need better tools because we're fighting against a system that was never meant to include parents. App stores make decisions for our children without our knowledge, and we're left powerless after the damage is done to our children.

The App Store Accountability Act would finally ensure PARENTS are informed, that app ratings reflect reality, and that app stores receive parental consent before a child can download apps on their devices.

Please give families the chance to truly protect our kids online and vote YES on the App Store Accountability Act

Sincerely,

Marilyn Tarrance

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

As Black Americans United for Tennessee, we are proud to stand boldly for faith, family, and freedom. Our organization implores you to follow suit by championing the App Store Accountability Act (H.R. 3149 / S. 1586) - an important parents' rights bill that will empower Black children and families and all Americans - within the House Energy & Commerce Committee.

Parents are the first line of defense when it comes to protecting children in the real world; the online world should be no exception.

Parents know best what online experiences are appropriate for their children. Still, the current app store's download settings for kids systematically deny parents the chance to review and manage their kids' digital consumption.

By verifying users' age at the app store level and requiring a parent's informed consent before a minor can download an app, the App Store Accountability Act allows parents real-time oversight into the apps that occupy increasing amounts of their kids' time. It also equips them with accurate and transparent age-rating information needed to understand the privacy and content risks associated with each app and make a confident choice about whether it's appropriate for their teens before it's ever installed.

Parents are speaking up, with a national poll finding 88% of moms and dads support requiring app stores to verify users' age and ask for permission to download. But we aren't asking for a lot — the App Store Accountability Act's one-step age check is technically feasible, privacy-preserving, and consistent with constitutional principles.

Our organization is committed to instilling the strong morals our children need to grow into respectable young adults. But the values we teach must be reinforced wherever our children are — in the home, in the classroom, and on their devices. By supporting the App Store Accountability Act, you can help parents reclaim the power to raise their kids and curb Big Tech's harmful influence.

Thank you for your consideration.

Sincerely,

Walter Blanks Jr

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

I am pleased to see the House Energy & Commerce Committee will soon meet to consider a package of children's online safety measures. As you and your colleagues deliberate, I wanted to register my support for the App Store Accountability Act (H.R. 3149 / S. 1586) – a common-sense online safety policy that protects kids and empowers parents.

We, rightfully, trust parents to protect kids' physical well-being; the App Store Accountability Act finally puts parents in charge of kids' digital health as well. By requiring parental permission for kids to download applications from the app store or make in-app purchases, the bill gives moms and dads deciding power over which online experiences are appropriate for their child.

Under current rules, parents are all-but powerless on the app store. On today's app store, Apple and Google have a direct line to our kids, advertising inappropriate and misleadingly rated apps at the top of their feeds with no meaningful way for parents to review the risks before they're installed. Big Tech prefers it this way – with Apple and Google skimming a cut off the top of every app store purchase, the more our kids buy, the better for their bottom line.

The App Store Accountability Act ends this exploitative practice, demanding that app stores not only ask parental permission for minors' app downloads but also equip parents with the accurate age-rating information they need to make an informed choice about whether a given platform is appropriate.

Together, these measures will make the digital world safer for kids overnight. Thankfully, they don't require any major system upgrades or data collection changes to implement; not only do app stores already collect and safely manage user age information, but they also operate familiar and easy-to-use interfaces ideal for parents to keep tabs on kids' digital activity.

I count myself among the 82% of voters – including 88% of parents – who support the App Store Accountability Act. I urge the Committee to prioritize this important policy and support the bill as it moves through the House.

Thank you for your consideration.

Sincerely,

Veronica Comfort

CONCERNED
WOMEN *for* AMERICA
LEGISLATIVE ACTION COMMITTEE

November 3, 2025

Dear member of the Energy and Commerce Committee,

On behalf of Concerned Women for America Legislative Action Committee (CWALAC), the largest public policy women's organization in the country, I write in strong support of the App Store Accountability Act sponsored by Rep. John James (R-Michigan) and Sen. Mike Lee (R-Utah).

This bill would empower parents to protect their children from inappropriate, age-restricted materials by implementing parental controls in app stores. This measure has received overwhelming support nationwide with polls suggesting 82% approval from voters.

Children are protected from purchasing inappropriate products in their local corner stores, but such protections do not exist in one of the most dangerous marketplaces of them all: the internet. Because of this, app stores regularly expose young children to explicit and violent content without their parents' knowledge. Additionally, age ratings on app stores are often inaccurate, and minors frequently sign away private information through confusing user agreements.

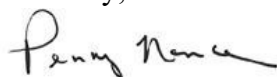
The App Store Accountability Act would protect children by empowering parents as the drivers of these decisions. The bill ensures parents a private right of action against app stores that fail to:

- Require for parental consent on age-registered materials
- Provide clear age ratings and descriptions of the apps available for download
- Allow parents to filter what their children can access on these markets

The lack of Congressional action in the rapidly developing marketplace has allowed app stores to exploit children to new, dangerous heights, and it has placed parents in a helpless position. That is a reality our members at Concerned Women for America know all too well.

We are proud to represent parents across the nation who stand firmly for Biblical values and earnestly seek to provide their children with the protective measures they deserve. But in a marketplace as diverse and accessible as the app store, it is nearly impossible for parents to stay on top of every trap awaiting their child online. That is why age rating displays and parental notification are a critical step forward, and one we are proud to endorse on behalf of our members.

Sincerely,



Penny Young Nance
CEO and President
Concerned Women for America LAC



615-500-4135



nicole@dignitydefense.org



December 1, 2025

To: **CC: HOUSE ENERGY & COMMERCE COMMITTEE**
CC: HOUSE ENERGY & COMMERCE COMMITTEE ON COMMERCE,
MANUFACTURING, & TRADE

The Honorable Brett Guthrie
2161 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Gus Bilirakis
2306 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Frank Pallone
2107 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Jan Schakowsky
2408 Rayburn House Office Building
Washington, D.C. 20515

RE: HELP PARENTS PROTECT KIDS BY PASSING THE APP STORE ACCOUNTABILITY ACT

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

Driven by our belief that family is sacred and parents know best, the Dignity Defense Institute is proud to support the App Store Accountability Act (H.R. 3149 / S. 1586). The bill, which is scheduled to be heard by the House Energy & Commerce Committee, codifies our conviction that parents, not Washington bureaucrats or Big Tech, should have final say over what kids experience online.

For too long, app stores have neglected to implement meaningful safety measures that protect minors from unsafe experiences. Apple and Google's app stores - the gateways to millions of platforms - have brokered exploitative contracts between kids and app developers that surrender minors' personal data and expose them to harmful content. By prioritizing monetizing kids' taps and engagement over their health and safety, app stores have left parents in the dark at every step of the process, forced to rely on lax parental controls and misleading age ratings that purposefully understate risks.

The App Store Accountability Act reforms the system without overcomplicating parents' jobs or compromising families' private information. Using information app stores already collect and



 615-500-4135

 nicole@dignitydefense.org

 December 1, 2025

securely store, the bill would require app stores to verify users' age and, for users who are minors, require a parent to sign-off on all app downloads and purchases.

The bill, which is broadly supported by a bipartisan majority of parents, comes at a critical time in the digital age. As parents, we are tasked with monitoring every app, website, and online interaction our children engage with. This is an overwhelming and simply impossible responsibility. We need a robust, app-store level accountability measure to ensure that every digital platform prioritizes the safety and privacy of our children.

We appreciate your consideration and hope you will support this bill when it comes before the House Energy & Commerce Committee in the coming days.

Sincerely,

 NICOLE
SMITH

President | Dignity Defense Institute

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://coppa.ca.gov/pdf/enf advisory202401.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,

A handwritten signature in black ink that reads "Morgan Reed". The signature is fluid and cursive, with the first name "Morgan" and the last name "Reed" clearly distinguishable.

Morgan Reed
President

ACT | The App Association



INTERNATIONAL UNION OF POLICE ASSOCIATIONS

THE ONLY UNION FOR LAW ENFORCEMENT OFFICERS

SAM A. CABRAL
International President

MICHAEL V. CRIVELLO
International Secretary-Treasurer

11-26-2025

The Honorable Gus Bilirakis
Chairman
Subcommittee on Commerce,
Manufacturing, and Trade
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Jan Schakowsky
Ranking Member
Subcommittee on Commerce,
Manufacturing, and Trade
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Brett Guthrie
Chairman
Energy & Commerce Committee
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Frank Pallone
Ranking Member
Energy & Commerce Committee
U.S. House of Representatives
Washington, D.C. 20515

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

On behalf of the International Union of Police Associations (IUPA), I write to express our strong support for the App Store Accountability Act and to emphasize its vital role in protecting America's children. I urge you to support the App Store Accountability Act during the upcoming subcommittee hearing and bring it to the House floor without delay.

Every day, law enforcement officers across the country work to keep young people safe – not just by responding to crime, but by preventing harm before it reaches them. The number one way we protect children is by helping them avoid dangerous situations, risky interactions, and predatory influences in the first place.

Today, mobile applications and the devices children carry with them have become one of the primary avenues through which children are exposed to threats. Online predators, drug traffickers, and individuals seeking to exploit young users rely on the anonymity and lack of oversight within app marketplaces to reach children more easily than ever before, and often without their parents having any idea. When app stores fail to maintain clear accountability standards, dangerous or deceptive applications can flourish, leaving families and law enforcement without meaningful resources and safeguards.

The App Store Accountability Act directly addresses these challenges by requiring greater transparency, stronger vetting of which applications are appropriate for children, restoring parental consent, and improved cooperation with lawful investigations. These measures will give

law enforcement clearer tools to intervene early – before a child is contacted by a predator, pulled into illicit activity, or exposed to harmful content. In short, this legislation strengthens the preventive work that officers view as the cornerstone of child protection and reinstates parents as the first line of defense.

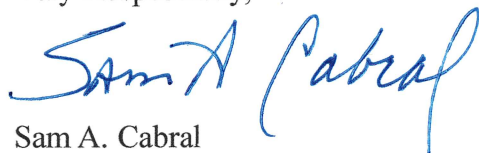
Support for this legislation is strong throughout the law enforcement community. In addition to the International Union of Police Associations, the following organizations stand united in urging action:

- Lakewood Police Union (Colorado)
- Milwaukee Police Association (Wisconsin)
- New York State Union of Police Associations (New York)
- Oklahoma State Bureau of Investigators Assertion (Oklahoma)
- Salt Lake Valley Law Enforcement Association (Utah)
- Toledo Police Patrolman's Association (Ohio)
- Virginia Beach PBA (Virginia)
- Washington Council of Police and Sheriffs (Washington)

We respectfully urge you to move this legislation forward without delay. Every day that passes without stronger safeguards in place increases the risks to children who depend on us to protect them – both offline and online. The App Store Accountability Act represents a meaningful, urgently needed step toward creating a safer digital environment for America's youth.

Thank you for your leadership and for your ongoing commitment to the safety and well-being of our communities. We stand ready to support your efforts as this critical legislation advances.

Very Respectfully,



Sam A. Cabral
International President
International Union of Police Associations



December 1, 2025

The Honorable Gus Bilirakis, Chairman
Subcommittee on Commerce,
Manufacturing, and Trade
Committee on Energy & Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Janice Schakowsky, Ranking Member
Subcommittee on Commerce,
Manufacturing, and Trade
Committee on Energy & Commerce
2322A Rayburn House Office Building
Washington, D.C. 20515

RE: December 2nd Hearing on “Legislative Solutions to Protect Children and Teens Online”

Dear Chairman Bilirakis, Ranking Member Schakowsky, and Honorable Members of the Subcommittee on Commerce, Manufacturing, and Trade:

Startups are creating new and innovative products that better the lives of users of all ages, improving the way individuals learn, work, and play. As a nonprofit that works to advance a policy environment where startups can succeed, we appreciate your attention to issues important to them, including the experiences of their customers. Startups take seriously their commitments to their users to create beneficial products and services while protecting their privacy and working to ensure a safe, relevant, and healthy user experience, including by upholding their obligations under current law and employing industry best practices.

Ultimately, problematic user content underlies many of the online safety issues that the subcommittee seeks to address with the pieces of legislation to be considered at the December 2nd hearing. Even if the age of a user could be determined and communicated with perfect accuracy (which is exceedingly difficult and comes with trade-offs), if an online service facilitates user speech or interaction between users, it cannot ensure—in real time, across all media, languages, cultures, and contexts—that users won’t encounter harmful content created and shared by other users. As Engine has explained to this committee, startups especially grapple with pressures of content moderation.¹ They do not have the resources to hire tens of thousands of content moderators or invest hundreds of millions of dollars in content moderation tools like their large competitors; they are least equipped to handle ruinous legal costs arising from user content; and they do not have the market share or long-standing relationships with their users to risk alienating their user base by either under- or over-moderating user content. Any legislation to address online safety issues must grapple with that reality and the inherent tradeoffs to innovation, expression, and user privacy and security.

¹ *Legislative Proposal To Sunset Section 230 of The Communications Decency Act: Hearing before the U.S. House Energy & Commerce Subcomm. on Comm’n & Tech.* 118th Congress (2024) (Testimony of Kate Tummarello), https://d1dth6e84htgma.cloudfront.net/05_22_24_Testimony_Tummarello_26a19b6b16.pdf.

Members of the subcommittee should be clear-eyed about what Congress can do to address these issues without running afoul of the Constitution or undermining the competitiveness of startups.

The wide range of legislation being considered at this week's hearing takes a variety of approaches to online safety, bringing along with them differing obligations and key definitions (for example, what qualifies as a "covered platform," the meaning of "know," and who qualifies as a "minor"). These incongruities in themselves threaten to increase costs for startups and undermine their competitiveness, leaving only the platforms policymakers are most concerned about in the marketplace.

We appreciate the recognition reflected in H.R. 6291, the Children and Teens' Online Privacy Protection Act, that larger platforms have both greater impact on online safety and greater resources to comply with more extensive regulatory requirements designed to improve it. In particular, the bill separates "High-Impact" platforms and subjects only those platforms to a higher, more uncertain, more costly knowledge standard, while maintaining the clear and certain "actual knowledge" standard for startups. As in last Congress, where the committee carried this approach across multiple bills,² this approach should be carried across all of the legislation where practicable—especially the Kids Online Safety Act, the Reducing Exploitative Social Media Exposure for Teens (RESET) Act, H.R. 2657, Sammy's Law, and H.R. 6253, Algorithmic Choice and Transparency Act. Unifying thresholds across legislation will help better balance Congress' desire to improve online safety and preserve competitiveness of U.S. startups.

Recognizing that companies of different sizes and resources will have differing abilities to determine users' age—under the risk of legal liability if they get it wrong—is crucial to an online safety framework that works for startups, but lawmakers should also work to tailor obligations under these proposals for small companies. A few provisions found in bills being considered are particularly unworkable for startups. For example, in the Kids Online Safety Act, covered platforms—of all sizes, including startups—would be required to conduct annual independent third-party audits. These audit requirements will be prohibitively expensive, and it is further unclear what independent third-party organizations would be prepared to conduct such audits. Using SOC 2 as an illustrative point of comparison (an audit for cybersecurity and privacy controls performed by many software startups), audits from reputable firms can cost between \$50,000-\$120,000³—or 1-2 months of an early-stage startup's resources.⁴ Asking startups to perform these audits annually is certain to discourage entry into this space, undermine competitiveness, and ensure that only large platforms remain.

² Amendment in the Nature of a Substitute to H.R. 7890, 118th Cong. at 12 (2024), <https://docs.house.gov/meetings/IF/IF00/20240918/117432/BILLS-118-HR7890-A000370-Amdt-7-U6.pdf>.

³ *Privacy Patchwork Problem*, 10 Engine (April 2023), <https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/6414a45f5001941e519492ff/1679074400513/Privacy+Patchwork+Problem+Report.pdf>

⁴ See *The State of the Startup Ecosystem*, 17 Engine (Apr. 2021), <https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/60819983b7f8be1a2a99972d/1619106194054/The+State+of+the+Startup+Ecosystem.pdf>.

Likewise, the premise of H.R. 6253, the Algorithmic Choice and Transparency Act, turns on requiring platforms to offer alternatives in how they display the content available on their services. This might sound reasonable on its face (indeed, some services differentiate themselves in the market this way), but requiring it as a matter of law in effect means that many startups would have to build another, duplicate version of their service. Startups put all of their limited resources into developing their original service, and it is unworkable to ask them to build an entirely new version.

Many questions of online safety depend first on determining the age of a given user. We appreciate the subcommittee's recognition that age verification requirements can be costly for startups⁵ (and carry other negative consequences for privacy, cybersecurity, and expression) by not explicitly requiring it, and generally avoiding liability standards that would require it in practice. In the handful of proposals where age verification is explicitly required for general purpose applications, it is to be performed by ostensibly larger entities—app stores and distributors—but even these approaches give rise to concerns that the subcommittee should be mindful to reconcile. Clarity about where and to what entities liability for (in)accuracy of age signals attaches is tantamount. Startups, i.e., developers, should not be liable for—nor need to further investigate—age signals shared by distributors. They should merely be called on to follow the signals they receive. And lawmakers must be clear-eyed about the fact that requiring developers to build their products around signals from distributors risks cementing the central role that distributors have in the mobile ecosystem—a role that facilitates many startups' go-to-market strategy but that critics, including some lawmakers, have said raises competition concerns.

We appreciate the subcommittee's work to bolster consumer protections online, especially for young users, and we strongly support thoughtful approaches that provide clarity for startups and strong protections for their users of all ages. We encourage the subcommittee to pursue legislation that avoids the unintended consequences to startups and their competitiveness described above, and we are eager to be a resource in continuing conversations.

Sincerely,

Engine Advocacy

700 Pennsylvania Ave SE
Washington, D.C. 20003
policy@engine.is

⁵ See *More than just a number: How determining user age impacts startups*, Engine (Aug. 2024), <https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/66ad1ff867b7114cc6f16b00/1722621944736/More+Than+Just+A+Number+-+Updated+August+2024.pdf> (documenting risks and costs of age verification, which could reach hundreds of thousands depending on a startups user count).

Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

December 1, 2025

Esteemed Committee Chair Guthrie and Committee Members,

As Utah organizations united in protecting parental rights, we believe the wellbeing of children is best safeguarded when parents, not tech companies—guide their online experiences. Today, minors are routinely bound to digital contracts that expose them to data collection, financial agreements, and targeted design they cannot legally consent to. The App Store Accountability Act (ASAA) fixes this by requiring age verification and parental consent *before app stores contract with minors*, just as minors cannot sign binding contracts offline.

This bill does not regulate speech or ideas. It regulates commercial conduct. In *Apple v. Pepper*, the Supreme Court confirmed that app stores function as retailers. Like any retailer, they can be required to verify age, prevent deceptive contracting, and obtain parental authorization. Protecting children from commercial exploitation safeguards contract rights; it does not censor speech.

Utah demonstrated that this model is both constitutional and bipartisan. SB142 passed with 96% support in the Senate and 95% in the House, proving that app store accountability protects families, not politics. Other federal proposals, like the Kids Online Safety Act (KOSA), the Algorithm Accountability Act, and the Google-backed Parents Over Platforms Act, address content and design transparency do not stop retailers from treating children as contract-worthy adults. Only the ASAA reaches the moment a corporation transacts with a child.

Families are not asking the government to parent for them. We are asking Congress to stop corporations from undermining parents. We are parents and community members raising children in a digital wilderness, and we know that when families have authority, children thrive. The ASAA restores responsibility where it belongs: with families who love, guide, and protect their children.

Respectfully,

On behalf of the undersigned organizations,

Association of Ministers in Utah- Pastor Rolondo Fernadez, President
Digital Childhood Institute- Melissa McKay, President
Empowered Parents Utah – Korrin Dickson, Board Chair
G-Rated School – Allie Terry and Liz Jenkins, Founders
Growing Unified Development – Marcus Carr, President
Hope Connecting Purpose Murray Latson, President
Hope of Utah – Ron Williams, President
Path Forward Utah – Jamie Renda, President
Latino Hope- Pastor Guillermo Rodeiguez, President
Moms for America, Utah– Cari Bartholomew, President
United Women’s Forum Salt Lake – Dawn Bates, President
Utah Citizens for the Constitution – Jen Brown, President
Utah Eagle Forum – Gayle Ruzicka, President
Utah Legislative Watch – MaryAnn Christensen, President
Utah Parents United – Corinne Johnson, President



CIFE
Center for Innovation and Free Enterprise

December 1, 2025

The Honorable Brett Guthrie
2161 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Frank Pallone
2107 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Gus Bilirakis
2306 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Jan Schakowsky
2408 Rayburn House Office Building
Washington, D.C. 20515

Re: App Store Accountability Act Protects Kids & Empowers Parents

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

The freedom to raise and protect their children is a fundamental right that every parent deserves. To uphold this right and protect the parent-child relationship, our organization urges you to support the [App Store Accountability Act](#) (H.R.3149 / S. 1586) during the subcommittee hearing on *Legislative Solutions to Protect Children and Teens Online* on December 2, 2025.

The App Store Accountability Act finally gives parents the tools to take charge of kids' online lives - importantly accomplishing this without over-involving the government, compromising families' privacy, or overstepping core constitutional liberties.

Building on the age-gating and data management capabilities Apple and Google already possess, the App Store Accountability Act requires app stores to verify users' age during account set-up and obtain permission from a linked parent account before a minor can download an app or make an in-app purchase. Not only is this solution simple, but it is also technically feasible - app stores already collect and securely store user age data, eliminating the need for parents to repeatedly upload sensitive personal identifying information to third-parties.

More broadly, the App Store Accountability Act reflects our core belief that parents, not tech companies or government agencies, should determine the content minors engage with online. In a digital world where child predators, scam artists, graphic violence and suggestive chatbots are overtaking platforms and hiding in plain sight, it's more important than ever that parents hold final decision-making power over what experiences and platforms are appropriate for their children to access.

Ultimately, we believe the App Store Accountability Act creates essential guardrails while preserving parents' ability to make rules that align with their household values. By ensuring age verification and parental consent at the app store level, this legislation places parents in control, where they belong.

Parents should be equipped with effective tools to oversee kids' digital experiences. Thank you for your attention to this important issue.

Sincerely,

Center for Innovation and Free Enterprise

PO Box 104
1220 L Street NW
Washington, DC 20044



The Honorable Gus M. Bilirakis

Chairman

Subcommittee on Commerce, Manufacturing, and Trade

Committee on Energy and Commerce

U.S. House of Representatives

Washington, DC 20515

The Honorable Jan Schakowsky

Ranking Member

Subcommittee on Commerce, Manufacturing, and Trade

Committee on Energy and Commerce

U.S. House of Representatives

Washington, DC 20515

The Honorable Brett Guthrie

Chairman

Committee on Energy and Commerce

U.S. House of Representatives

Washington, DC 20515

The Honorable Frank Pallone, Jr.

Ranking Member

Committee on Energy and Commerce

U.S. House of Representatives

Washington, DC 20515

Members of the Subcommittee on Commerce, Manufacturing, and Trade

Committee on Energy and Commerce

U.S. House of Representatives

Washington, DC 20515

Dear Chairman Bilirakis, Ranking Member Schakowsky, Chairman Guthrie, Ranking Member Pallone, and Members of the Subcommittee:

Thank you for the opportunity to submit this letter. I want to organize my letter around three points that reflect what our organization has seen and what I believe Congress must confront directly.

First, social media and artificial intelligence are killing our children physically, mentally, emotionally, and spiritually.

As CEO of Suicide Awareness Voices of Education (SAVE), one of the nation's oldest national suicide prevention organizations, I see every day how young people are being harmed by technologies that were built without any regard for their safety.

We cannot afford polite language that softens the truth for the benefit of the companies creating these harms. If we are serious about saving children today and in the future, we must speak in terms that match the severity of the crisis.

These technologies are killing children physically through self-harm and suicide; mentally through anxiety, depression, and psychological deterioration; emotionally by eroding their resilience, identity, and sense of self-worth; and spiritually by draining hope, purpose, and meaning from their lives.

This is not a theoretical concern or an emerging danger. It is happening right now, in real time, to families in every part of the country. Children are being exposed to content, algorithms, pressures, and interactions that overwhelm their developing minds. These platforms and systems play an undeniable role in pushing vulnerable youth toward self-harm, despair, and suicide. That is the reality we hear from parents and loved ones week after week. It is the reality that too often gets buried under statistics and policy arguments. But it is the reality this Committee must begin with.

What compounds the crisis is that these systems are designed to target vulnerabilities: insecurity, loneliness, identity confusion, social anxiety, trauma, and impulsivity. Children do not have the brain development, emotional maturity, or life experience to navigate these environments safely. Yet they are placed inside systems designed to extract their attention, shape their worldview, and influence their behavior in ways that even adults struggle to manage.

This is not simply a matter of harmful content. It is the cumulative effect of design, algorithms, virality, dopamine driven engagement loops, and AI-driven recommendation systems that know more about a child's vulnerabilities than their own parents do. When we talk about harms to children, we cannot continue to view social media and AI as neutral platforms. They are active participants in shaping the emotional, cognitive, and psychological landscape of American youth.

Second, the National Strategy for Suicide Prevention must be reopened and rewritten.

I have publicly called for the Strategy to be reopened, which I detail in my essay, "The US Needs a New Suicide Prevention Plan That Tackles Social Media and AI," published in Tech Policy Press: <https://www.techpolicy.press/the-us-needs-a-new-suicide-prevention-plan-that-tackles-social-media-and-ai/>

As a signatory to the most current National Strategy for Suicide Prevention, I want to be clear. I am not calling for the Strategy to be discarded. Much of its foundation remains valuable. But it must be rewritten for the world our children now live in. It does not meaningfully address social media, algorithmic amplification, or the rapid evolution of AI.

A national strategy that does not confront these technologies is outdated. And this is not a failure of any administration. It is the inevitable result of a framework designed to last ten years trying to keep pace with technologies that change every week.

From the time the current Strategy was released a little over a year ago, the landscape of AI related harm has accelerated dramatically. Nowhere is AI even mentioned. And the differences between the Strategy written ten years ago and the one we have today with respect to social media lack the urgency and accountability required to meet this crisis.

We cannot comprehensively address suicide prevention without speaking transparently to the online forces accelerating risk for an entire generation. Suicide is increasingly a leading cause of death among young people. Emergency department visits for self-harm have surged. Parents report children falling into online communities that normalize or directly instruct self-harm. These realities demand a strategy built for the digital world as it truly exists.

There is currently no federal entity, framework, or strategy capable of keeping pace with the youth suicide risks created by social media and AI. This is a national level policy vacuum, and every month that passes widens it. Right now, parents are fighting a technological battle they cannot win alone, and a modernized National Strategy would finally give families the federal partner they do not currently have.

The speed of technological change is no longer an abstract concern. It is an operational problem for Congress and for those of us working to prevent youth suicide. This crisis does not recognize political boundaries, and neither will the solutions. There is nothing partisan about keeping children alive. If we do not modernize our national suicide prevention framework now, the next generation of technology driven harms will outpace our ability to respond or protect vulnerable youth. This is not simply a mental health concern. It is a national child protection and suicide prevention issue at technological scale. History will record what Congress chose to do at this moment when the facts were clear and the consequences unmistakable.

A ten-year national strategy cannot keep pace with technology that evolves in real time. Social media evolves in real time. AI evolves in hyper time. Our prevention framework cannot move at a slower pace than the technologies shaping children's lives.

Reopening the Strategy is not merely an update. It is an opportunity to build a modern, responsive, and evidence-based partner for families, schools, and advocacy organizations in the fight to prevent youth suicide. A revised national strategy, aligned with the realities children face online, can become one of the most powerful tools this country has to protect young people.

Third, Big Tech and AI companies must be required to fund the solutions to the problems they have created, and their funding must come with no influence, control, or decision-making authority.

These companies should be responsible for paying for a national response. That includes funding training in schools for children and parents about the benefits and dangers of social media, the internet, and AI. They should bear the cost of suicide prevention education, mental health harm reduction, and other services that address the very problems their products have contributed to. These financial responsibilities should not be optional. They should not be left to families, schools, or taxpayers. They should be borne by the companies whose platforms and systems have helped create this crisis.

One additional obligation must be restored and made explicit: Big Tech must owe children a legally enforceable Duty of Care. This safeguard was removed from the House version of KOSA, and its absence leaves an unprotected gap at the center of this debate. No industry whose products directly shape the development, health, and safety of children should be allowed to operate without a clear, affirmative Duty of Care. For sectors that interact with children, such as cars, toys, medicine, and food, this duty is the baseline expectation. The platforms influencing children's behavior, emotions, and mental health at scale should not be held to a lesser standard. A Duty of Care is a foundational expectation that companies must eliminate practices that knowingly endanger children and that they must design with safety, not manipulation or engagement maximization, at the core.

To be explicit, Big Tech and AI companies should also be required to fund:

- **A National Warning Label System** on every platform and every AI tool that reaches minors.
- **Comprehensive digital safety education** in K to 12 schools, including curriculum, teacher training, and parent learning sessions, created independently of the companies that caused the problem.
- **Suicide prevention and mental health training**, including gatekeeper training, crisis response programs, and harm reduction strategies for youth.
- **Specialized education on self-harm, exploitation, algorithmic risk, and AI manipulation**, tailored for minors, parents, and educators.
- **Family support services**, including crisis navigation, counseling resources, and connections to evidence-based interventions.
- **Research on youth mental health and technology** that is fully independent, transparent, and insulated from corporate influence.
- **Public awareness campaigns** that warn families about the dangers of social media and AI at scale, similar to the counter-marketing efforts required of the tobacco industry.
- **Restorative and remedial programs** in communities disproportionately harmed by platform-induced mental health crises.
- **Screening tools, early intervention programs, and technology safety resources** for pediatricians, schools, and youth-serving nonprofits.

I also want to be 100 percent clear about one additional point. Funding these solutions does not entitle Big Tech or AI companies to direct them, influence them, shape their curriculum, determine their messaging, or participate in their governance. The companies that created the crisis cannot control the programs meant to mitigate it.

Their role must be limited to paying for the work. The design, content, oversight, and implementation of these efforts must remain fully independent, led by public institutions, independent researchers, and organizations whose first and only obligation is the safety and wellbeing of children.

On behalf of SAVE, I wish to thank you for your work. Taken together, the various bills before you show something important. Congress is not blind to this crisis. You see it. You hear it. You know it. The names of these bills read like a catalog of the dangers facing our children.

The families we serve are not asking for perfection. They are asking for protection. They are asking for a country willing to meet the danger with the same seriousness, urgency, and courage that this moment demands.

Sincerely,

A handwritten signature in black ink, consisting of a stylized 'E' followed by a long horizontal stroke that loops back to the right.

Erich Mische
Chief Executive Officer
SAVE

Memorandum

To: Digital Childhood Alliance
 From: Tony Fabrizio, Bob Ward & John Ward
 Date: May 1, 2025
 Re: Parental Consent for Minor App Downloads

In our recently completed survey of voters nationwide, which included an oversample of voters who are parents/guardians of children under 18, there is wide, strong and bipartisan support for requiring app stores to obtain parental approval before children under 18 download apps. Parents are even more intensely supportive of the idea than voters overall. And overwhelming majorities believe a person should be 18 before entering into contracts, with parents needing to agree to an app's Terms of Service on a minor's device.

Strong, bipartisan support for requiring app stores to obtain parental approval to download apps

More than four-in-five voters overall (82%) support requiring app stores to obtain parental approval for minors to download apps. Among parents and Trump voters, that share is even higher at 88%, with more than two-thirds *strongly* supporting this requirement. Democrats (80%) and Independents (79%) are also broadly supportive of this requirement.

Do you support or oppose requiring app stores to obtain parental approval for minors to download apps?

	Overall	Parents	Trump Voters	Republicans	Independents	Democrats
Total Support	82	88	88	86	79	80
Total Oppose	11	7	8	10	11	13
Strongly Support	55	69	67	68	49	48
Somewhat Support	27	19	21	18	30	33
Somewhat Oppose	7	4	4	4	8	9
Strongly Oppose	4	3	4	6	3	5
Not Sure	7	5	4	4	10	6

Voters say it would be easier to provide approval through app stores versus individual apps

A clear majority of voters (63%) say it would be easier for parents to provide approval via an app store when their child requests to download an app. By contrast, less than one-quarter of voters (22%) say it would be easier to provide approval separately in each app. Parents themselves say it would be easier to provide approval in one place vs. in each individual app by a 68% - 21% margin. This preference is also consistent across partisan lines.

In your opinion, which of the following would be an easier way for parents to provide approval for their child to use an app?

	Overall	Parents	Trump Voters	Republicans	Independents	Democrats
Providing approval in one place, such as an app store, when their child requests to download the app	63	68	63	62	64	63
Providing approval separately in each app after it has already been downloaded	22	21	25	24	21	22
Not Sure	15	11	12	14	15	15

Legislators who support requiring app store parental approval to download apps stand to benefit

By a better than 8:1 margin, voters say they would be more, rather than less, likely to vote for a legislator who favors requiring app stores to obtain parental approval for minors to download apps. Parents and Trump voters are more positively inclined to vote for such a legislator than voters overall.

Would you be more likely or less likely to vote for a legislator who favors requiring app stores to obtain parental approval for minors to download apps, or would it make no difference?

	Overall	Parents	Trump Voters	Republicans	Independents	Democrats
More Likely	42	49	52	52	37	37
Less Likely	5	6	4	3	6	6
Makes No Difference	43	33	37	38	46	47
Not Sure	9	12	8	6	12	10

Overwhelming agreement that people should be 18 to enter into contracts, with large majorities saying parents should be required to give consent for app terms of service (TOS)

When asked about the age at which people should be able to enter contracts, about nine-in-ten voters (89%) say 18 years old, rather than 16 or 13. A similarly large share of voters (83%) say parents should be required to give consent before children under 18 can agree to an app's terms of service.

Now, turning to another topic, if you had to choose, at which of the following ages do you think people should be able to enter into and sign contracts?

	Overall	Parents	Trump Voters	Republicans	Independents	Democrats
18 years old	89	88	92	92	88	87
16 years old	6	6	4	5	6	7
13 years old	1	1	-	1	1	1
Not Sure	4	5	3	3	6	5

When users download an app, they typically need to agree to the app's terms of service, which describe the rules, policies, and conditions for accessing and using the app. Do you think parents should be required to give consent before children under 18 can agree to an app's terms of service?

	Overall	Parents	Trump Voters	Republicans	Independents	Democrats
Yes	83	85	90	89	80	80
No	9	5	6	6	11	11
Not Sure	7	9	5	5	9	9

Voters want an independent organization to assign age ratings to apps

There is strong backing for an independent organization to assign age ratings to apps – similar to the ones used for movies and video games. Among parents in particular, more than three-in-four are supportive of this idea.

Do you think there should be an independent organization that helps assign age ratings to apps – similar to the ones for movies and video games?

	Overall	Parents	Trump Voters	Republicans	Independents	Democrats
Yes	73	76	68	69	72	78
No	16	12	19	17	17	12
Not Sure	11	12	13	13	11	10

Methodology

Fabrizio Ward, on behalf of the Digital Childhood Alliance, surveyed 1,000 registered voters nationwide, with an oversample of 500 registered voters who are parents or guardians of children under 18 who live in their household. The surveys were conducted April 21-25, 2025 via a mixed mode of interviewing, including 25% of interviews conducted by a live interviewer calling landline phones, 35% conducted by a live interviewer calling cell phones, and 40% of the interviews conducted online via text-to-web. The sample was sourced from the voter list. The margin of error for national registered voters is $\pm 3.1\%$ at the 95% confidence level. The margin of error for parents is $\pm 4.38\%$. The national registered voter sample was weighted by gender, age, race/ethnicity, education, and recalled 2024 vote to match registered voter targets based on voter file data, Census data, and 2024 election results. The parents sample was weighted by gender, age, race/ethnicity, education, and recalled 2024 vote to match targets from parents sampled in the core, Census data, and AP VoteCast data. Percentages reported above may not add up to 100% in all cases, due to rounding.

December 1, 2025

The Honorable Brett Guthrie
2161 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Frank Pallone
2107 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Gus Bilirakis
2306 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Jan Schakowsky
2408 Rayburn House Office Building
Washington, D.C. 20515

Re: The App Store Accountability Act

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

Members of the College Republicans at Indiana University (IU) are leaders of the college Republican movement. We are IU's premier organization dedicated to developing student leaders and promoting conservative principles. For the sake of young people across the country, we urge you to support the [App Store Accountability Act](#). It will protect children and teens from dangers lurking online.

College students understand how unchecked the digital ecosystem is. We are part of the first generation to grow up with ubiquitous access to smart devices. Many of our peers have been victims of online predators and inappropriate or harmful digital content, and it is only becoming more common for young children and teens today. With a few clicks, a child can access inappropriate and offensive media. We ask that your Committee reaffirm that parents have the right to protect their children from harmful content.

The App Store Accountability Act would give parents the power to dictate what content their children are allowed to see. It would require parents to approve any app before a child can download it to his or her device, helping foster meaningful discussions between children and parents about safe online habits. Parents can also ensure the content their child sees aligns with their family and religious values.

It is our understanding that the House Energy & Commerce Subcommittee on Commerce, Manufacturing, and Trade will be holding a hearing on childhood digital safety on December 2, 2025. We applaud your attention to this crisis threatening our nation's youth, and respectfully urge you to conduct

a timely markup and vote so Members can take the necessary next steps to advance these urgent safeguards.

As college Republicans, our goal is to encourage students to become active in the political process by registering to vote and learning about candidates and issues. The young conservative movement is growing like never before, and we are united in support of common-sense, pro-family legislation like the App Store Accountability Act.

The Indiana University College Republicans thanks you for your hard work and encourages you to continue to support its advancement.

Sincerely,

Indiana University College Republicans
1309 E Tenth St
Bloomington, IN 47405



Chairman Brett Guthrie
2161 Rayburn House Office Building
Washington, D.C. 20515

Chairman Gus Bilirakis
2306 Rayburn House Office Building
Washington, D.C. 20515

Ranking Member Frank Pallone
2107 Rayburn House Office Building
Washington, D.C. 20515

Ranking Member Jan Schakowsky
2408 Rayburn House Office Building
Washington, D.C. 20515

Re: App Store Accountability Act to Protect Kids & Empowers Parents

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

On behalf of [Latinos for Tennessee](#), we are writing to urge your support during the House Energy & Commerce Committee hearing for an urgent piece of legislation that embodies our organization's faith-based and family-centered values: the [App Store Accountability Act](#) (H.R. 3149 / S. 1596).

The App Store Accountability Act delivers needed reforms to the app store – the gateway to millions of digital platforms – to help keep kids safe and parents informed. Harnessing app stores' built-in age-verification and data management capabilities, the bill transforms the app store into a streamlined checkpoint for informed parental consent, empowering parents to review, block and approve all platforms minors request to download, all in one place.

For far too long, app stores have operated with little accountability and left parents in the dark. Children have been able to download harmful platforms and even unknowingly agree to complex contracts at just the touch of a button. Not only do these agreements give apps sweeping access to kids' personal data – ranging from photos, contact lists, exact locations and even microphones and cameras – but the apps themselves can also expose children to digital dangers they are unprepared to navigate.

We hope you will stand with the [88% of American parents](#) who support the App Store Accountability Act's common-sense premise: just like kids can't open a library card or attend a school field trip without a parent's signature, app stores should have to ask a parent's permission before entering a contract with a minor that allows them to download an app or make an in-app purchase.

Guided by our firm belief that [empowering parents](#) protects kids and strengthens communities, we humbly ask for you to support the App Store Accountability Act and advance this important bill out of the subcommittee and to the full House Energy & Commerce Committee.

We welcome this opportunity to align children's online experiences with their families' values and stand ready to lend our voices and resources to help put kids' safety first.

Sincerely,



Raul Lopez
Chairman of the Board & Co-Founder
Latinos for Tennessee



Tommy Vallejos
Executive Director & Co-Founder

cc:

House Energy & Commerce Committee

House Energy & Commerce Committee on Commerce, Manufacturing & Trade



December 1, 2025

The Honorable Brett Guthrie
Chairman
U.S. House Committee on
Energy and Commerce
Washington, DC 20515

The Honorable Frank Pallone
Ranking Member
U.S. House Committee on
Energy and Commerce
Washington, DC 20515

The Honorable Gus Bilirakis
Chairman
U.S. House Subcommittee on
Commerce, Manufacturing, and Trade
Washington, DC 20515

The Honorable Jan Schakowsky
Ranking Member
U.S. House Subcommittee on
Commerce, Manufacturing, and Trade
Washington, DC 20515

RE: H.R. 6291, Children and Teens' Online Privacy Protection Act ("COPPA 2.0")

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

The Main Street Privacy Coalition (MSPC) and its member organizations appreciate the Committee's work in developing H.R. 6291, the Children and Teens' Online Privacy Protection Act ("COPPA 2.0"), to amend the Children's Online Privacy Protection Act of 1998 ("COPPA"). In particular, we appreciate the work of Reps. Tim Walberg and Laurel Lee in introducing a revised version of COPPA 2.0 that addresses two significant concerns Main Street businesses raised with past versions of the House bill and the current version of the Senate bill.

The MSPC member associations represent a broad array of companies that line America's Main Streets, from retailers to restaurants, grocery stores to convenience stores, hotels to resorts, and gas stations to a wide range of franchise establishments. MSPC members' companies interact with consumers on a daily basis and can be found in every town, city, and state, providing jobs, supporting our economy, and serving Americans as a vital part of their communities. Collectively, the industry sectors that MSPC trade groups represent directly employ approximately 34 million Americans and constitute one-sixth of the U.S. economy by contributing \$4.5 trillion to the annual U.S. gross domestic product.¹

First, MSPC greatly appreciates that H.R. 6291 *preserves* COPPA's nearly three-decade primacy as the country's uniform national standard for children's privacy regulation and strengthens the existing preemption clause enacted in 1998. Second, MSPC is grateful that the bill recognizes the significant differences between Main Street businesses and high-impact social media companies by maintaining COPPA's actual knowledge standard for Main Street businesses while raising the bar for social media company practices that have driven legislators' concerns over the past several years.

¹ Additional information about the Main Street Privacy Coalition can be found at: <https://mainstreetprivacy.com>

Preserving COPPA's Primacy as a 27-Year Uniform, National Standard

As introduced, H.R. 6291 properly preserves COPPA as the uniform, national standard for children's privacy legislation. Main Street businesses have raised significant concerns with other versions of this legislation, including S. 836, that would amend and reverse the 27-year COPPA federal preemption standard that protects all American children equally, regardless of where they live, by preempting inconsistent state laws. We are concerned that S. 836 overturns the uniformity that has been a foundational principle of federal children's privacy law for over a quarter-century and encourages development of 51 different laws for the same personal data processed in interstate commerce. This would unduly burden Main Street businesses operating across state lines that have complied with COPPA since 1998. Further, that policy would result in children and teens being protected differently depending on the state in which they live, a condition and location over which these young individuals have no control. As Congress works to reform COPPA to establish an improved federal framework, it should protect and strengthen the balance achieved in the updated law by preserving COPPA as the uniform, national standard for children's and teens' privacy.

Maintaining an "Actual Knowledge" Standard for Main Street Businesses

H.R. 6291 greatly benefits from years of work by the bill sponsors to develop an appropriate definition for the term "knowledge" that recognizes the significant differences between Main Street businesses and high-impact social media companies. MSPC believes it is wholly appropriate for the Committee to adopt a more rigorous knowledge standard for Big Tech social media companies that have a history of abuses and collect significant amounts of highly sensitive data about children and teens, including the content of their communications, which provides greater awareness of their users' ages. Main Street businesses, on the other hand, do not collect nor wish to have this type of sensitive data or communications, and they lack any history of abuse that would justify altering their standard away from the "actual knowledge" standard in COPPA to a more subjective one. The careful balance achieved in the bill's context-dependent definition of "knowledge" is also supported by the hearing record before the Committee, which predominantly documents serious abuses by Big Tech social media companies (not Main Street businesses) in how they treat children and teens even when they could be aware of their age. It is important the bill maintain an actual knowledge standard for Main Street businesses selling goods to the general public in high volume on a daily basis because they lack the data and context to determine every customer's age in a mass market with a broad consumer base.

In closing, MSPC strongly supports passage of H.R. 6291 to maintain COPPA's primacy as a uniform, national law. We also strongly support the two-tiered knowledge standard that ensures Main Street businesses are not held liable for information they do not actually know.

Sincerely,

Main Street Privacy Coalition

cc: The Honorable Tim Walberg
The Honorable Laurel Lee
Members of the Committee on Energy and Commerce



December 1, 2025

The Honorable Gus Bilirakis, Chairman
House Subcommittee on Commerce, Manufacturing, and Trade
2306 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Jan Schakowsky, Ranking Member
House Subcommittee on Commerce, Manufacturing, and Trade
2408 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Bilirakis and Ranking Member Schakowsky:

At Apple, we want users of all ages to have the best possible experience with our technology. That's why we design all of our products, features, and services to protect the safety and privacy of our users — especially when it comes to kids and teens.

We believe we all have a role to play in keeping kids safe online, and at Apple, we're continuing to empower parents with innovative resources and tools that help keep children safe while also protecting their privacy. We appreciate your committee's interest and leadership on this important issue, and we welcome this opportunity to share our perspective and learnings as you consider federal legislation to strengthen protections for children online.

Apple's Tools For Parents

For many years, Apple has built safety and privacy into the core of our operating systems, creating a trusted ecosystem for our users. We also build them into our guidelines for developers on the App Store, which we rigorously enforce. This focus is not an afterthought; it is our starting point — and we are constantly innovating to empower parents and protect children's experience on our devices.

That includes the easy-to-use tools we've built to help parents protect kids and teens online, empowering them with the information and controls to make the right decisions for their families. Tools like Screen Time and Ask to Buy allow parents to manage how their children use their devices and approve — or decline — any app download. Parents can also use Communication Limits to limit who can start a conversation with their kids, and Content Restrictions to ensure that children only access age-appropriate apps, websites, and media. And with Communication Safety — which is on by default for all users under 18 with our latest software — we've pioneered a system that uses on-device intelligence to protect children from viewing or sharing photos or videos that contain nudity via Messages or AirDrop, without Apple ever seeing the photos. This technology is a prime example of our approach: providing powerful protection while rigorously preserving user privacy.



We are constantly innovating to build on this foundation. This year, as detailed in our White Paper, [Helping Protect Kids Online](#), we expanded these protections to help shield children from sensitive content in FaceTime in real time, and we created tools for developers to integrate this new capability into their apps as well. In September, we also released a new age assurance tool that further empowers parents and helps developers provide age-appropriate experiences. This privacy-preserving solution allows a parent to share their child's age range with an app developer, without having to share sensitive, specific information like a birthdate or government ID. We're constantly innovating to expand our protections for parents and developers, and over time, we've enabled more of our safety features by default to strengthen safety protections from the moment our users first access their Apple devices.

Beyond the software tools and features we offer, we enforce rigorous safety guidelines across our entire digital ecosystem. On the App Store, we have long enforced strict rules that require apps to protect children from inappropriate content, safeguard their data, and prohibit tracking children for advertising purposes or sharing children's data with data brokers. Should a developer be found to be in breach of these guidelines, we take immediate action to ensure they either come into compliance or face removal from our platform.

Online Safety, Privacy and Public Policy

While both platforms and developers have important roles to play in keeping kids safe online, there is also a critical role for thoughtful public policy. We welcome legislative efforts that aim to strengthen protections for kids, and we have been an engaged partner in these discussions.

This year, for instance, Apple endorsed S. 1748, the Kids Online Safety Act (KOSA), and we look forward to engaging with your committee as it considers companion legislation. We appreciate that KOSA emphasizes holding platforms accountable for the design of their services and equipping parents with robust tools — while also protecting and prioritizing their privacy. This legislation recognizes that accountability and empowerment are safer for families than mandating the collection of additional personal data, especially about children.

Unfortunately, not all legislative proposals are equally protective of privacy or focused on holding all players in the ecosystem accountable. Some well-intended proposals for age verification at the app marketplace level, for example, would require the collection of sensitive information about anyone who wants to download an app, even if it's an app that simply provides weather updates or sports scores. Consistent with principles of data minimization — collecting and using only the minimum amount of data required to deliver a service — Apple does not do this.

We share the goal of strengthening kids' online safety, but we are very concerned that such legislation could threaten the privacy of all users by forcing millions of adults to



surrender their private information for the simple act of downloading an app. There are better proposals that help keep kids safe without requiring millions of people to turn over their personal information. Apple's age assurance feature is one such example of a more achievable, privacy-focused path forward.

We recommend that any proposal to mandate app marketplace- or device-level age assurance should, at a minimum:

- Recognize that both app marketplaces and developers have a shared responsibility to keep children safe online; for instance, by ensuring that developers who already possess specific information about a user's age cannot disregard such knowledge.
- Clarify that compliance does not require the collection of sensitive information about children, like birth certificates or social security numbers.
- Entrust parents to provide the age of their child when establishing a child's account.
- Focus age assurance efforts on ensuring that parents who establish an account for their child are adults.
- Clarify that any personal information utilized to determine age need not be retained by app marketplaces or developers.
- Empower parents to decide whether the age range of their children is shared with developers.

By adhering to these principles, we can both protect children from online harms and protect their privacy as well. We can also mitigate the risks of scams and fraud that could result from children's personal information being collected, retained, or shared unnecessarily.

In sum, we believe everyone has a role to play and are committed to doing our part. We will continue to ensure families using our devices have intuitive tools to guide their children's digital experiences—and protect their privacy along the way. Other platforms and developers should also design their products with safety at the forefront.

By working together, we can build a digital future that is not only innovative and open but also safe and trusted for generations to come. We look forward to continuing to work with the committee on legislative proposals intended to keep children safe online.

Thank you,

A handwritten signature in black ink, appearing to be 'Hilary Ware', is located below the 'Thank you,' text.

Hilary Ware
Global Head of Privacy
Apple



CC: Members of the US House Of Representatives Committee on Energy and Commerce



1455 3rd Street
San Francisco, CA 94158

December 2, 2025

From:
Chan Park
Head of U.S. and
Canada Policy and
Partnerships
OpenAI

To:
The Honorable Gus
Bilirakis
Chairman
Subcommittee on
Commerce,
Manufacturing, and
Trade
Committee on
Energy and
Commerce
Washington, DC
20515

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

Re: Support for H.R. 6289, the Promoting a Safe Internet for Minors Act; the Assessing Safety Tools for Parents and Minors Act; and H.R. 5360, the AI Warnings And Resources for Education (AWARE) Act

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

OpenAI appreciates the opportunity to submit this statement for the record as the Subcommittee on Commerce, Manufacturing, and Trade considers legislative proposals to promote online safety for children and teens. Our mission is to ensure that artificial intelligence benefits all of humanity, which necessarily includes the young people who are growing up with these technologies, as well as the parents, educators, and communities who guide them.

OpenAI supports H.R. 6289, the *Promoting a Safe Internet for Minors Act*, from Representatives Laurel Lee and Darren Soto. The bill directs the Federal Trade Commission, working with government, education, nonprofit, and industry partners, to lead a nationwide public awareness campaign on safe internet use for minors. By promoting best practices, keeping families informed about online risks and benefits, and reporting annually to Congress, it would provide lasting infrastructure to help parents, educators, and young people navigate online spaces more safely. We appreciate Representatives Lee and Soto's leadership in updating the *Protecting Children in the 21st Century Act* to create a coordinated, evidence based approach to online safety that reflects how kids and teens actually use technology today.

We also support the *Assessing Safety Tools for Parents and Minors Act*, led by Representatives Russ Fulcher and Greg Landsman. The bill directs the FTC, with input from parents, industry, technologists, and mental health and privacy experts, to evaluate how companies use parental controls, safety settings, labels, and educational tools to protect minors online. The resulting report would assess the effectiveness of current tools and recommend improvements, helping policymakers focus on measures that work in practice. We appreciate Representatives Fulcher and Landsman for advancing a bipartisan, expert informed review of real world safety tools.

OpenAI further supports H.R. 5360, the *AI Warnings and Resources for Education (AWARE) Act*, introduced by Representatives Erin Houchin and Jake Auchincloss. The bill directs the FTC to develop clear educational resources for parents, educators, and minors on responsible use of AI chatbots. These materials would

explain responsible use, privacy, and data collection practices and offer practical guidance for parents overseeing their children's use of AI tools. By investing in accessible, model neutral education, the *AWARE Act* would help families understand both the benefits and limitations of AI systems. We thank Representatives Houchin and Auchincloss for recognizing the importance of practical guidance for parents and students.

These legislative proposals align closely with the public policy frameworks we have recently released on teen safety and AI literacy. In our [Teen Safety Blueprint](#), we set out standards for age appropriate product safeguards, privacy protective age estimation, and meaningful parental controls, and in our [Teen AI Literacy Blueprint](#), we call for practical support that helps teachers, families, and teens use AI safely, critically, and creatively. Taken together, these three bills would help operationalize those frameworks by strengthening public education about online risks and safeguards, driving evidence-based improvements in safety tools, and ensuring parents, teachers, and minors have clear resources for navigating AI enabled services. We view these bills as consistent with the principles in our blueprints and as an important step toward a shared goal of helping young people stay safe while benefiting from the opportunities AI can provide.

OpenAI is committed to working with Congress and stakeholders across the country to ensure that AI is developed and deployed in ways that are safe, beneficial, and broadly accessible, especially for children and teens. We thank the Committee for holding today's hearing, and we stand ready to serve as a resource as you continue examining how best to protect young people online while supporting innovation.

Sincerely,

A handwritten signature in black ink, appearing to read 'Chan Park', with a stylized flourish at the end.

Chan Park
Head of U.S. and Canada Policy and Partnerships
OpenAI



Statement for the Record
Hearing Before the Subcommittee on Commerce, Manufacturing, and Trade
Energy and Commerce Committee
United States House of Representatives
“Legislative Solutions to Protect Children and Teens Online”

December 2, 2025

Dear Chairman Bilirakis, Ranking Member Schakowsky, Chairman Guthrie, Ranking Member Pallone, and distinguished Members of the House Energy and Commerce Committee:

NetChoice respectfully submits this statement for the record regarding legislative solutions to protect kids online. NetChoice is a trade association of leading internet companies committed to promoting the value, convenience, and choice that internet business models provide to American consumers. Our mission is to make the internet safe for free enterprise and free expression.

We commend Chairman Guthrie and Chairman Bilirakis for convening this critically important hearing and for their steadfast leadership in addressing the complex challenges facing young people in the digital age. The Committee's comprehensive approach—examining 19 bills addressing various aspects of online child safety—demonstrates the seriousness with which you are approaching this issue. We share your commitment to protecting young people online, and we appreciate the opportunity to contribute to this vital conversation.

Effective child protection requires careful, evidence-based policymaking that respects constitutional principles, empowers families, holds bad actors accountable, and avoids unintended consequences that could harm the very children we seek to protect. We believe many of the proposals under consideration today can advance these goals when properly tailored to pass constitutional muster while achieving meaningful safety improvements.

NetChoice's Constitutional Track Record

NetChoice has been at the forefront of defending the First Amendment rights of both platforms and their users—including minors—in courts across the country. We have successfully challenged numerous state laws that, while framed as protecting children, would unconstitutionally restrict speech and limit young people's access to information. Our record demonstrates our unwavering commitment to defending constitutional rights while seeking genuine solutions to protect children.

Key Cases and Constitutional Principals

NetChoice v. Bonta (9th Circuit, 2024): The Ninth Circuit held that requiring platforms to assess and mitigate "harm" to children transforms design regulation into content regulation subject to strict scrutiny. The court recognized that vague harm-prevention mandates would lead platforms to block lawful content across the ideological spectrum—from conservative political organizing and religious expression to educational resources and community discussions. When the government demands that platforms opine on what speech might "harm" minors, it inevitably results in censorship that silences viewpoints bureaucrats. The Ninth Circuit emphasized that California had less restrictive means available, including empowering parental control tools, promoting digital education, and enforcing existing criminal laws.¹

Moody v. NetChoice (Supreme Court, 2025)²: Our challenges to Texas and Florida social media laws established that content moderation is protected editorial activity under the First Amendment. These victories affirm that states cannot compel platforms to host speech or dictate how they curate content. These cases protect the rights of platforms to curate and maintain a safe, appropriate environment for all users, including minors.

Free Speech Coalition v. Paxton (Supreme Court, 2025): While NetChoice was not a party in this case, this decision provides important guidance. The Court upheld Texas's age verification requirement for commercial websites with substantial sexually explicit material—but this narrow holding applies only to content unprotected as to minors, not general-purpose platforms hosting primarily protected speech. The distinction between pornography websites and social media platforms where Americans share news, organize politically, discuss their values and beliefs, engage in commerce, and exercise their First Amendment rights is constitutionally significant. Texas appropriately targeted actual obscenity for minors rather than censoring access to lawful speech, demonstrating how states can protect children online without infringing on the constitutional rights of citizens or overriding the authority of parents to guide their own children's development.

These cases establish several principles for constitutionally sound legislation:

1. **Content moderation restrictions** violate the First Amendment's guarantee that curators of speech can exercise editorial control over the speech on their services;
2. **Narrow targeting** of truly unprotected content for minors (like pornography) is permissible under *Paxton*;
3. **Compelled discussion of potential "harm" provisions** that require subjective content judgments will not survive scrutiny;
4. **Less restrictive alternatives** must be considered—parental tools, education, and enforcement; and
5. **Parental rights** cannot be overridden by one-size-fits-all government mandates.

¹ *NetChoice, LLC v. Bonta*, 113 F.4th 1101 (9th Cir. 2024)

² *Moody v. NetChoice, LLC*, 603 U.S. 703 (2024)

Legislation Under Consideration

Legislation such as the Promoting a Safe Internet for Minors Act and the Assessing Safety Tools for Parents and Minors Act represent exactly the kind of "less restrictive alternative" that courts have consistently identified as preferable to speech restrictions. The Promoting a Safe Internet for Minors Act would direct the FTC to launch a nationwide education campaign to teach children how to stay safe on the internet. Digital education empowers young people with the knowledge and skills to navigate online spaces safely, make informed decisions about their privacy, recognize manipulation and harmful content, and exercise their own judgment—all without government censorship or platform liability that inevitably leads to over-blocking of lawful speech.

Similarly, the Assessing Safety Tools for Parents and Minors Act directs the FTC to evaluate what is actually working to protect children online through education, parental controls, age-appropriate content labels, and privacy and safety settings. Evidence-based policymaking is essential in this rapidly evolving space. Too often, legislative proposals are driven by anecdotes, moral panic, or assumptions about technology rather than rigorous assessment of what interventions actually improve outcomes for children.

However, the App Store Accountability Act raises significant concerns. The Act would force app stores to verify users' ages and require parental consent for minors, which raises constitutional issues, weakens privacy, and imposes heavy regulatory burdens on platforms and developers. Rather than protecting young users, such legislation would chill free speech and restrict both minors' and adults' access to lawful apps and content. App store age-verification mandates also create new security and data-privacy risks by requiring collection and retention of sensitive personal information for all users—even those merely browsing benign apps.

The RESET Act also raises concerns. This legislation would prohibit anyone under 16 from establishing social media accounts, even on platforms that have implemented proper protective measures, thus contravening both First Amendment protections and this Committee's stated goal of safeguarding minors. Multiple state laws with comparable restrictions have already been blocked by courts for probable First Amendment violations.

Several other bills in this package contain provisions that merit careful examination. We are encouraged by the major revisions to the Kids Online Safety Act, including eliminating the vague and likely unconstitutional duty of care. However, the bill continues to incentivize covered services to verify the ages of their users in order to identify which users are minors and therefore be able to comply with the law.

We cannot emphasize enough that the Senate version of KOSA is a deeply flawed bill that threatens free speech. Its broad duty of care would force platforms to censor lawful speech based on vague standards of "harm" to minors—an approach federal courts have repeatedly rejected. The Senate bill represents the kind of government-mandated content moderation struck down in *NetChoice v. Bonta*. Rather than protecting children, it would empower officials and platforms to control what young people can access—fundamentally violating the First Amendment and parental rights. Any path forward on KOSA must reject this censorship framework and embrace constitutional alternatives that empower parents without sacrificing fundamental freedoms.

We look forward to working with the Committee to analyze implementation details, assess constitutional implications, and identify opportunities to strengthen protections while respecting fundamental rights.

Conclusion

Protecting children online is a goal we all share. But we must pursue that goal with wisdom, nuance, and respect for constitutional principles. Laws that sound tough on Big Tech may make for good headlines, but if they fail to protect children while infringing on rights and creating new privacy risks, they serve no one.

NetChoice stands ready to work with Committee members to advance legislation that effectively protects children while respecting constitutional principles and family autonomy. We believe this Committee is well-positioned to lead the nation toward solutions that can achieve bipartisan support, withstand judicial scrutiny, and make a genuine difference in young people's lives.

We appreciate the Committee's leadership on this critical issue and look forward to continued engagement as these proposals advance. Together, we can protect children and empower parents without sacrificing the constitutional freedoms that make America exceptional.

Sincerely,

Amy Bos

Vice President of Government Affairs, NetChoice

House Energy & Commerce Committee
Subcommittee on Commerce, Manufacturing, and Trade
2123 Rayburn House Office Building
Washington, D.C. 20515
December 2, 2025

Re: Letter for the Record for the Subcommittee on Commerce, Manufacturing, and Trade Hearing:
"Legislative Solutions to Protect Children and Teens Online"

Dear Chair Bilirakis and Ranking Member Schakowsky:

Thank you for convening this important legislative hearing focused on bills that protect children and teens online. We commend you and the subcommittee for its leadership in focusing attention on the digital threats facing young people and for recognizing the need to strengthen personal safeguards that can endure as technology continues to evolve.

Families today confront an online environment that is both empowering and perilous. While digital tools offer valuable opportunities for learning, creativity, and connection, they also expose children to significant risks, ranging from inappropriate content to aggressive data collection, scams, and identity theft. With more than a million children impacted by identity theft last year alone, young people remain uniquely vulnerable to misuse of their personal information.

Parents need resources that help them guide their children's digital lives with confidence. Understanding what personal information is, how it can be used, and why it must be protected is crucial. Clear privacy settings, accessible controls, and guidance on reducing exposure to data brokers and other third parties can help families create safer online environments. While putting requirements on companies is one way to provide support, there are also ways that children and families can be empowered to take matters into their own hands by using privacy-preserving technologies. Tools that remove exposed personal data, monitor for suspicious activity, and offer pseudonymous or persistent, virtual identifiers also provide valuable layers of protection, helping mitigate risks before they escalate.

As the subcommittee evaluates legislative solutions, we encourage a balanced approach that strengthens privacy and safety while preserving a supportive relationship between parents and their children. Tools that empower families, reduce unnecessary data exposure, and promote responsible online behavior, including the ability to protect private and sensitive data, can meaningfully enhance child safety without encouraging excessive surveillance or limiting access to beneficial information.

We appreciate the subcommittee's sustained attention to this issue and applaud your commitment to developing durable protections that meet the needs of children and families in the digital age. Thank you for your continued work to ensure a safer and more trustworthy online environment for America's youth.

Sincerely,

A black and white image of a handwritten signature, which appears to read "Arjun Bhatnagar".

Arjun Bhatnagar
Chief Executive Officer
Cloaked Inc.
www.cloaked.com



Tuesday, December 2nd, 2025

Subcommittee on Commerce, Manufacturing, and Trade Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

Dear Members of the Subcommittee on Commerce, Manufacturing, and Trade,

On behalf of the undersigned organizations, we write to express urgent concerns with the **Kids Online Safety Act (KOSA)**. While protecting young people online is a shared priority, this legislation poses a threat to the very youth it purports to protect, particularly in the current political climate. KOSA would empower government censorship of inclusive content, severely limit access to lifesaving resources, and grant sweeping enforcement powers to an administration that has demonstrated open hostility toward LGBTQ+ people, Black people, and other communities of color, and women.

The Political Reality Has Changed

Since taking office, the Trump administration has systematically targeted LGBTQ+ communities and communities of color: eliminating federal grants supporting LGBTQ+ and DEI initiatives, scrubbing Black history and LGBTQ+ content from government websites, accelerating book bans, weaponizing healthcare policy, and transforming schools into battlegrounds over identity¹. These attacks directly impact young people. LGBTQ+ youth face a mental health crisis—73% report anxiety symptoms, 58% experience depression, and one in five transgender youth have attempted suicide². Yet suicide prevention resources have been defunded, affirming school policies rescinded, and under Project 2025, federal agencies now openly question the legitimacy of LGBTQ+ lives.

KOSA would hand the Federal Trade Commission (FTC) authority to define and enforce what constitutes "harmful" content for minors instead of mandating that platforms provide age-appropriate options or user ratings for expansive parental and youth controls. When federal

¹Documentation of Trump administration actions available through federal agency policy trackers and LGBTQ+ advocacy organization monitoring reports, January 2025-present.

² The Trevor Project, 2024 National Survey on LGBTQ Youth Mental Health.



officials convene panels attacking gender-affirming care³, and the bill's own sponsor explicitly states its goal is preventing the "indoctrination" of children with transgender content⁴, this is not hypothetical—it is a blueprint for state-sanctioned censorship.

Constitutional and Technical Concerns

Vague Standards and Prior Restraint: KOSA's "duty of care" standard lacks constitutional precision, creating liability pressures that will compel platforms to over-censor protected speech. The outcome resembles the prior restraint struck down in *Bantam Books, Inc. v. Sullivan*, where government pressure to suppress disfavored content—even without direct prohibition—violated the First Amendment⁵.

Weaponized Enforcement Mechanisms: KOSA grants the FTC unprecedented discretion to determine what content harms minors, with state attorneys general empowered to enforce these standards according to local political priorities. The outcome would create a patchwork of censorship where the most restrictive state effectively governs national discourse—a dynamic the Supreme Court has repeatedly rejected⁶.

Inevitable Suppression of Vital Information: LGBTQ+ and reproductive health organizations—The Trevor Project, Planned Parenthood, GLSEN, PFLAG—already see their content wrongly flagged or suppressed by algorithmic moderation⁷. Under KOSA, such erasures would become systematic and intentional. For the 60% of LGBTQ+ youth who already cannot

³ Federal Trade Commission, "The Dangers of Gender-Affirming Care for Minors" panel event, July 2025. Available at: <https://www.ftc.gov/news-events/events/2025/07/dangers-gender-affirming-care-minors>

⁴ NBC News, "Senator appears to suggest bipartisan bill will censor transgender content," citing Sen. Marsha Blackburn's statements on KOSA's intended scope. Available at: <https://www.nbcnews.com/nbc-out/out-politics-and-policy/senator-appears-suggest-bipartisan-bill-will-censor-transgender-content-rcna103479>

⁵ *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58 (1963) (holding that informal government pressure to suppress distribution of books constituted unconstitutional prior restraint).

⁶ See *Brown v. Entertainment Merchants Ass'n*, 564 U.S. 786 (2011) (striking down content-based restrictions on minors' access to information); *Ashcroft v. ACLU*, 542 U.S. 656 (2004) (affirming strict scrutiny for content-based internet regulations).

⁷ Multiple LGBTQ+ organizations report content moderation systems flagging health information, suicide prevention resources, and community support content as "sensitive" or "potentially harmful," leading to reduced visibility or removal.



access needed mental health care⁸, and the 45% who face barriers to parental consent for services⁹ losing online resources could be catastrophic.

The Empirical Evidence Is Clear

LGBTQ+ youth, particularly those in rural communities and conservative environments, depend on internet access to find affirming information, build community, and access resources unavailable locally¹⁰. Recent research demonstrates that access to safe online spaces directly improves mental health outcomes for LGBTQ+ youth. Any legislation restricting youth access to information must be evaluated against this reality: for many LGBTQ+ young people, online resources are not supplemental—they are survival tools.

Our Position

LGBTQ+ advocates engaged in good-faith negotiations to narrow KOSA's scope and add safeguards. However, the political environment has undergone a fundamental shift. The same officials driving book bans and school censorship now explicitly identify KOSA as a mechanism to suppress LGBTQ+ content online. Passing this bill would deliver them precisely the authority they seek.

We therefore call on Congress to:

1. **Reject any version of KOSA** that enables content-based censorship and enforcement by partisan officials, or jeopardizes LGBTQ+ youth access to affirming resources.
2. **Conduct comprehensive impact assessments** examining how KOSA would affect marginalized youth populations across different age groups (acknowledging that the needs of toddlers, elementary school, preteens, 13-15, 16-17, and 18-21-year-olds are different) before any committee or floor consideration.
3. **Hold hearings centered on LGBTQ+ youth voices across age, race, gender, disability, and language identities**, ensuring that the young people most affected by

⁸ The Trevor Project, 2024 National Survey (finding 60% of LGBTQ+ youth who wanted mental health care in the past year were unable to access it).

⁹ GLSEN & Trevor Project research data on parental permission barriers to mental health services for LGBTQ+ youth.

¹⁰ TechCrunch, "LGBTQ+ youth have worse mental health outcomes without access to safe online spaces, studies show," September 25, 2025. Available at: <https://techcrunch.com/2025/09/25/lgbtq-youth-have-worse-mental-health-outcomes-without-access-to-safe-online-spaces-studies-show/>



this legislation testify on how it would impact their lives and well-being.

4. **Pursue alternative approaches** to youth safety that do not rely on government-defined content standards or create new censorship infrastructure that removes age-appropriate parental and youth consent and considerations.

Protecting young people online cannot come at the cost of silencing them. KOSA, as currently constructed, would do precisely that.

Sincerely,

Center for Black Equity

COLAGE

Hispanic Technology & Telecommunications Partnerships

GLSEN

LGBT Tech

National Black Justice Collective

National LGBTQ Task Force Action Fund

One Family Coalition



New requirements for apps available in Texas

October 8, 2025

Beginning January 1, 2026, a new state law in Texas — SB2420 — introduces age assurance requirements for app marketplaces and developers. While we share the goal of strengthening kids' online safety, we are concerned that SB2420 impacts the privacy of users by requiring the collection of sensitive, personally identifiable information to download any app, even if a user simply wants to check the weather or sports scores. Apple will continue to provide parents and developers with industry-leading tools that help enhance child safety while safeguarding privacy within the constraints of the law.

Once this law goes into effect, users located in Texas who create a new Apple Account will be required to confirm whether they are 18 years or older. All new Apple Accounts for users under the age of 18 will be required to join a Family Sharing group, and parents or guardians will need to provide consent for all App Store downloads, app purchases, and transactions using Apple's In-App Purchase system by the minor. This will also impact developers, who will need to adopt new capabilities and modify behavior within their apps to meet their obligations under the law. Similar requirements will come into effect later next year in Utah and Louisiana.

Today we're sharing details about updates that we're making and the tools we'll provide to help developers meet these new requirements.

To assist developers in meeting their obligations in a privacy-preserving way, we'll introduce capabilities to help them obtain users' age categories and manage significant changes as required by Texas state law. The Declared Age Range API is available to implement now, and will be updated in the coming months to provide the required age categories for new account users in Texas. And new APIs launching later this year will enable developers, when they determine a significant change is made to their app, to invoke a system experience to allow the user to request that parental consent be re-obtained. Additionally, parents will be able to revoke consent for a minor continuing to use an app. More details, including additional technical documentation, will be released later this fall.

We know protecting kids from online threats requires constant vigilance and effort. That's why we will continue to create industry-leading features to help developers provide age-appropriate experiences and safeguard privacy in their apps and games, and empower parents with a comprehensive set of tools to help keep their kids safe online.



Developer News **New requirements for apps available in Texas**

Platforms

- iOS
- iPadOS
- macOS
- tvOS
- visionOS
- watchOS

Tools

- Swift
- SwiftUI
- Swift Playground
- TestFlight
- Xcode
- Xcode Cloud
- Icon Composer
- SF Symbols

Topics & Technologies

- Accessibility
- Accessories
- Apple Intelligence
- App Store
- Audio & Video
- Augmented Reality
- Business
- Design
- Distribution
- Education
- Fonts
- Games
- Health & Fitness
- In-App Purchase
- Localization
- Maps & Location
- Machine Learning & AI
- Open Source
- Security
- Safari & Web

Resources

- Documentation
- Sample Code
- Tutorials
- Downloads
- Forums
- Videos

Support

- Support Articles
- Contact Us
- Bug Reporting
- System Status

Account

- Apple Developer
- App Store Connect
- Certificates, IDs, & Profiles
- Feedback Assistant

Programs

- Apple Developer Program
- Apple Developer Enterprise Program
- App Store Small Business Program
- MFI Program
- Mini Apps Partner Program
- News Partner Program
- Video Partner Program
- Security Bounty Program
- Security Research Device Program

Events

- Meet with Apple
- Apple Developer Centers
- App Store Awards
- Apple Design Awards
- Apple Developer Academies
- WWDC

Get the Apple Developer app.

Light Dark **Auto**

Copyright © 2025 Apple Inc. All rights reserved. [Terms of Use](#) [Privacy Policy](#) [Agreements and Guidelines](#)

English



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

For Your Information

FTC Approves Final Order in Case About Apple Inc. Charging for Kids' In-App Purchases Without Parental Consent

March 27, 2014



Tags: [Consumer Protection](#) | [Bureau of Consumer Protection](#) | [deceptive/misleading conduct](#) | [Technology](#) | [Credit and Finance](#) | [Payments and Billing](#) | [FinTech](#)

Following a public comment period, the Federal Trade Commission has approved a final order resolving FTC allegations that Apple Inc. unfairly charged consumers for in-app purchases incurred by children without their parents' consent.

The settlement was first announced by the Commission in January. In its complaint, the agency alleged that Apple failed to notify parents that entering their password would approve a purchase and then open a 15-minute window in which unlimited charges could be made without authorization. In the complaint, the FTC cited examples of children incurring thousands of dollars in in-app purchases without their parents' consent.

Under the settlement, by March 31, 2014, Apple must change its billing practices to ensure that it has obtained express, informed consent from consumers before charging them for in-app purchases.

Apple also must provide full refunds, totaling a minimum of \$32.5 million, to consumers who were billed for in-app purchases that were incurred by children and were either accidental or not authorized by the consumer. Should Apple issue less than \$32.5 million in refunds to consumers within the 12 months after the settlement becomes final, the company must remit the balance to the Commission. By April 15, 2014, Apple must notify all consumers charged for in-app purchases with instructions on how to obtain a refund for unauthorized purchases by kids.

The Commission vote approving the final order and letters to members of the public was 3-1, with Commissioner Wright voting in the negative. (FTC File No. 112-3108, the staff contacts in the Bureau of Consumer Protection are Duane Pozza, 202-326-2042; Jason Adler, 202-326-3231; and Miya Rahamim, 202-326-2351.)

The Federal Trade Commission works for consumers to prevent fraudulent, deceptive, and unfair business practices and to provide information to help spot, stop, and avoid them. To file a complaint in English or Spanish, visit the FTC's online Complaint Assistant or call 1-877-FTC-HELP (1-877-382-4357). The FTC enters complaints into Consumer Sentinel, a secure, online database available to more than 2,000 civil and criminal law enforcement agencies in the U.S. and abroad. The FTC's website provides free information on a variety of consumer topics. Like the FTC on Facebook, follow us on Twitter, and subscribe to press releases for the latest FTC news and resources.

Press Release Reference

[Apple Inc. Will Provide Full Consumer Refunds of At Least \\$32.5 Million to Settle FTC Complaint It Charged for Kids' In-App Purchases Without Parental Consent](#)

Contact Information

MEDIA CONTACT:

Jay Mayfield
Office of Public Affairs
202-326-2181

**UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION**

COMMISSIONERS: **Edith Ramirez, Chairwoman**
 Julie Brill
 Maureen K. Ohlhausen
 Joshua D. Wright

In the Matter of

APPLE INC., a corporation.

DOCKET NO. C-4444

DECISION AND ORDER

The Federal Trade Commission having initiated an investigation of certain acts and practices of the Respondent named in the caption hereof, and Respondent having been furnished thereafter with a copy of a draft complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge Respondent with a violation of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45 *et seq.*; and

Respondent and counsel for the Commission having thereafter executed an Agreement Containing Consent Order ("Consent Agreement"), which includes a statement by Respondent that it neither admits nor denies any of the allegations in the draft complaint, except as specifically stated in the Consent Agreement, and, only for purposes of this action, admits the facts necessary to establish jurisdiction; and waivers and other provisions as required by the Commission's Rules; and

The Commission having thereafter considered the matter and having determined that it has reason to believe that Respondent has violated the FTC Act, and that a complaint should issue stating its charges in that respect, and having thereupon accepted the executed Consent Agreement and placed such Consent Agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comments, and having duly considered any comments received from interested persons pursuant to Commission Rule 2.34, 16 C.F.R. § 2.34, now in further conformity with the procedure prescribed in Commission Rule 2.34, the Commission hereby issues its complaint, makes the following jurisdictional findings, and enters the following order:

1. Respondent Apple Inc. ("Apple") is a California corporation with its principal place of business at 1 Infinite Loop, Cupertino, California 95014.
2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of Respondent, and the proceeding is in the public interest.

ORDER

DEFINITIONS

For the purposes of this order, the following definitions shall apply:

1. **"Account Holder"** means an individual or entity, with a billing address in the United States, that controls an account to which Apple may bill In-App Charges.
2. **"Application"** or **"App"** means any software application that can be installed on a mobile device.
3. **"Clear and Conspicuous"** or **"Clearly and Conspicuously"** means:
 - A. In textual communications, the disclosure must be in a noticeable type, size, and location, using language and syntax comprehensible to an ordinary consumer;
 - B. In communications disseminated orally or through audible means, the disclosure must be delivered in a volume, cadence, language, and syntax sufficient for an ordinary consumer to hear and comprehend them;
 - C. In communications disseminated through video means: (1) written disclosures must be in a form consistent with definition 3.A and appear on the screen for a duration sufficient for an ordinary consumer to read and comprehend them, and be in the same language as the predominant language that is used in the communication; and (2) audio disclosures must be consistent with definition 3.B; and
 - D. The disclosure cannot be combined with other text or information that is unrelated or immaterial to the subject matter of the disclosure. No other representation(s) may be contrary to, inconsistent with, or in mitigation of, the disclosure.
4. **"Defendant"** means Apple Inc. and its successors and assigns.

5. **“Express, Informed Consent”** means, upon being presented with options to provide or withhold consent, an affirmative act communicating informed authorization of In-App Charge(s), made proximate to an In-App Activity for which there is an In-App Charge and to Apple’s Clear and Conspicuous disclosure of all material information related to the billing, including:

A. If consent is sought for a specific In-App Charge: (1) the In-App Activity associated with the charge (as provided to Apple by the App’s developer); (2) the specific amount of the charge; and (3) the account that will be billed for the charge; or

B. If consent is sought for potential future In-App Charges: (1) the scope of the charges for which consent is sought, including the duration and Apps to which consent applies; (2) the account that will be billed for the charge; and (3) method(s) through which the Account Holder can revoke or otherwise modify the scope of consent on the device, including an immediate means to access the method(s).

Provided that the solicitation of the “affirmative act” and the disclosure of the information in definitions 5.A and 5.B above must be reasonably calculated to ensure that the person providing Express, Informed Consent is the Account Holder.

Provided also that if Apple obtains Express, Informed Consent to potential future In-App Charges as set forth in definition 5.B above, it must do so a minimum of once per mobile device.

6. **“In-App Activity”** or **“In-App Activities”** means any user conduct within an App including the acquisition of real or virtual currency, goods, or services, or other Apps.

7. **“In-App Charge”** means a charge associated with In-App Activity billed by Apple.

8. **“Consumer Redress Period”** means the twelve (12) month period of time between the entry and the first anniversary of this order.

I.

IT IS FURTHER ORDERED that Apple and its officers, agents, and employees, and all other persons in active concert or participation with it, who receive actual notice of this order, whether acting directly or indirectly, are restrained and enjoined for the term of this order from billing an account for any In-App Charge without having obtained Express, Informed Consent to Apple’s billing that account for the In-App Charge. If Apple seeks and obtains Express, Informed Consent to billing potential future charges for In-App Activities, Apple must allow the Account Holder to revoke such consent at any time. Apple shall fully comply with this Section I by no later than March 31, 2014.

II.

IT IS FURTHER ORDERED that Apple shall provide full refunds to Account Holders who have been billed by Apple for unauthorized In-App Charges incurred by minors as follows:

A. Apple shall provide prompt refunds to Account Holders for the full purchase price of any Eligible In-App Charge(s). For purposes of this Section II, an "Eligible In-App Charge" is an In-App Charge that the Account Holder indicates was incurred by a minor and was accidental or not authorized by the Account Holder. For purposes of this Section II.A, a "prompt" refund means a refund provided within the later of fourteen (14) days of a request for refund of an Eligible In-App Charge by the Account Holder or the completion of a fraud investigation. Apple may decline a refund request for an Eligible In-App Charge only if it has sufficient credible evidence that the refund request is fraudulent. Apple may process all refund requests through its customer service channels, which include a contact phone number and web form through which consumers may contact Apple directly.

B. Apple shall refund no less than \$32,500,000.00 for Eligible In-App Charges pursuant to section II.A of this order, and such amount shall not constitute a penalty. Solely for the purposes of this section II.B of this order, Apple may approximate that 50% of all refunds provided to Account Holders for In-App Charges relate to Eligible In-App Charges.

C. Within thirty (30) days of the end of the Consumer Redress Period, Apple shall provide the Commission with records sufficient to show the refunds requested and paid to Account Holders for In-App Charges during the Consumer Redress Period, and any requests that were denied under Section II.A of this order.

D. If Apple fails to refund \$32,500,000.00 pursuant to section II.B of this order, the balance of that amount shall be remitted to the Commission within forty-five (45) days of the end of the Consumer Redress Period.

E. All funds paid to the Commission pursuant to section II.D of this order may be deposited into a fund administered by the Commission or its designee to be used for equitable relief, at the Commission's sole discretion, for informational remedies regarding In-App Charges by children or consumer redress and any attendant expenses for the administration of any redress fund. Any money not used for such purposes shall be deposited to the United States Treasury. Apple shall have no right to challenge the Commission's choice of remedies under this Paragraph.

F. Apple shall provide an electronic notice to any Account Holder who has made an In-App Purchase prior to March 31, 2014. Apple shall send such notice within fifteen (15) days after March 31, 2014. The electronic notice shall include a subject line relating to the content of the notice and contain the following information, disclosed in a Clear and Conspicuous manner and in writing: (1) that refunds are available for Account Holders that have been billed for In-App Charges incurred by minors that were accidental or not authorized by the Account Holder, (2) that such refunds are available until the end of the Consumer Redress Period, and (3) instructions regarding how to obtain refunds pursuant to section II.A of this order, including

means of contacting Apple for a refund. Apple shall send the notice to the current or last known email address for the Account Holder.

G. Sections II.A and II.B of this order shall be effective beginning on the date that the order is entered, and will terminate at the end of the Consumer Redress Period.

III.

IT IS FURTHER ORDERED that Respondent and its successors and assigns for five (5) years after the date of issuance of this order, shall maintain and upon request make available to the Federal Trade Commission business records demonstrating their compliance with the terms and provisions of this order, including but not limited to:

- A. All consumer complaints conveyed to Respondent, or forwarded to Respondent by a third party, that relate to the conduct prohibited by this order and any responses to such complaints;
- B. Refund requests related to In-App Charges, and refunds paid by Respondent related to In-App Charges; and
- C. Records necessary to demonstrate full compliance with each provision of this order.

IV.

IT IS FURTHER ORDERED that Respondent and its successors and assigns shall deliver a copy (written or electronic) of this order to all current and future principals, officers, and corporate directors, and to all current and future managers, employees, agents, and representatives who participate in the design or implementation of Respondent's process through which Account Holders incur In-App Charges; the billing by Respondent of such charges; or Respondent's customer service relating to such charges, and shall secure from each such person a signed and dated statement acknowledging receipt of the order. Respondent shall deliver this order to current personnel within thirty (30) days after the date of service of this order, and to future personnel within thirty (30) days after the person assumes such position or responsibilities.

V.

IT IS FURTHER ORDERED that Respondent and its successors and assigns shall notify the Commission within fourteen (14) days of any change in the corporation that may affect compliance obligations arising under this order, including but not limited to a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. All notices required by this Part shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

VI.

IT IS FURTHER ORDERED that Respondent or its successors and assigns shall, ninety (90) days after March 31, 2014, file with the Commission a report, in writing, setting forth in detail the manner and form in which they have complied with this order. Within ten (10) business days of receipt of a written notice from a representative of the Commission, Respondent shall submit additional compliance reports.

VII.

This order will terminate on March 25, 2034, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

- A. Any Part in this order that terminates in less than twenty (20) years; and
- B. This order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that the Respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal. Respondent may seek modification of this order pursuant to 15 U.S.C. § 45(b) and 16 C.F.R. 2.51(b) to address relevant developments that affect compliance with this order, including, but not limited to, technological changes and changes in methods of obtaining Express, Informed Consent.

By the Commission, Commissioner Wright dissenting.

Donald S. Clark
Secretary

SEAL:
ISSUED: March 25, 2014



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

For Your Information

FTC Approves Final Order in Case About Google Billing for Kids' In-App Charges Without Parental Consent

December 5, 2014



Tags: [Consumer Protection](#) | [Bureau of Consumer Protection](#) | [Technology](#) | [Credit and Finance](#) | [Payments and Billing](#)

Following a public comment period, the Federal Trade Commission has approved a [final order resolving FTC allegations that Google, Inc., unfairly billed consumers](#) for in-app charges incurred by children without their parents' consent.

[The settlement was first announced by the Commission in September.](#) It resolves allegations that Google billed consumers millions of dollars for charges incurred by children without consent from account holders. When Google first introduced in-app charges to the Google Play store in 2011, the FTC's complaint alleged, Google billed for such charges without any password requirement or other method to obtain account holder authorization. The complaint also alleged that even after requiring a password to incur in-app charges, [the company failed to tell parents that entering the password would then open a 30-minute window during which children could make unlimited charges without authorization.](#)

[The settlement requires Google](#) to provide full refunds of unauthorized in-app charges incurred by children and [to modify its billing practices to obtain express, informed consent from consumers before billing them for in-app charges.](#) If the company gets consumers' consent for future charges, consumers must have the option to withdraw their consent at any time.

In addition, Google is required to contact all consumers who had an in-app charge to inform them of the refund process for unauthorized in-app charges by children within 15 days of the order being finalized. Google must make these refunds promptly, upon request from an account holder. Should the company provide less than \$19 million in refunds within a year of the settlement's approval, the company will be required to remit the balance to the Commission for use in providing additional remedies to consumers or for return to the U.S. Treasury.

The Commission vote approving the final order and response letters to commenters was 4-0-1, with Commissioner Wright recused. (FTC File No. 122-3237, the staff contacts in the Bureau of Consumer Protection are Duane Pozza, 202-326-2042 and Jason Adler, 202-326-3231.)

The Federal Trade Commission works for consumers to prevent fraudulent, deceptive, and unfair business practices and to provide information to help spot, stop, and avoid them. To file a complaint in English or Spanish, visit the FTC's online Complaint Assistant or call 1-877-FTC-HELP (1-877-382-4357). The FTC enters complaints into Consumer Sentinel, a secure, online database available to more than 2,000 civil and criminal law enforcement agencies in the U.S. and abroad. The FTC's website provides free information on a variety of consumer topics. Like the FTC on Facebook, follow us on Twitter, and subscribe to press releases for the latest FTC news and resources.

Press Release Reference

[Google to Refund Consumers at Least \\$19 Million to Settle FTC Complaint It Unlawfully Billed Parents for Children's Unauthorized In-App Charges](#)

Contact Information

MEDIA CONTACT:

Justin Cole

Director, Office of Public Affairs

202-326-3330

**UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION**

COMMISSIONERS: **Edith Ramirez, Chairwoman**
 Julie Brill
 Maureen K. Ohlhausen
 Joshua D. Wright
 Terrell McSweeney

In the Matter of

**GOOGLE INC.,
a corporation.**

DOCKET NO. C-4499

DECISION AND ORDER

The Federal Trade Commission having initiated an investigation of certain acts and practices of the Respondent named in the caption hereof, and Respondent having been furnished thereafter with a copy of a draft complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge Respondent with a violation of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45 *et seq.*; and

Respondent and counsel for the Commission having thereafter executed an Agreement Containing Consent Order ("Consent Agreement"), which includes a statement by Respondent that it neither admits nor denies any of the allegations in the draft complaint, except as specifically stated in the Consent Agreement, and, only for purposes of this action, admits the facts necessary to establish jurisdiction; and waives and other provisions as required by the Commission's Rules; and

The Commission having thereafter considered the matter and having determined that it has reason to believe that Respondent has violated the FTC Act, and that a complaint should issue stating its charges in that respect, and having thereupon accepted the executed Consent Agreement and placed such Consent Agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comments, and having duly considered the

comments received from interested persons pursuant to Commission Rule 2.34, 16 C.F.R. § 2.34, now in further conformity with the procedure prescribed in Commission Rule 2.34, the Commission hereby issues its complaint, makes the following jurisdictional findings, and enters the following order:

1. Respondent Google Inc. (“Google”) is a Delaware corporation with its principal place of business at 1600 Amphitheatre Parkway, Mountain View, California 94043.
2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of Respondent, and the proceeding is in the public interest.

ORDER

DEFINITIONS

For the purposes of this order, the following definitions shall apply:

1. **“Account Holder”** means an individual or entity, with a billing address in the United States, that controls an account to which Google may bill In-App Charges.
2. **“Application”** or **“App”** means any software application that can be installed on a mobile device.
3. **“Clear and Conspicuous”** or **“Clearly and Conspicuously”** means:
 - A. In textual communications, the disclosure must be in a noticeable type, size, and location, using language and syntax comprehensible to an ordinary consumer;
 - B. In communications disseminated orally or through audible means, the disclosure must be delivered in a volume, cadence, language, and syntax sufficient for an ordinary consumer to hear and comprehend them;
 - C. In communications disseminated through video means: (1) written disclosures must be in a form consistent with definition 3.A and appear on the screen for a duration sufficient for an ordinary consumer to read and comprehend them, and be in the same language as the predominant language that is used in the communication; and (2) audio disclosures must be consistent with definition 3.B; and
 - D. The disclosure cannot be combined with other text or information that is unrelated or immaterial to the subject matter of the disclosure. No other representation(s) may be contrary to, inconsistent with, or in mitigation of, the disclosure.
4. **“Respondent”** or **“Google”** means Google Inc. and its successors and assigns.

5. **“Express, Informed Consent”** means, upon being presented with options to

provide or withhold consent, an affirmative act communicating informed authorization of In-App Charge(s), made proximate to an In-App Activity for which there is an In-App Charge and to Clear and Conspicuous disclosure of all material information related to the billing, including:

A. If consent is sought for a specific In-App Charge: (1) the In-App Activity associated with the charge; (2) the specific amount of the charge; and (3) the account that will be billed for the charge (e.g., the Google account); or

B. If consent is sought for potential future In-App Charges: (1) the scope of the charges for which consent is sought, including the duration, devices, and Apps to which consent applies; (2) the account that will be billed for the charge; and (3) method(s) through which the Account Holder can revoke or otherwise modify the scope of consent on the device, including an immediate means to access the method(s).

Provided that in obtaining Express, Informed Consent, Google may rely on information provided by the App’s developer about the In-App Activity associated with the In-App Charge.

Provided also that the means of requesting the “affirmative act” and the disclosure of the information in definitions 5.A and 5.B above must be reasonably calculated to ensure that the person providing Express, Informed Consent is the Account Holder.

Provided also that if Google obtains Express, Informed Consent to potential future In-App Charges as set forth in definition 5.B above, it must do so a minimum of once per account or mobile device.

6. **“In-App Activity”** or **“In-App Activities”** means any user conduct within an App including the acquisition of real or virtual currency, goods, or services or other Apps.

7. **“In-App Charge”** means a charge associated with In-App Activity billed by Google.

8. **“Consumer Redress Period”** means the twelve (12) month period of time between the entry and the first anniversary of this order.

I.

IT IS FURTHER ORDERED that Google and its officers, agents, and employees, and all other persons in active concert or participation with it, who receive actual notice of this order, whether acting directly or indirectly, **are restrained and enjoined for the term of this order from billing an account for any In-App Charge without having obtained Express, Informed Consent to Google’s billing that account for the In-App Charge.** If Google seeks and obtains Express, Informed Consent to billing potential future charges for In-App Activities, Google must allow the Account Holder to revoke such consent at any time.

Provided that this section does not apply where Google does not control the user interface in which the In-App Charge is incurred.

Provided also that, where an Account Holder provides Express, Informed Consent to potential future In-App Charges at the account level, Google will provide, at least once before the first In-App Charge on a device, Clear and Conspicuous disclosure of the information in 5.B.

II.

IT IS FURTHER ORDERED that Google shall provide full refunds to Account Holders who have been billed by Google for unauthorized In-App Charges incurred by minors as follows:

A. Google shall provide prompt refunds to Account Holders for the full purchase price of any Eligible In-App Charge(s). For purposes of this Section II, an "Eligible In-App Charge" is an In-App Charge that the Account Holder indicates was: (1) paid by the Account Holder and incurred by a minor; (2) and was accidental or not authorized by the Account Holder; and (3) has not already been refunded. For purposes of this Section II.A, a "prompt" refund means a refund provided within the later of (1) thirty (30) days for a refund issued by check or ten (10) days for a refund issued by other means of a request for refund of an Eligible In-App Charge by the Account Holder; or (2) the completion of a fraud investigation. Google may decline a refund request for an Eligible In-App Charge only if it has sufficient credible evidence that the refund request is fraudulent. Google may process all refund requests through its customer service channels, which include a contact phone number and web form through which consumers may contact Google directly.

B. Google shall refund no less than \$19,000,000 for Eligible In-App Charges pursuant to section II.A of this order, and such amount shall not constitute a penalty.

C. Within thirty (30) days of the end of the Consumer Redress Period, Google shall provide the Commission with records sufficient to show the refunds requested and paid to Account Holders for In-App Charges during the Consumer Redress Period, and any requests that were denied under Section II.A of this order.

D. If Google fails to refund \$19,000,000 pursuant to section II.B of this order, the balance of that amount shall be remitted to the Commission within forty-five (45) days of the end of the Consumer Redress Period.

E. All funds paid to the Commission pursuant to section II.D of this order may be deposited into a fund administered by the Commission or its designee to be used for equitable relief, at the Commission's sole discretion, for informational remedies regarding In-App Charges by children or consumer redress and any attendant expenses for the administration of any redress fund. Any money not used for such purposes shall be deposited to the United States Treasury. Google shall have no right to challenge the Commission's choice of remedies under this Paragraph.

F. Google shall provide an electronic notice to any Account Holder who has made an In-App Purchase prior to entry of the order. Google shall send such notice within fifteen (15) days after entry of the order. The electronic notice shall include a subject line relating to the content of the notice and contain the following information, disclosed in a Clear and Conspicuous manner and in writing: (1) that refunds are available for Account Holders that have been billed for In-App Charges incurred by minors that were not authorized by the Account Holder, (2) that such refunds are available until the end of the Consumer Redress Period, and (3) instructions regarding how to obtain refunds pursuant to section II.A of this order, including means of contacting Google for a refund. Google shall send the notice to the current or last known email address for the Account Holder.

G. Sections II.A and II.B of this order shall be effective beginning on the date that the order is entered, and will terminate at the end of the Consumer Redress Period.

III.

IT IS FURTHER ORDERED that Respondent and its successors and assigns for five (5) years after the date of issuance of this order, shall maintain and upon request make available to the Federal Trade Commission business records demonstrating their compliance with the terms and provisions of this order, including but not limited to:

A. All complaints from United States consumers conveyed to Respondent, or forwarded to Respondent by a third party, that relate to the conduct prohibited by this order and any responses to such complaints;

B. Refund requests from United States consumers related to In-App Charges, and refunds paid by Respondent related to In-App Charges; and

C. Records necessary to demonstrate full compliance with each provision of this order.

IV.

IT IS FURTHER ORDERED that Respondent and its successors and assigns shall deliver a copy (written or electronic) of this order to all current and future principals, officers, and corporate directors, and to all current and future managers, employees, agents, and representatives who have supervisory responsibility regarding the design of the platform in which Account Holders incur In-App Charges and those who implement that design. For the duration of the Consumer Redress Period, Respondent and its successors and assigns shall deliver a copy (written or electronic) of this order to all current and future employees who have responsibility for providing refunds to consumers in connection with this order. Respondent shall deliver this order to current personnel within thirty (30) days after the date of service of this order, and to future personnel within thirty (30) days after the person assumes such position or responsibilities.

V.

IT IS FURTHER ORDERED that Respondent and its successors and assigns shall notify the Commission within fourteen (14) days of any change in the corporation that may affect compliance obligations arising under this order, including but not limited to a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. All notices required by this Part shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

VI.

IT IS FURTHER ORDERED that Respondent or its successors and assigns shall, ninety (90) days after entry of the order, file with the Commission a report, in writing, setting forth in detail the manner and form in which they have complied with this order. Within ten (10) business days of receipt of a written notice related to this order from a representative of the Commission, Respondent shall submit an additional compliance report setting forth the manner and form in which Respondent has complied with this order.

VII.

This order will terminate on December 2, 2034, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

- A. Any Part in this order that terminates in less than twenty (20) years; and
- B. This order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that the Respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date

such dismissal or ruling is upheld on appeal. Respondent may seek modification of this order pursuant to 15 U.S.C. § 45(b) and 16 C.F.R. 2.51(b) to address relevant developments that affect compliance with this order, including, but not limited to, technological changes and changes in methods of obtaining Express, Informed Consent.

By the Commission, Commissioner Wright recused.

Donald S. Clark
Secretary

SEAL:

ISSUED: December 2, 2014



December 2, 2025

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

We, the undersigned coalition of child advocacy organizations, remain steadfast in our endorsement of the App Store Accountability Act and ask for your support for the bill during the upcoming hearing by the House Energy & Commerce Subcommittee on Commerce, Manufacturing, and Trade.

Parents want to keep their children safe, but they are battling a broken system. As the gatekeepers to the digital world, app stores have allowed children to download apps with potentially inappropriate content without their parents ever knowing. In the process, children are able to agree to complex contracts that grant sweeping access to their microphone, exact location, browsing history, and more.

The App Store Accountability Act offers a common-sense solution: give parents a way to review and manage the apps their kids can access and the accurate age-rating information to make informed choices about which platforms are appropriate. Importantly, the App Store Accountability Act accomplishes this goal in a content-neutral manner that does not encroach constitutional rights to free speech and privacy.

Unsurprisingly, this privacy-preserving child safety measure has won broad support from parents. A poll by the Digital Childhood Alliance found that [88% of parents nationwide](#) want app stores to require parental approval before minors can download any app. The App Store Accountability Act would give parents this key tool, answering their calls for safe, streamlined oversight measures that put power where it belongs: with parents.

This year, the App Store Accountability Act was signed into law in Utah, Louisiana, and Texas with bipartisan support. Next year, more than one dozen additional states are expected to follow suit. With strong state momentum building, the time is now for Congress to step up to protect every child across the country and hold app marketplaces accountable by passing the App Store Accountability Act.

Thank you for your commitment to making our digital world safer for children and more manageable for parents. We encourage a more narrowly tailored preemption clause within the bill and then urge you to push this legislation forward in Congress. We continue to vocally support this bill with improved preemption language and are available to assist in any means necessary to ensure the App Store Accountability Act becomes law.

Sincerely,

Digital Childhood Alliance
3Strands Global Foundation
A Butterfly Gets Her Wings Back LLC
Addo Recovery - Washington
Alabama Policy Institute
Alaska State Representative Sarah Vance
Alexander Neville Foundation

All Girls Allowed, Inc.
Allies Against Slavery
American Principles Project
American Youth Association
ANEW Life International
Anna McAdams
Better Screen Time
Better Tech Project
Bilateral Safety Corridor Coalition
Black Americans United for Tennessee
Bowman Therapeutics
Breaking Generational Cycles
CA Survivor Coalition
Call to Freedom, Inc.
Center for Arizona Policy
Center for Christian Virtue
Center for Innovation and Free Enterprise
Chains Interrupted
Children at Risk
Christian Life Commission
Citizens for Renewing America
Concerned Women for America LAC
CORAFID Centre for Innovation and Research
David's Legacy Foundation
Defend Young Minds
DejaVuAI Inc.
Demand Disruption
Digital Childhood Institute
Digital Progress Institute
Dignity Defense Institute
Dr. Jill Manning, PLLC
Drew Boa Coaching LLC
Eagle Venture Fund
Ed & Nancy Hanenburg Children's Advocacy Center
Educate and Empower Kids
Elijah Rising
Empowered Parents Utah
Ethics and Public Policy Center
Evan Swarztrauber
Faith Wins America
Family Policy Alliance
Freedom Church Alliance
Frontline Policy
Georgia Center for Opportunity
GoSendMe Global
G-Rated School
Greenway Recovery
Growing Unified Development
Guided Purposes, LLC
Hannah's Hope
Healthy Screen Habits

Heritage Action
Hookers For Jesus
Hope Against Trafficking
Hope Connecting Purpose
Hope of Utah
Igniting Ember, Inc
Indiana University College Republicans
Innocence en Danger - Sellier
Institute for Families and Technology
Kentucky Family Foundation
KIDS TOO
Kingdom Forerunners
Latinos for Tennessee
Liberty Leaders Unite
Louisiana Family Forum
Luke Hogg
Lynn's Warriors
Magdalene House Austin
Massachusetts Family Institute
Mayor Melissa Elliott, Henderson, NC
Meg Leta Jones
Michigan Association of Non-Public Schools (MANS)
Minnesota Family Council
Moms for America, Utah
Moms for Liberty (National)
More Too Life
National Association of Christian Lawmakers
National Center for Missing and Exploited Children Texas
NC Stop Human Trafficking
New Jersey Coalition Against Human Trafficking
No Trafficking Zone
North Carolina Family Policy Council
Not On our Watch Texas
Nurses United Against Human Trafficking
Operation Parent KY
Palmetto Family Alliance
Parents Who Fight
Path Forward Utah
Paving the Way Foundation
Prevent Child Abuse Kentucky
Project STAND
Protect Life Michigan
Protect Young Eyes
Protecting the Gift
Refuge for Women Chicago
Resiliency Foundation
Rest Stop Ministries
Restore the Child, PLLC
Revelation & Restoration
Runaway Girl
Scarlet Road

Scrolling 2 Death
Sex Trade Survivor Caucus
Shield North Carolina
Skull Games
Smart Families
Society for the Improvement of Rural People (SIRP)
South Dakota Family Voice
Street Grace
Suicide Awareness Voices of Education (SAVE)
Survivor Leader Network of San Diego
Talk More. Tech Less.
Tech Safe Solutions LLC
Texans Care for Children
Texas Medical Foundation
Texas Pastor Council
Texas Public Policy Foundation
Texas Youth Foundation
TexProtects
The Commons
The Freeman Project Safe Housing
The Hope Foundation
The Institute for Family Studies
The Stop Trafficking Project®
The WellHouse
Tin Man Ministries
Tina Descovich
Traffick911
Trafficking in America Task Force
Transformation Garden
Truth in Education
Unbound Now
Utah Citizens for the Constitution
Utah Eagle Forum
Utah Legislative Watch
Utah Parents United
Utah Women's Forum, Salt Lake
Vessels of Mercy International, Inc.
Victims2Survivors – U.S.
Walk Her Home
Wyoming Family Alliance
Yellowstone Human Trafficking Task Force
Zoe Ministries of Delaware

cc: Speaker Mike Johnson
House Majority Leader Steve Scalise
House Minority Leader Hakeem Jeffries
House Energy & Commerce Committee
House Energy & Commerce Committee Subcommittee on Commerce, Manufacturing, and Trade



Monday, December 1, 2025

House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

Re: The App Store Accountability Act

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

The Alabama Policy Institute (API) believes the family unit is the cornerstone of our society. We write to support the advancement of the [App Store Accountability Act](#) introduced by Sen. Mike Lee and Rep. John James. Legislation like this is the best way to keep children safe online while preserving parental rights and empowering American families.

Right now, malicious online actors are waging war on American families. Modern technology has created a pipeline of inappropriate, violent, and dangerous content – all of which feeds directly to our children. Parents across the country, regardless of their political leanings, are asking for help. Even the most responsible parents struggle to manage and monitor what their children see online.

At API, we advocate for policies that reinforce three core values: free markets, limited government, and strong families. The App Store Accountability Act, which requires app stores to obtain parental consent and age verification for a minor to download an app, aligns with these values.

A [recent survey of Alabama voters](#), commissioned by API, found that 83% of voters, including 83% of parents, support requiring app stores to obtain parental approval for children and teens to download apps. We also found that broad support exists across voters from rural areas and small towns, as well as suburban and urban areas. And more than 6 in 10 said it would be easier for parents to provide approval in one place.

Legislation can never replace a parent's responsibility to protect their children, but it can give them the resources they need to ensure their little ones are safe from digital harm. This bill puts the responsibility on app stores to create an easy system for parents to supervise their children.



We understand that the Subcommittee on Commerce, Manufacturing, and Trade plans to hold a hearing on childhood digital safety on December 2, 2025. We commend your focus on this escalating crisis threatening our nation's youth and respectfully urge you to advance these critical protections without delay.

Parents must take the lead. Other initiatives seek to increase government involvement, but this bill takes the government out of the parent-child relationship. It is the only proposed solution that stays true to our commitment to limited government. Just as parents have a right to protect their kids from harmful content in school, they should have the same right to protect them from harmful content online.

Thank you for considering our concerns with the current state of childhood online safety. We trust that this Committee will recognize the promise this bill holds for protecting future generations of Americans.

Sincerely,

Stephanie Smith
Alabama Policy Institute President/CEO
stephanies@alabamapolicy.org
205-243-6088



Michael J. Murphy
Sheriff

Jason C. Pless
Undersheriff

LIVINGSTON COUNTY

OFFICE OF THE SHERIFF

150 S. HIGHLANDER WAY • HOWELL, MICHIGAN 48843
TELEPHONE (517) 546-2440 • FAX (517) 552-2542

Dear Members of the House Energy & Commerce Committee,

As the Sheriff of Livingston County, I am writing in strong support of the App Store Accountability Act (H.R. 3149). Our deputies – and those across the country – see a growing number of cases where criminal activity begins online. This legislation would give families a critical layer of protection to keep children safe.

Across Michigan, we are seeing an alarming increase in crimes that start online. Predators are using gaming platforms, chat features, and social apps that mask identity and allow direct access to children. The National Center for Missing & Exploited Children has reported a 300% increase in online enticement cases between 2021 and 2023. Last year, the Internet Crimes Against Children Task Force Program supported nearly 203,000 investigations and more than 12,600 arrests nationwide. These numbers reflect the reality that we see on the ground.

By the time these cases reach law enforcement, much of the harm has already occurred. While we work tirelessly to investigate these cases and make arrests, meaningful prevention must happen earlier – before a dangerous app ever reaches a child's device.

The App Store Accountability Act would help families do exactly that. By requiring app stores to verify a user's age, obtain parental approval before minors download apps or make in-app purchases, and apply accurate age ratings, the bill provides parents with a clear checkpoint that does not exist today. These safeguards understandably have broad public support—88% of parents agree that app stores should involve parents before giving minors access to apps.

This legislation offers a practical, commonsense way to reduce the risk to children and to support the work of law enforcement. I respectfully urge the committee to advance the App Store Accountability Act and help protect families in Livingston County and across the country.

Thank you for your commitment to public safety and to our nation's children.

Sincerely,

A handwritten signature in blue ink, reading "Michael J. Murphy".

Mike Murphy - Sheriff, Livingston County - Michigan

December 1, 2025

Chairman Brett Guthrie

House Energy and Commerce Committee
2125 Rayburn House Office Building
Washington, D.C. 20515

Ranking Member Frank Pallone

House Energy and Commerce Committee
2125 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Guthrie and Ranking Member Pallone,

As organizations that have supported the Kids Online Safety Act (KOSA) and represent parents, young people, researchers, and children's safety advocates, **we write to express our strong opposition to the federal AI preemption.** Recent reporting has indicated that the Committee is considering advancing kids' safety legislation with restrictive AI preemption that would nullify state laws designed to protect residents using AI products.

We believe deeply in the Committee's shared goal to protect young people online through regulation. For too long, the technology industry has maintained the majority of control over its products, distribution, and improvements despite extensive research that its products can be harmful, especially to children. The American people have relied upon industry to self-regulate in the face of overwhelming evidence that they cannot be trusted. Regulation is desperately needed to rein in social media and now AI companies that have addicted young people and kept them hooked on their products, exacerbating mental health conditions like anxiety, depression, and eating disorders.

Ensuring the United States remains at the forefront of AI is imperative, but this cannot happen without addressing the widespread risks of AI and the possible catastrophic risks of frontier AI models. One should not come at the cost of the other, nor does it need to. Safeguarding innovation and protecting the public requires strong, comprehensive federal legislation paired with effective state and local regulations that address any gaps in AI governance across sectors and use cases.

Two-thirds of states have already advanced AI legislation to address gaps in federal protections. Over the summer, 850 parents, 17 Republican Governors, 45 Attorneys General, 99 Senators, 230 state lawmakers, and 130 kids' safety organizations opposed the proposed moratorium on states' rights to regulate AI that was initially included in the reconciliation package. This near-universal consensus reflects an essential principle: states are closest to their constituents and must retain the authority to hold companies accountable when federal frameworks prove insufficient or are nonexistent.

States have a sovereign right—and constitutional responsibility—to protect their own residents, especially in areas where federal law offers no viable alternative. AI regulation requires ongoing, adaptive governance as the technology rapidly evolves, and states must retain the authority to respond swiftly as new harms emerge. While federal standards can provide important long-term guardrails, federal preemption would permanently constrain state legislatures' ability to address problems we cannot yet fully anticipate. Handing over this authority in exchange for a static federal policy would erode state sovereignty and leave communities without timely, locally responsive protections.

A strong KOSA and robust AI regulations must pass independently and without further delay.

The stakes are too high to accept a federal provision that undermines existing state protections.

Parents who have lost children to technology harms have fought for years to secure federal protections. Young people have shared their experiences with online harm to ensure that the next generation does not face the same fate. They all deserve federal action. However, their advocacy should not be weaponized to strip away the state authority they also need. We must have both: strong federal guardrails and the ability of their state to act when federal rules fall short. These objectives are complementary, not contradictory. Preemption transforms advocates' hard-won voice into a tool for industry, effectively telling these parents that we will pass the bill you fought for, but only if you accept that states can never do better. That is not an acceptable outcome.

Congress has two principled paths forward. The first is to strengthen federal standards by working through normal legislative processes, issue by issue, developing comprehensive AI protections that set a national floor. When federal protections are strong and comprehensive, preemption becomes a reasonable trade-off. The second is to maintain state authority by passing federal protections where federal action is most effective, while allowing states to remain laboratories of democracy on AI governance, as they have been in privacy, data security, and algorithmic accountability.

The Committee has expressed its commitment to child online safety, and maintaining state sovereignty over technology governance is critical to that. States, their attorneys general, bereaved parents, youth, and the American public all support maintaining state authority over AI, especially in the absence of well-thought-out federal regulations. We call on Congress to advance this consensus by passing strong federal protections while preserving state capacity to create guardrails tailored to their residents' needs.

Federal legislation should complement state efforts and fill genuine gaps, not eliminate the tools states need to fulfill their constitutional duty to protect their people. We look forward to working with the Committee to bring about a safer internet for America's youth.

Respectfully,

Design It For Us

Encode AI

Issue One

National Center on Sexual Exploitation

ParentsTogether Action

Young People's Alliance

November 24, 2025

Speaker Mike Johnson
United States House of Representatives
568 Cannon House Office Building
Washington, D.C. 20515

Chairman Brett Guthrie
House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

Minority Leader Hakeem Jeffries
United States House of Representatives
2433 Rayburn House Office Building
Washington, D.C. 20515

Ranking Member Frank Pallone
House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

Dear Speaker Johnson, Minority Leader Jeffries, Chairman Guthrie, and Ranking Member Pallone:

We are parents of children and teens who were hurt or died because many social media platforms and products are designed to addict, exploit, and abuse America's young people. Our kids died from suicide, fentanyl poisoning, dangerous challenges, overdoses, and are victims and survivors of severe mental health harms, sexual exploitation, and self-harm. **As parents who have had kids hurt or die because tech companies continue to prioritize profit over our children's lives, we write to urge you, as leaders of the U.S House of Representatives and the Committee on Energy and Commerce, to pass strong kids online safety and privacy legislation, including the [Kids Online Safety Act \(KOSA\)](#).**

America's kids are needlessly suffering because tech companies feel no duty to kids or families to design their products and platforms in ways that don't cause tragic, irreversible harm. Social media has caused a 156% increase in suicide among 12-16-year-olds, a 350% increase in opioid deaths in minors, a 40% increase in hospital admissions for mental health harms, and skyrocketing rates of anxiety and depression. The lifelong consequences of the harms we've experienced do not discriminate based on how we vote, which state we live in, or which political party we belong to. **This is a bipartisan problem for which there can be a meaningful, bipartisan solution.**

KOSA passed the Senate last year by a vote of 91-3 because it contained tangible, critical protections for our kids including a meaningful duty of care, transparency requirements, protections for stronger state laws, and protections for the rights of parents to file cases against the tech companies in connection with design-based harms. There have been numerous bipartisan bills introduced, many of which have been enacted at the state level. State attorneys general and governors from both sides of the aisle are acting right now to try and protect our kids from tech company abuses. In Congress there have been numerous bipartisan statements and hearings during which members of Congress, on a bipartisan basis, call for Congress to act, yet children continue to needlessly suffer and die while

waiting for the desperately needed protections that KOSA and other legislation would provide.

We urge you to stand strongly against the demands of the tech industry to gut KOSA and other children's online privacy and safety legislation of their most fundamental requirements and protections. Tech companies know they cannot ignore the public outcry from parents in every state any longer, but these same companies also continue to quietly urge Congress to *look like* it is doing something while asking policymakers to strip the key requirements and protections from KOSA as well as other legislation.

Unless and until tech companies are legally required to put children's safety ahead of their bottom lines, kids will pay the price. We beg you to oppose any efforts to gut KOSA and other legislation of its power to actually prevent harm. This includes maintaining strong duties of care that will protect kids from addiction, self-harm, drug sales, substance abuse, suicidality, and sexual violence and exploitation, allowing public transparency into the safety of platforms and products that are marketed and used by kids and teens, protecting state efforts to take further action to protect our kids, and maintaining protections for state laws that empower parents to hold tech companies legally accountable.

The version of KOSA that passed the Senate has been endorsed by more than 250 national, state, and local organizations; grieving families like ours who have had kids hurt or die; by doctors and mental health professionals, child safety advocates, technology companies committed to responsible innovation, educational organizations, and law enforcement officials. Yet as Congress continues to get bogged down in political divisions and tech's manipulation campaign, more children have suffered and died. These are children who Congress could have saved.

The legislative framework of KOSA is sound, the support is overwhelming, and the need is urgent. **We call upon you to pass KOSA and other kids' online safety and privacy legislation that doesn't just look good on the surface, but that is *actually effective* in protecting kids and teens from the immeasurable harm we've experienced.** As parents of kids who have died or been severely injured, we stand ready to support you in standing up to tech companies and saving America's kids.

Sincerely,

Amy, parent of Alexander, 14, San Tan Valley, Arizona
Jennie, parent of Mason, 16, Bentonville, Arkansas
Aaron, parent of Avery, Forever 16, Olympia, Washington
Adrian, parent of Dezhanaya, Boston, Massachusetts
Adriane, parent of Harper, 14, Pompano Beach, Florida
ÀkiA

Alannah, parent of Merlin, Michigan
Alicia, Nevada
Amanda, Arizona
Amanda, parent of Owen, 17, Warwick/East Greenwich, Rhode Island
Amy, parent of Julia “Frog”, 18, Newburgh, Maine
Andrea, parent of Ashley, Grand Junction, Colorado
Andrea, parent of Tyler, 19, Sandown, New Hampshire
Andrea, parent of Zachary, Forever 21, Norwood, Massachusetts
Angela, parent of Jakob, 19, Lincoln Park, Michigan
Angelicia, parent of Giovanni, 11, Syracuse, New York
Annetta, parent of Amelia, 15, California
Annie, parent of Griffin (“Bubba”), 13, Madison, Wisconsin
April, California
April, parent of Melissa, 17, Billings, Montana
AR, Vermont
Archila, parent of Breely, 12, Texas
Ashley, parent of Jaleah, 17, Rockville Centre, New York
Ashley, parent of Kristopher, 13, Brooksville, Florida
Ashley, parent of Madison, 16, Forest, Virginia
Austin, parent of Michelle, South Dakota
Benelisa, parent of Jules, 14, Chicago, Illinois
Bichloan, Nevada
Blair, parent of Brantley, Forever 17, Jonesboro, Louisiana
Brad, parent of Evan, 16, Aurora, Missouri
Brandi, parent of Paige, 15, Onaway, Michigan
Brandi, parent of Tahrique, 11, Gowen, Michigan
Brandy, parent of Englyn, 14, New Iberia, Louisiana
Brandy, parent of Shayne, 19, Judsonia, Arkansas
Brett, parent of Riley, 23, Butler, Alabama
Bridgette, parent of Devin, 19, Hastings, Minnesota
Brittney, parent of Dexon, 14, Joseph, Utah
Brittney, parent of Makayla, 20, Ashland, Oregon
C., New York
Candace, Tustin, California
Carl, parent of Harry, 17, Canada
Carla, Oklahoma

Carol, Browns Summit, North Carolina
Carol, parent of Amanda, Forever 15
Carri, parent of Hayley, 15, North Carolina
Carri, parent of Kaitlyn and Hayley, 19 and 15, Statesville, North Carolina
Carrie, parent of Jack, Forever 18, Green Bay, Wisconsin
Carrie, parent of Joshua, 17, Woodbine, Georgia
Casey, parent of Emma, 12, Fresno, California
Cassius, parent of Kyleigh, 17, Oakley
Charay, parent of London, Forever 12, Ovid, Michigan
Charlotte, Houston, Texas
Charmelle, Owosso, Michigan
Chasity, parent of Amari, 14, Monroe, Wisconsin
Chelsea, parent of Peyton, 17, Florida
Cheryl, parent of McKenna, 16, Tampa Bay, Florida
Chris, parent of Kayleigh, 19, Chester, Illinois
Christina, parent of Jacob, 22, Kentucky
Christina, Pennsylvania
Christina, Washington
Christine, parent of Alexandra, 20, Temecula, California
Christine, parent of Grace, Forever 15, Maryland
Christopher William, parent of Luis "Monk", 17, Tucson, Arizona
Cindy, parent of Dylan, 18, Los Angeles, California
Colleen, Encinitas, California
Connie, Chester, South Carolina
Courtney, Illinois
CP
Cynthia, parent of Juliana, 13, Thornton, Colorado
Cynthia, parent of Kyra, 16, New York
Cynthia, parent of Mollie, 17, Birmingham, Alabama
D., Georgia
Dale, parent of Albert, 21, New York
Damian, parent of Kamari, Peoria, Illinois
Damon, parent of Parker, 14, Jasper, Alabama
Dani, parent of Alex, Forever 18, Lynnwood, Washington
Dannishia, parent of Chrishawn, 17, Portland, Oregon
Daphne, parent of Destiny, 13, Lithonia, Georgia

Darcy, parent of Jordan, 27, Colorado
Darren, parent of Riley, 15, Potsdam, New York
Dave, parent of Mason, 16, Centerton, Arkansas
Deanna, parent of Reyna Luna, 13, Rowland Heights, California
Debbie, grandparent of Elijah, 12, Gainesville, Georgia
Devon, parent of Anne Taylor, 14, Easton, Maryland
Deysi, parent of Diego, 18, Los Angeles, California
Diana, parent of Juan, 16, Fort Myers, Florida
Diane, parent of Martina, 14, Bainbridge Island, Washington
Dianne, parent of Mallory, 12, Rockaway, New Jersey
Donald, parent of Keziah, Arizona
Dondée, parent of Jedda, 17, Rome, Georgia
Donna, parent of CJ, 17, Salem, Wisconsin
Edwin, parent of Dazire, 18, Otego, New York
Eleni, Colorado
Elle, Mercer Island, Washington
Ellen, parent of Jools, 14
Emily, Hustonville, Kentucky
Emily, parent of Christian, 15, California
Emily, parent of Quincy, 11, Kirkland, Washington
Erin, parent of Emily, 17, Kendall Park, New Jersey
Fran, parent of Sophia, 20, Washington
Frances, parent of Rey, 16, Glendale, Arizona
Frank, parent of Marcello, 16, Leominster, Massachusetts
G A, California
Georgia, parent of Jared, 19, Aberdeen, Washington
Georgina, parent of Berlin, 15, Hagerstown, Maryland
Gregorio, parent of Brantley, Forever 17, Jonesboro, Louisiana
Greta, parent of Leasia and Marlic, Marion, Mississippi
Heriberto, parent of Arriani, 9
Hillary, parent of Jaeleigh, 13, Plaquemine, Louisiana
Isa, Staten Island, New York
Jackie, parent of Angela, 17, Morristown, Tennessee
Jacob
Jacqueline, parent of Braidon, 13, Crossville, Tennessee
Jaime, parent of Daniel, 16, Santa Clarita, California

Jajaira, N., New Hampshire
James, parent of Harper, 14, Pompano Beach, Florida
James, parent of Jayson Patrick, 21, Wamego, Kansas
Jane, New Jersey
Janeen, parent of Michael, 21, DeForest, Wisconsin
Jason, parent of London, 12, Ovid, Michigan
Jason, parent of Penelope, 15, Vancouver, British Columbia, Canada
Jennifer, Michigan
Jennifer, parent of Braden, Forever 15, Ohio
Jennifer, parent of Brady, Forever 21
Jennifer, parent of Ian, Forever 16, New Port Richey, Florida
Jennifer, parent of Jayson Patrick, 21, Wamego, Kansas
Jennifer, parent of Jessica, Florida
Jennifer, parent of Julia, Portland, Oregon
Jennifer, parent of Kevin, 20 (would be 23), Silver Spring, Maryland
Jennifer, parent of Michael, Forever 15, Cda, Idaho
Jeremy, El Cajon, California
Jerry, parent of Alexis and Jerry, 15 and 14, Dallas, Texas
Jess, parent of Nayelie, 16, Los Angeles, California
Jess, parent of Zaye, 11.5, New Mexico
Jessica, parent of Jacob, 15, Waynesboro, Virginia
JG, Cleveland, Ohio
Joann, parent of Mason, Forever 15, Wadesville, Indiana
Jodi, parent of Harper and Hayla, 12 and 10, Florida
John, parent of Jordan, 17, Marquette, Michigan
John, parent of Jordyn, 13, Menomonee Falls, Wisconsin
Joseph, parent of Emily, 17, Kendall Park, New Jersey
Joshua, parent of LJ, 18, Texas
Joy, parent of Jocelyn, 15, California
Joyce
Judy, parent of Erik, 12, Los Angeles, California
Julianne, Nevada
Julie, parent of Faith, 20, Florence, Kentucky
Kamille, parent of Timjay, 18, Chicago Heights, Illinois
Karl, parent of Dexon, 14, Richfield, Utah
Katherine, parent of Jack, 17, Baltimore, Maryland

Katherine, parent of Saniah, 16, Cedar Rapids, Iowa
Kathryn, parent of Chantel, Indiana
Kathryn, parent of Kennedy, 12, La Vernia, Texas
Kathy, Anthony, Yonkers
Kathy, parent of Sequoyah, Forever 16, Los Angeles, California
Kaydence, Greers Ferry, Arkansas
Kelley, parent of Christian, 11, Florida
Keri, parent of Liam, 20, Austin, Texas
Kerrainn
Kerri, parent of Gillian, 19
Khristen, parent of Cashmere, 18, North Carolina
Khurshidakhon, parent of Naeema, 17, Los Angeles, California
Kimberly, parent of August, 16, Palmdale, California
Kimberly, parent of Max, Forever 18, Thornton, Colorado
Kimberly, parent of Skyler, 18, East Greenbush, New York
Kimika, parent of Rihanna and Gihanna, 18 and 18, Denver, Colorado
Krislynn, parent of Chandler, Forever 18, Austin, Texas
Krista, parent of Paris, 13, Athens, Georgia
Kristen, parent of Bethany, 24, Denver, Colorado
Kristi, Michigan
Kristin, parent of Carson, Forever 16, Mesa, Arizona
Kristin, parent of Charla, Buffalo, Missouri
Kristina, parent of Morgan Danielle, Forever 15, Wisconsin
Kyle, Colorado
Lacie, parent of Mira Oscar, 15, Forestcity, Illinois
Latasha, parent of William, 15, Des Moines, Iowa
Lateresa, parent of Pharaoh, 10, Pontiac, Michigan
Latina, parent of Tamir, Newark, New Jersey
LaToya, parent of Amiah, 14, Decatur, Georgia
Laura, parent of Brillion, 18, Bellevue, Washington
Lauren, parent of Brooke, 14, Franklin Lakes, New Jersey
Lauri, parent of Bradley, 20, Santa Cruz, California
Leasia, parent of Armani, Mississippi
Leon, parent of Leon Jr, 16, Allen, Texas
Leona, parent of Leilani, 14, Denver, Colorado
Liam, parent of Maia, 13, Basildon Essex, UK

Lisa, parent of Fernando, 17, Gilroy, California
Lisa, parent of Isaac, 13, United Kingdom
Lisa, parent of Mia, 17, Virginia Beach, Virginia
Lori, parent of Annalee, 18, Merino, Colorado
Lucinez, parent of Jacob, 11, Brooklyn, New York
Luke, Kronenwetter, Wisconsin
Mahsa, parent of Finale, 18, Scottsdale, Arizona
Maidel, parent of Isabella, 17, Miami, Florida
Malsabel, parent of Alan, 17, Merced, California
Mandy, parent of Ashton, 10, Marysville, California
Maria, California
Maria, parent of Albert, 9, Miami, Florida
Maria, parent of Anastasia, 20, San Diego, California
Maria, parent of Audrey, 18, California City
Maria, parent of Ricardo, 13, Buena Park, California
Marie, parent of Liz and Lilly, 13 and 9, Portland, Oregon
Marni, parent of Lexi, 17, Pleasant Grove, Utah
Martika, parent of , 9, Maryland
Mary, parent of Hannah, 11, Maine
Mary, parent of Riley, Forever 15, Canton, New York
Maureen, parent of Cedric, Forever 20, California
Maya, parent of Charles, 21, Florida
Meg, Las Vegas, Nevada
Megan, parent of Sewell, 14, Orlando, Florida
Melissa Grace, parent of Chevy Andre, Jourdyn, and Jericho, would have been 17, 17, and 4, Norco, California
Melissa, parent of Hunter, 15, Leavenworth, Kansas
Melissa, parent of Savannah, 17, Lawrence, Indiana
Melissa, parent of Trinity, Kansas City, Missouri
Melissa, Perry, Michigan
Michael, parent of Kevin, Forever 20, Rockville, Maryland
Michelle, parent of Jack Paul, Forever 16, Fort Atkinson, Wisconsin
Mirna, parent of Matthew, 10, Fremont, California
Misty, parent of Kaylie, 17, San Tan Valley, Arizona
Monica, parent of Aunnica, 19, San Diego, California
Myra, 15, Baton Rouge, Louisiana

Naika, Massachusetts
Nayeli, parent of Aliney, 16, Nipomo, California
Nicole, parent of Aaleyah, 16, Bronx, New York
Nicole, parent of Olivia, 20, Laingsburg, Michigan
Nina, Ovid, Michigan
Oscar, parent of Emily, 17, New Brunswick, New Jersey
Patti, parent of Lauren, 18, Colorado
Paul, parent of Kaelyn, Middletown, Rhode Island
Paula, New York
Pauline, parent of Ryan, 17, Corvallis, Oregon
Piedad, parent of a 15-year-old, Alcalde, New Mexico
Porshea
Quintasha, parent of Zoey, Zamora, and Zamir, 11, 7, and 5, Savannah, Georgia
Rachel, Michigan
Rachel, parent of Gabriel, 21, Chariton, Iowa
Ramel, parent of Jordan, 27, Colorado Springs, Colorado
Raymond, Owosso, Michigan
Regina, parent of Jewels, 15, Roseville, California
Renea, parent of Madison, 20, Harrison, Ohio
Renee, Michigan
Renee, parent of Bryan Richard, 15, New Jersey
Rima, parent of Anya, 18, Montpelier, Vermont
Robert, parent of Kaysha, 25, Cartersville, Georgia
Robin, parent of Lauren, Pennsylvania
Roe, parent of Sal Jr, 28, Lodi, New Jersey
Roger, parent of Chloe, 16, New Rockford, North Dakota
Ronald, parent of Aalways, San Pablo, California
Rosanna, parent of Brielle, 15, Staten Island, New York
Roxanne, parent of Evelyn, 16, Iowa
Rubyie, parent of Eugene, Rasberry, Kemonee, and Jonay, Lancaster, California
Ryan, parent of Alyvia, 14, Missouri
Samantha, Carterville, Illinois
Samantha, parent of Evelyn, 13, Parker, Colorado
Sandra, parent of JL, 17, Los Angeles, California
Sandra, parent of Leona, 16, Federal Way, Washington
Sara, parent of Sierra, 16, California

Sarah, parent of Braylin, Georgia
Sarah, parent of Eleanor, 15
Sarah, parent of Ezekiel, Kansas City, Missouri
Sewell Jr, parent of Sewell III, 14, Orlando, Florida
Shannon, Douglas, Arizona
Shannon, Owosso, Michigan
Shannon, parent of Luis, 17, Tucson, Arizona
Shaun, parent of Dade, Collierville, Tennessee
Shauna, parent of Mia, 17, Memphis, Tennessee
Shawane, parent of Leon Jr, 16, Allen, Texas
Shelly, parent of Noah, 24, Harrisburg, Pennsylvania
Sheree, parent of Zikeya, Zimair, and Zair, 18, 17, and 17, Philadelphia, Pennsylvania
Sherry, parent of Geneva, 20, Alabama
Shirley, parent of Ryan, 15, New Windsor, New York
SS, New Jersey
Stacey, parent of Paris, 15, Opalocka, Florida
Staycie, parent of Lyra, 14, Mission Viejo, California
Stephanie, Utah
Suelema, parent of Amir, 11, South Carolina
Sumer, parent of Karma, 17, Ohio
Susan, parent of Carilyn, 19, Mountain View, California
Suzanne, 14, Spokane Valley, Washington
Ta, parent of Tanner, 19, Olympia, Washington
Tabitha, parent of Ilileana, 16, Schertz, Texas
Tammy, parent of Haley, 17, Brodhead, Kentucky
Tammy, parent of Selena, 11, Enfield, Connecticut
Tanisha, parent of Jakeira, 16, Los Angeles, California
Tanya, parent of Emilio, 15, Mattoon, Illinois
Taren, parent of Selah and Akila, Rancho Cucamonga, California
TD, Lubbock, Texas
Tiffany
Tina, parent of Megan, 13, St. Charles, Missouri
Todd, parent of Matthew, 12, Accokeel, Maryland
TONEY, parent of Englyn, 14, New Iberia, Louisiana
Tonya, Laingsbury, Michigan
Tricia, parent of Levi, Forever 13, Pennsylvania

Valena, parent of Larah, 15, San Tan Valley, Arizona

Valerie, Georgia

Valerie, Murrieta, California

Vanessa, parent of Dazire, 18, New York

Victoria, parent of Ava, 15, New York

Virginia

Wendy, parent of Tyler, 16, Glenpool, Oklahoma

William, parent of Juliana, 13, Thornton, Colorado

Yolanda, parent of Smith, 17, Little Rock, Arkansas

Yvonne Sherie, parent of Don'Nae, 14, Portland, Oregon

Yvonne, parent of Serenity, 15, Norman, Oklahoma

Zachary, Tucson, Arizona

Zelda, parent of Ben, 13, Morrice, Michigan

OPPOSE House KOSA & COPPA 2.0

Bills Eviscerate the Rights of Parents to Seek Justice & Accountability

Big Tech and social media companies' predatory products and targeting practices are fueling a mental health and safety crisis with America's kids and teens. Legislation is needed to protect kids' safety and privacy online; critical to this legislation is language protecting state laws as well as the rights parents have under those laws allowing them to hold tech companies accountable when tech companies profit from the abuse and harm of children. **Tech's push for sweeping preemption should be seen for what it is: total immunity for hurting kids.**

Unfortunately, both House KOSA and COPPA, as introduced in the 119th Congress, include the following express preemption provisions which eviscerate more protective and consistent state laws as well as parents' rights to file cases in court for the deaths and harm of their kids:

- House KOSA, Page 26, line 23: SEC. 10. RELATIONSHIP TO STATE LAWS. No State or political subdivision of a State may prescribe, maintain, or enforce any law, rule, regulation, requirement, standard, or other provision having the force and effect of law, if such law, rule, regulation, requirement, standard, or other provision relates to the provisions of this Act.
- House COPPA 2.0, Page 35, line 20: (d) PREEMPTION.—No State, or political subdivision of a State, may maintain, enforce, prescribe, or continue in effect any law, rule, regulation, requirement, standard, or other provision having the force and effect of law that relates to the provisions of this Act. ''
- *The following additional bills have the same or very similar preemption language as above and therefore must also be opposed:
 - H.R. _____, Reducing Exploitative Social Media Exposure for Teens (RESET) Act
 - H.R. 3149, App Store Accountability Act
 - H.R. 6265, Safer Guarding of Adolescents from Malicious Interactions on Network Games (GAMING) Act
 - H.R. 6273, Stop Profiling Youth and (SPY) Kids Act
 - H.R. 6257, Safe Messaging for Kids Act
 - H.R. _____, Parents Over Platforms Act
 - H.R. 6253, Algorithmic Choice and Transparency Act
 - H.R. _____, Safeguarding Adolescents from Exploitative (SAFE) Bots Act

Cases of kids who were killed by fentanyl poisoning, sexually exploited or assaulted, targeted by manipulative practices, or driven to commit severe self-harm or suicide are worthy of being heard in a court of law. Congress shouldn't bow to the complaints of billion-dollar tech companies that have for decades profited off targeting America's kids and now don't want to answer for the harm they've caused.

Tech companies' number one priority is to shut down the cases filed by parents for three reasons:

- 1) Discovery: The most powerful mechanism a civil lawsuit holds is the discovery process—a mechanism by which a court makes a company turn over key internal company information about whether, how, and why they chose profits over the safety of kids. Preempting the rights of families to file cases against Tech keeps this critical information hidden.
- 2) FTC Fines are a Drop in the Bucket for Global Tech Giants: Tech companies consider a Federal Trade Commission (FTC) fine as the cost of doing business, especially when government agencies are understaffed, under resourced, and subject to the political whims of the White House; this leaves parents seeking direct accountability as the only potent driver of accountability and change.
- 3) Tech Companies Would Have to Follow the Law: Because tech companies can use their wealth, power, and market dominance to try and control government agencies and those in power, civil cases filed directly by parents are the primary incentive for tech companies to follow kids' privacy and safety laws.

KOSPA, KOSA, COPPA 2.0 & Preemption

In the 118th Congress, S. 2073, the Kids Online Safety and Privacy Act (“KOSPA”) (passed by the Senate with 91 votes), the House-introduced versions of the Kids Online Safety Act *in the 118th Congress* (“KOSA”), and the Children’s Online Privacy Protection Act (“COPPA 2.0”) each *already contain a preemption provision*. With the inclusion of the broader, more sweeping preemption provisions referenced above in House KOSA and COPPA, existing rights will be stripped away from families and the work of state legislatures to grant kids and parents additional rights than those contained in the federal bills will be wiped out. Without preserving rights under state law, parents are left at the mercy of overburdened and under resourced government agencies.

In the 118th Congress, KOSPA, as well as House-introduced KOSA and COPPA 2.0, contained language which will have the effect of preempting state laws that conflict with the requirements of the federal proposals, eliminating any possibility that tech companies will have to comply with contradictory state and federal requirements. This preemption provision only preserves state laws that are not in conflict with the federal law and that give parents a chance to seek justice in court pursuant to their rights under those state laws.

In the 119th Congress, Tech is now, unsurprisingly, working with House Republican leadership to enact sweeping preemption language, and for good reason—tech knows that under broad preemption, they will *never* be held legally accountable for the massive abuse perpetrated against America’s kids on their platforms. Big Tech is clinging to sweeping preemption language to shut down the most effective method for holding it to account—parents’ cases.

Kids Social Media Cases

In 2022, hundreds of parents, school districts, cities, and states took legal action against Meta Platforms, Instagram, Snap, TikTok, ByteDance, YouTube, Google, and Alphabet. [In re: Social Media Adolescent Addiction/Personal Injury Products Liability Litigation \(MDL No. 3047\)](#) is a ground-breaking Multi-District Litigation (“MDL”) comprised of cases from all over the country and includes families whose children have been seriously injured or killed due to social media. The parents’ cases allege that the defendant companies failed to take reasonable steps to protect kids online because their platforms and the algorithmic designs used by those platforms are defective because they are purposely designed in ways that result in serious harm including addiction, sexual exploitation, self-destructive behavior, depression, eating disorders, self-harm, and suicide.

Despite the social media companies’ attempt to get these cases dismissed, in November 2023, a federal judge denied them and allowed many of the parents’, school districts, and cities’ claims to move forward. Speaking on behalf of all the tech companies during the hearing in 2023, TikTok attorney Geoffrey Drake [argued](#) that the companies had no duty to design a platform in a safe way.

Revelations Recently Unsealed in the Kids Social Media MDL Through the Discovery Process

On November 21st, 2025, several documents in the Kids Social Media MDL were unsealed and the revelations are stunning. Those include:

- Meta was well aware of the addictive nature of its products, highlighted by employees who wrote, “IG is a drug,” and, “LOL, I mean, all social media. We’re basically pushers.” (Source [here](#).)
- According to a reported quote from one Meta executive, CEO Mark Zuckerberg suggested that “teen time spent be our top goal of 2017.” (Source [here](#).)
- Meta was aware that “optimizing its products to increase teen engagement resulted in serving them more harmful content but did so anyway.” (Source [here](#).)
- Meta’s internal documents stated that “people who stopped using Facebook for a week reported lower feelings of depression, anxiety, loneliness and social comparison.” (Source [here](#).)
- After Meta suppressed its internal findings of the harms caused by its products, an employee reportedly compared Meta to tobacco companies for “doing research and knowing cigs were bad and then keeping that info to themselves.” (Source [here](#).)
- One Meta employee was reportedly surprised to find that “[y]ou could incur 16 violations for prostitution and sexual solicitation, and upon the 17th violation, your account would be suspended.” (Source [here](#).)

- A Meta internal review concluded, according to these documents, that beauty filters exacerbated the “risk and maintenance of several mental health concerns, including body dissatisfaction, eating disorders, and body dysmorphic disorder,” and that Meta knew that “children are particularly vulnerable.” While Meta prohibited beauty filters in 2019, the company later reversed course and released them the following year after realizing that banning beauty filters would have a “negative growth impact.” (Source [here](#).)
- Internal documents from TikTok indicated the app’s safety features for kids under age 14 were weaker than those provided on the app’s Chinese equivalent, according to one expert opinion – which included review of sealed evidence – that was included in the filing. According to reports, the document is quoted as reading in the expert opinion, “We give spinach to kids in China and opium to kids in America.” (Source [here](#).)
- In 2017, employees at Snap emailed about daily users of their app, which counts how many days in a row friends communicate using a “Snapstreak”, saying, “Yeah we seem to have tapped into some mass psychosis where 17 million people must keep the streaks going,” to which another employee wrote in response, “I’m glad what we are making will make it even more fun to streak.” (Source [here](#).)
- Meta used location data to send out notifications to students in “school blasts” during the school day, according to one filing, and as one employee allegedly said, “[o]ne of the things we need to optimize for is sneaking a look at your phone under your desk in the middle of Chemistry :).” (Source [here](#).)
- Meta allegedly “stalled internal efforts to prevent child predators from contacting minors for years due to growth concerns, and pressured safety staff to circulate arguments justifying its decision not to act.” (Source [here](#).)

State Law is Critical

Legal accountability incentivizes Big Tech to follow the law, and state laws are the *only method* by which parents are empowered to enforce policies meant for their kids’ protection. Big Tech treats FTC fines as the cost of doing business. In 2019, Google agreed to pay \$170 million to resolve COPPA violations in a settlement with the FTC and New York’s attorney general. But by 2020, Google was violating COPPA again, this time gathering data from children using their educational tools and using it to serve children targeted ads.¹

In contrast, consider when Facebook was sued under the Illinois Biometric Information Privacy Act (“BIPA”). After unsuccessfully fighting to get out of the lawsuit, Facebook settled for \$650 million *and* agreed to disable the “Facial Recognition” setting, *by default*, until being granted consent to run a biometric scan. Illinois citizens—children and adults alike—who were members of the class were paid approximately \$345 each, saw their biometric information purged by Facebook, *and* forced the platform to alter their business practices going forward.² Just like tobacco, e-cigarettes, opioids, and countless other atrocities—change only comes when lawsuits hold industry accountable.

Facebook did not want to reform its biometric policies—violating privacy rights and selling or utilizing that data is a central component of Big Tech’s business model. If they must face privacy lawsuits, they would prefer to restrict potential litigants to the FTC and state attorneys general, over whom they have a great amount of influence, rather than face the parents whose rights they violated or whose children they hurt. **This is why Tech insists on preemption as the price for regulation—they know that cases filed by parents drive change and are the only system over which Tech can’t wield undue influence. Congress should reject Tech’s call for sweeping preemption and instead prioritize the safety of kids online.**

¹ See First Am. Class Action Compl. In *H.K. through Farwell v. Google LLC*.
<https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=3189&context=historical>.

² *In re Facebook Biometric Info. Privacy Litig.*, No. 3:15-cv-03747-JD (N.D. Cal.).



December 1, 2025

The Honorable Gus Bilirakis, Chairman
House Subcommittee on Commerce, Manufacturing, and Trade
2306 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Jan Schakowsky, Ranking Member
House Subcommittee on Commerce, Manufacturing, and Trade
2408 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Bilirakis and Ranking Member Schakowsky:

At Apple, we want users of all ages to have the best possible experience with our technology. That's why we design all of our products, features, and services to protect the safety and privacy of our users — especially when it comes to kids and teens.

We believe we all have a role to play in keeping kids safe online, and at Apple, we're continuing to empower parents with innovative resources and tools that help keep children safe while also protecting their privacy. We appreciate your committee's interest and leadership on this important issue, and we welcome this opportunity to share our perspective and learnings as you consider federal legislation to strengthen protections for children online.

Apple's Tools For Parents

For many years, Apple has built safety and privacy into the core of our operating systems, creating a trusted ecosystem for our users. We also build them into our guidelines for developers on the App Store, which we rigorously enforce. This focus is not an afterthought; it is our starting point — and we are constantly innovating to empower parents and protect children's experience on our devices.

That includes the easy-to-use tools we've built to help parents protect kids and teens online, empowering them with the information and controls to make the right decisions for their families. Tools like Screen Time and Ask to Buy allow parents to manage how their children use their devices and approve — or decline — any app download. Parents can also use Communication Limits to limit who can start a conversation with their kids, and Content Restrictions to ensure that children only access age-appropriate apps, websites, and media. And with Communication Safety — which is on by default for all users under 18 with our latest software — we've pioneered a system that uses on-device intelligence to protect children from viewing or sharing photos or videos that contain nudity via Messages or AirDrop, without Apple ever seeing the photos. This technology is a prime example of our approach: providing powerful protection while rigorously preserving user privacy.



We are constantly innovating to build on this foundation. This year, as detailed in our White Paper, [Helping Protect Kids Online](#), we expanded these protections to help shield children from sensitive content in FaceTime in real time, and we created tools for developers to integrate this new capability into their apps as well. In September, we also released a new age assurance tool that further empowers parents and helps developers provide age-appropriate experiences. This privacy-preserving solution allows a parent to share their child's age range with an app developer, without having to share sensitive, specific information like a birthdate or government ID. We're constantly innovating to expand our protections for parents and developers, and over time, we've enabled more of our safety features by default to strengthen safety protections from the moment our users first access their Apple devices.

Beyond the software tools and features we offer, we enforce rigorous safety guidelines across our entire digital ecosystem. On the App Store, we have long enforced strict rules that require apps to protect children from inappropriate content, safeguard their data, and prohibit tracking children for advertising purposes or sharing children's data with data brokers. Should a developer be found to be in breach of these guidelines, we take immediate action to ensure they either come into compliance or face removal from our platform.

Online Safety, Privacy and Public Policy

While both platforms and developers have important roles to play in keeping kids safe online, there is also a critical role for thoughtful public policy. We welcome legislative efforts that aim to strengthen protections for kids, and we have been an engaged partner in these discussions.

This year, for instance, Apple endorsed S. 1748, the Kids Online Safety Act (KOSA), and we look forward to engaging with your committee as it considers companion legislation. We appreciate that KOSA emphasizes holding platforms accountable for the design of their services and equipping parents with robust tools — while also protecting and prioritizing their privacy. This legislation recognizes that accountability and empowerment are safer for families than mandating the collection of additional personal data, especially about children.

Unfortunately, not all legislative proposals are equally protective of privacy or focused on holding all players in the ecosystem accountable. Some well-intended proposals for age verification at the app marketplace level, for example, would require the collection of sensitive information about anyone who wants to download an app, even if it's an app that simply provides weather updates or sports scores. Consistent with principles of data minimization — collecting and using only the minimum amount of data required to deliver a service — Apple does not do this.

We share the goal of strengthening kids' online safety, but we are very concerned that such legislation could threaten the privacy of all users by forcing millions of adults to



surrender their private information for the simple act of downloading an app. There are better proposals that help keep kids safe without requiring millions of people to turn over their personal information. Apple's age assurance feature is one such example of a more achievable, privacy-focused path forward.

We recommend that any proposal to mandate app marketplace- or device-level age assurance should, at a minimum:

- Recognize that both app marketplaces and developers have a shared responsibility to keep children safe online; for instance, by ensuring that developers who already possess specific information about a user's age cannot disregard such knowledge.
- Clarify that compliance does not require the collection of sensitive information about children, like birth certificates or social security numbers.
- Entrust parents to provide the age of their child when establishing a child's account.
- Focus age assurance efforts on ensuring that parents who establish an account for their child are adults.
- Clarify that any personal information utilized to determine age need not be retained by app marketplaces or developers.
- Empower parents to decide whether the age range of their children is shared with developers.

By adhering to these principles, we can both protect children from online harms and protect their privacy as well. We can also mitigate the risks of scams and fraud that could result from children's personal information being collected, retained, or shared unnecessarily.

In sum, we believe everyone has a role to play and are committed to doing our part. We will continue to ensure families using our devices have intuitive tools to guide their children's digital experiences—and protect their privacy along the way. Other platforms and developers should also design their products with safety at the forefront.

By working together, we can build a digital future that is not only innovative and open but also safe and trusted for generations to come. We look forward to continuing to work with the committee on legislative proposals intended to keep children safe online.

Thank you,

A handwritten signature in black ink, appearing to be 'Hilary Ware', is located below the 'Thank you,' text.

Hilary Ware
Global Head of Privacy
Apple



CC: Members of the US House Of Representatives Committee on Energy and Commerce

CALIFORNIA PRIVACY PROTECTION AGENCY

400 R ST. SUITE 350
SACRAMENTO, CA 95811
cppa.ca.gov



December 1, 2025

The Honorable Brett Guthrie, Chair
The Honorable Frank Pallone, Ranking Member
The Honorable Gus Bilirakis, Subcommittee Chair
The Honorable Jan Schakowsky, Subcommittee Ranking Member
House Committee on Energy and Commerce
2125 Rayburn House Building
Washington, DC 20515

Re: HR 6291, The Children’s Online Privacy Protection Act (2025)

Dear Chair Guthrie, Ranking Member Pallone, Subcommittee Chair Bilirakis, and Subcommittee Ranking Member Schakowsky,

The California Privacy Protection Agency (CalPrivacy or Privacy Agency)¹ writes in respectful opposition to the preemption language to HR 6291, The Children’s Online Privacy Protection Act (HR 6291 or COPPA 2.0).² CalPrivacy appreciates the House Energy and Commerce Committee (Committee) and its Subcommittee on Commerce, Manufacturing, and Trade for considering legislation regarding children and teens online. New federal privacy protections, however, should not come at the expense of protections that children enjoy. The current version of COPPA 2.0 includes preemption language that could eliminate key privacy protections that minors have under California law, leaving this vulnerable group less protected.³ States play a crucial role in protecting children, and we urge the Committee to amend COPPA 2.0 to truly protect children’s privacy by setting a floor, not a ceiling on those rights.

Background

For years, California has played a leading role in developing strong privacy protections. In 1972, California voters established the right of privacy in the California Constitution, amending it to include privacy as one of Californians’ “inalienable” rights.⁴ California passed the first data breach notification law in 2002 and was the first state to require businesses to post privacy policies outlining their data use practices.⁵ In 2018, it became the first state in the nation to adopt

¹ Established by California voters in 2020, the California Privacy Protection Agency was created to protect Californians’ consumer privacy. The Privacy Agency implements and enforces the California Consumer Privacy Act and the Delete Act. It is governed by a five-member board that consists of experts in privacy, technology, and consumer rights.

² Children’s Online Privacy Protection Act, HR 6291, 119th Cong. (2025), https://d1dth6e84htgma.cloudfront.net/01_H_R_6291_COPPA_2_0_18d36ec858.pdf

³ US House Energy & Commerce Committee Subcommittee on Commerce, Manufacturing, and Trade Hearing on “Legislative Solutions to Protect Children and Teens Online,” December 2, 2025, <https://energycommerce.house.gov/events/cmt-subcommittee-legislative-solutions-to-protect-children-and-teens-online>.

⁴ Cal. Cons. Art. 1 § 1.

⁵ Cal. Civ. Code § 1798.82; National Council of State Legislators, *Summary of Security Breach Notification Laws* (last updated January 17, 2022), <https://www.ncsl.org/technology-and-communication/security-breach-notification-laws>.

a comprehensive consumer privacy law, the California Consumer Privacy Act (CCPA),⁶ and since then nearly 20 states across the country have enacted similar comprehensive privacy laws.⁷ Then, in 2020, with millions of votes, California voters passed Proposition 24, which amended the CCPA and established the Privacy Agency.

Rights COPPA 2.0 Seeks to Eliminate

The preemption language in COPPA 2.0 is unusually expansive, and the full extent of its impact on California law would be a fact-specific determination. Below are just two examples of rights provided to minors in California, set to go into effect on January 1, 2026, that the preemption provision in COPPA 2.0 seeks to remove.

- **Heightened protections for sensitive personal information, including the right to limit use and disclosure.** Effective January 2026, the personal information of minors under 16 is considered sensitive personal information under the CCPA and its implementing regulations. Thus, minors will be afforded additional rights, including the right to further limit the use and disclosure of their personal information to what is reasonably necessary to provide the requested service.⁸ HR 6921 does not provide a comparable right. While COPPA 2.0 includes a purpose standard, it is less restrictive than California's because information can be "consistent with the context of a particular transaction" without being necessary for the requested service. COPPA 2.0 could remove important limits on the use and disclosure of minors' personal information.
- **Risk assessment requirement for sensitive personal information.** Under the CCPA and implementing regulations, businesses that process sensitive personal information will be required to conduct a risk assessment before processing the personal information and reviewed for accuracy at least once every three years thereafter.⁹ Businesses must also immediately update the risk assessment for any material changes. The goal of the risk assessment is to assess whether the risks of processing the personal information outweigh the benefits. This bill does not provide a comparable right. COPPA 2.0 could eliminate key guardrails over businesses' use of minors' personal information.

Federal Privacy Laws Traditionally Support States' Ability to Legislate

Traditionally, federal privacy laws have established a baseline of protections and preserved states' abilities to adopt stronger protections for their residents. This is critical for vulnerable populations, like minors, whom states are well equipped to protect. This multi-level governance has proven successful — the CCPA operates successfully alongside COPPA, providing additional protections as California has deemed necessary. Indeed, at least ten federal privacy statutes do not preempt states from enacting additional protections, including the Health Insurance Portability and Accountability Act (HIPAA), the Fair Credit Reporting Act (FCRA), Title I of the Electronic Communications Privacy Act (ECPA), the Video Privacy Protection Act, and the Driver's Privacy Protection Act, among others.¹⁰ California's increased protections in

⁶ Cal. Civ. Code § 1798.100 et seq.

⁷ Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, Oregon, New Hampshire, New Jersey, Rhode Island, Tennessee, Texas, Utah, and Virginia. *See*, IAPP, US State Comprehensive Privacy Laws Report: 2024 Legislative Session (October 2024), https://iapp.org/media/pdf/resource_center/us_state_privacy_laws_report_2024_session.pdf.

⁸ 11 CCR § 7001(bbb)(4).

⁹ Ca. Civ. Code § 1798.185(14)(B); 11 CCR § 7150.

¹⁰ 45 C.F.R. Part 160, Subpart B; 15 U.S.C. § 1681, et seq.; 18 U.S.C. § 2501-2523; 18 U.S.C. § 2710 et seq.; 18 U.S.C. § 2712. *See also*, Employee Polygraph Protection Act, 29 U.S.C. § 2009 et seq.; Telephone Consumer Protection Act, 47 U.S.C. § 227; Family Educational Rights and Privacy Act, 20 U.S.C. § 1232(g); Right to Financial Privacy Act, 12 U.S.C. § 3401 et seq.

these areas have not prevented it from becoming one of the largest economies in the world.¹¹

Conclusion

Preemption could strip away existing state protections that children currently enjoy in California. That would be a significant step backward in privacy protection at a time when parents are increasingly concerned about their children's privacy and security online, and when challenges from new technology are developing quickly. For these reasons, we respectfully request that the Committee reject the preemption provision in HR 6291 and uphold its longstanding approach to federal privacy legislation: establish a baseline for protections while preserving states' authority to adopt stronger laws.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Tom Kemp", written over a light gray horizontal line.

Tom Kemp
Executive Director
California Privacy Protection Agency

cc: Members, House Committee on Energy & Commerce

¹¹ Office of Governor Gavin Newsom, *California is Now the Fourth Largest Economy in the World* (April 23, 2025), <https://www.gov.ca.gov/2025/04/23/california-is-now-the-4th-largest-economy-in-the-world/>

#PassKOSA!



October 15, 2025

The Honorable John Thune
Senate Majority Leader
511 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Mike Johnson
Speaker of the House
568 Cannon House Office Building
Washington, DC 20515

The Honorable Chuck Schumer
Senate Minority Leader
322 Hart Senate Office Building
Washington, DC 20510

The Honorable Hakeem Jeffries
House Minority Leader
2267 Rayburn House Office Building
Washington, DC 20515

The Honorable Ted Cruz
Chair, U.S. Senate Committee on Commerce,
Science, and Transportation
167 Russell Senate Office Building
Washington, DC 20510

The Honorable Brett Guthrie
Chair, U.S. House Committee on Energy and
Commerce
2161 Rayburn House Office Building
Washington, DC 20515

The Honorable Maria Cantwell
Ranking Member, U.S. Senate Committee on
Commerce, Science, and Transportation
511 Hart Senate Office Building
Washington, DC 20510

The Honorable Frank Pallone
Ranking Member, U.S. House Committee on
Energy and Commerce
2107 Rayburn House Office Building
Washington, DC 20515

Dear Majority Leader Thune, Minority Leader Schumer, Chair Cruz, Ranking Member Cantwell, Speaker Johnson, Minority Leader Jeffries, Chair Guthrie, and Ranking Member Pallone:

The undersigned organizations—who collectively represent advocates, citizens, health care professionals, law enforcement officers, researchers, parents, academicians, students, and family members who have survived *preventable deaths* of beloved children—appeal to you in sorrow to pass the *Kids Online Safety Act* (KOSA), [S.1748](#), the most effective legislative response to the indisputable dangers facing children online, this Congress.

As you are aware, KOSA passed the U.S. Senate by a vote of 91-3 on July 31, 2024. The version introduced in the U.S. Senate this Congress, S.1748, has been scrutinized by first amendment attorneys and scholars to verify that **the bill protects the free speech rights of all Americans**. It addresses the conduct of companies prioritizing profit over safety, not the content of online communication. S. 1748 does not give the FTC or state attorneys general the power to bring lawsuits over content or speech.

Every industry in America, from car makers to toy producers to nuclear energy companies, must assure their products and services are safe for consumers. Industry spends money and time testing products and perfecting services to avoid causing harm that could trigger liability claims. Requiring companies to ensure that their products are safe is a bedrock U.S. legal concept. However, digital platforms have

#PassKOSA!



largely avoided this requirement when courts interpreted the *Communications Decency Act of 1996* as providing near blanket immunity from responsibility for what happens to users while they are online.

But **large social media companies are highly aware of the impact that their addictive algorithms have** on America's youth—something that we know as a result of 40 congressional hearings since 2019, multi-state litigation, and reports from whistleblowers who informed Big Tech executives about disturbing results of internal research.¹

The strength of KOSA is the legal concept at its heart: a “duty of care” to its users. This provision will compel covered social media companies to center online safety and wellbeing rather than profit alone. Implementing the duty of care will lead to decreased exposure of minors to algorithms that promote suicide and eating disorders, online bullying, illegal drug use, and sexual predators.

We know social media is fueling a youth mental health crisis in the United States. And we have seen time and again large social media companies refuse to police themselves in the absence of regulations. With this bipartisan legislation, Congress has the potential, and the obligation, to significantly improve young people's overall wellbeing by transforming the digital environment for children and teens.

Thank you for using your power to prioritize the health and safety of 73.1 million children under the age of 18 in the United States.² On June 27, in *Free Speech Coalition v. Paxton*, the Supreme Court affirmed an “important government interest” in protecting children online.³

We will not rest until KOSA is law.

Sincerely,

408 Organizations (Representing 50 states and the District of Columbia)

National Organizations

Active Minds

Alliance to End Human Trafficking

Altus Solutions, Inc.

American Association for Psychoanalysis in Clinical Social Work

American Compass

American Federation of Teachers (AFT)

American Youth Association (AYA)

Better Screen Time

¹ Dara Kerr, “Meta Failed to Address Harms to Teens, Whistleblower Testifies as Senators Vow Action,” NPR, November 7, 2023, <https://www.npr.org/2023/11/07/1211339737/meta-failed-to-address-harm-to-teens-whistleblower-testifies-as-senators-vow-act>

² “Older Adults Outnumber Children in 11 States and Nearly Half of U.S. Counties.” June 26, 2025. Reuters. <https://www.census.gov/newsroom/press-releases/2025/older-adults-outnumber-children.html>

³ “Free Speech Coalition, Inc., et al. v. Paxton, Attorney General of Texas.” Supreme Court of the United States. June 27, 2025.

#PassKOSA!



Bruderhof Communities
Center for Countering Digital Hate
Center for Digital Democracy
Children and Screens: Institute of Digital Media and Child Development
Clinical Social Work Association
Coalition Against Trafficking in Women (CATW)
Common Sense Media
Concerned Women for America Legislative Action Committee
Consumer Action
Covenant House International (providing direct services in: AL, CA, FL, GA, IL, LA, MD, MI, MO, NJ, NY, PA, TX, and Washington, DC)
Digital Childhood Alliance
Digital Progress Institute
Early Childhood Workgroup, Fairplay's Action Network
Eating Disorders Coalition for Research, Policy & Action
Enough is Enough
Fairplay
General Federation of Women's Clubs (50 Chapters & District of Columbia)
Heritage Action for America
Institute for Families and Technology
International Federation of Eating Disorders Dietitians
Institute for Family Studies
Interparliamentary Taskforce on Human Trafficking
Issue One
Knights of Columbus
Legacy of Hope International
MAMA: Mothers Against Media Addiction
Mental Health America
Monte Nido
NAACP
National Alliance for Eating Disorders
National Association of Pediatric Nurse Practitioners
National Center on Sexual Exploitation (NCOSE)
National Children's Alliance
National Council of Catholic Women
Nurses United Against Human Trafficking
Online Harms Prevention Workgroup of Parents Action Network
Parents Rise
Parents Television and Media Council
ParentsSOS
Pioneers International
Plan International USA

#PassKOSA!



Project HEAL
Prostitution, Research, and Education (PRE)
Protect All Children from Trafficking
Psychotherapy Action Network
Raven
REDC Consortium
Rescue America
Rights4Girls
Sex Trade Survivor Caucus
Shared Hope International (founded by former Rep. Linda Smith)
Smartphone Free Childhood US
Street Grace
The Anxious Generation Movement
The Jed Foundation
The Kennedy Forum (founded by former Rep. Patrick J. Kennedy)
The Tech Oversight Project
TJP Advocacy
Women's Liberation Front
World Without Exploitation

State & Local Organizations

Alabama

Katie's Truth
Kingdom Forerunners
Pike Regional Child Advocacy Center
Rescue Innocence Movement
The WellHouse

Alaska

Alaska Eating Disorders Alliance
MY House Matsu

Arizona

Arizona Anti-Trafficking Network
Center for Arizona Policy
Hickey Family Foundation
Katie Klein Consulting
Pearl at the Mailbox

Arkansas

The Genesis Project

#PassKOSA!



California

#HalfTheStory
3Strands Global Foundation
Alexander Neville Foundation
Ameera Foundation
Bay Area Nutrition
Because Justice Matters
Bilateral Safety Corridor Coalition
Central Valley Justice Coalition
Community Against Sexual Harm (CASH)
Core Wellness Living and Family Therapy Inc.
Courageous Women Association
Dance Awareness: No Child Exploited (DA:NCE)
Diamond Collective
Eating Disorders Resource Center (EDRC)
Emerge Counseling & Consulting
Equip
Exodus Cry
Father-Con
Finding Kids
Fitness n Mind
Global Hope 365
Jewish Family & Children's Services (San Francisco Bay Area)
Keeping Every Girl Free
MAMA & Distraction Free Schools California
New Day for Children
No App for Life
Olson Counseling Services Inc.
Pasadena Waldorf School
Positive Change Consultants
Recovery Record, Inc.
Resilient Ones
St. Irenaeus Bridge of Light Ministry
Survivor Leader Network of San Diego
Tech Oversight California
The Healthy Teen Project
Therapy with KB
Thriving in Freedom
Treasures
Valley Federation of Eating Disorder Professionals
Within Health
Wolverton Bailey Foundation

#PassKOSA!



NATIONAL
CENTER ON
SEXUAL
EXPLOITATION

Colorado

Annalee's Hope
Association for the Recovery of Children
Colorado Children's Alliance
Pornography is Not Education

Connecticut

Defend Young Minds
Empowered Network
Guided Purposes, LLC
Jacqui Cambell Nutrition
New Englanders Against Sexual Exploitation, CT Chapter
Partnership to End Human Trafficking
UConn Rudd Center for Food Policy & Health

Delaware

Be BRAVE
Esperanza Events & Consulting
Zoe Ministries of Delaware

Florida

America's Future, Inc.
Amy Jaffe Nutrition, LLC
ANEW Life International
Campaign Against Human Trafficking Southshore
Direct Access Counseling & Supportive Services
FLITE Center
Foundation Risk Partners
Kairos Digital
Lehigh Community Services
One More Child, Inc.
Paving the Way Foundation
Reflective Spaces Ministry, Corp.
SEA WAVES
Southwest FL Coalition Against Human Trafficking
Two Girls and a Bible, Inc.
United Abolitionists, Inc.
Wings of Shelter International, Inc.
Victims2Survivors-US

Georgia

Evolve Psychotherapy

#PassKOSA!



Rescuing Hope
Social Media Harms
The Emily Program

Hawaii

Ho'ola Na Pua

Idaho

Bright Tomorrows Child Advocacy Center
Citizens for Decency
Upper Valley Child Advocacy Center

Illinois

Alternatives Center
Be Real USA
Buckets Over Bullying/Bronstein Family Foundation
Dualang Ministries 4
Ernestine's Daughter
KIDS TOO
Moving Toward Health PC
Nourishment Works PC

Indiana

Christine Anderson, Inc.
Farrington Specialty Centers
Indiana Department of Child Services
Newburgh Police Department
Raindrops Rising Foundation
Resiliency Foundation
Whittington Services for Children and Families
Vickie Health LLC

Iowa

Chains Interrupted
Eating Disorder Coalition of Iowa

Kansas

Free State Nutrition
International Public Policy Institute
Screen Guardians
The Stop Trafficking Project®

Kentucky

EAT LAB, University of Louisville

#PassKOSA!



Kentucky Eating Disorder Council
Women Graduates USA

Louisiana

Free NOLA, Inc.
Dragonfly Harbor
Louisiana United Methodist Children and Families
Louisiana CASA
Metanoia Manor
Methodist Children's Home
Michelle Johnson Consulting LLC
Waldorf School of New Orleans

Maine

Ashley McHan Mindbody Psychotherapy
Just Love Worldwide
Nutrition Care Center
Turn the Tide Coalition

Maryland

Children and Adults with Attention-Deficit/Hyperactivity Disorder (CHADD)
Grace McComas Memorial
Maryland Coalition Against Pornography
Matthew Minor Awareness Foundation
Waldorf School of Baltimore

Massachusetts

Academy for Eating Disorders
All Girls Allowed
Becca Schmill Foundation
Culture Reframed
Defending the Early Years
Enough Abuse
Massachusetts PTA
My Life My Choice
Nourishing Words
NourishRX
Safe Exit Initiative
Stop Predatory Gambling
Sudbury for Digital Balance
The Multi Service Eating Disorders Association Inc. (MEDA)
Turning Life On

#PassKOSA!



Michigan

Center for Eating Disorders
Michigan Eating Disorders Alliance (MiEDA)
Protect Young Eyes

Minnesota

Alison Raman Counseling
Alternative Solutions
Devin J. Norring Foundation
Suicide Awareness Voices of Education (SAVE)
The Link MN
WithAll

Mississippi

Center for Violence Prevention
Rootdown

Missouri

ACCESS Lab at Washington University in St. Louis
Lion's Heart Montessori
Missouri Eating Disorders Council
Paradigm Shift Training and Consulting
Parent Pro Tech

Montana

Council of Catholic Women
ProjectSTAND
The Lifeguard Group
STEP, Inc.
The Worthy Ranch
Yellowstone Human Trafficking Task Force

Nebraska

Central Plains Child Advocacy Center
Disrupting Traffick
For Such a Time As This
Honesty Project
Tredas
Victress MVMT

Nevada

Awaken Reno

#PassKOSA!



CONVO Church
I AM Jessica Kay
Theravada Mental Health
Human Trafficking Prevention Alliance

New Hampshire

Beauty from Ashes Ministry
EXPOSE
New Hampshire Traffick Free Coalition

New Jersey

Emmy's Champions
Healing on Hudson
Mitola Nutrition
New Jersey Coalition Against Human Trafficking
Rest and Digest Nutrition LLC

New Mexico

Educate and Empower Kids

New York

Coalition Against Trafficking in Women
Eating Disorder Treatment Collaborative
Holy Family Parish
Joyful Heart Foundation
Lynn's Warriors
Marsh Law Firm PLLC
Mentari
National Organization for Women (NY Chapter)
Peace of Christ Parish (Rochester)
Sanctuary for Families
St Michael's Institute
The Emilee Connection
Waldorf Early Childhood Association of North America
Waldorf School of Saratoga Springs
WECAN
Western NY Comprehensive Care for Eating Disorders
Women's Justice NOW
Wonder Girls USA

North Carolina

AbolitionNC
Bannister Consultancy

#PassKOSA!



Chrysalis Center for Counseling and Eating Disorder Treatment
City of Henderson, NC
Designed for Joy
Essential Nutrition & Wellness
Forever Free Human Trafficking Rescue
Genesis...A New Beginning
Greenhouse Psychology and Wellness, PLLC
NC Stop Human Trafficking
Onehope Refuge
Pace & Tebb Nutrition Consulting
Project Light Rowan
Ruby Oak Nutrition
Safelight
Shield North Carolina
Stand Against Trafficking USA
Survivor Network NC

North Dakota

31:8 Project
Children's Advocacy Centers of North Dakota
ConnectUS Therapy
Families Flourish ND
Northern Plains Children's Advocacy Center
Red River Children's Advocacy Center

Ohio

Abolition Ohio
An Athlete's Silence
Broken to Beautifully Whole
Delta Counseling
Fully Nourished Nutrition, LLC
She Has A Name
Unite for Social Media

Oklahoma

Allied Nutrition Care
Deaf Church Oklahoma Inc.
Laureate Eating Disorder
Tech Safe Solutions
Truckers Against Trafficking

Oregon

Amanda Birkhead Nutrition Counseling

#PassKOSA!



Breaking Generational Cycles
Bridging the Gap-Oregon
Trafficking Law Center

Pennsylvania

Balanced Nutrition, LLC
Carpe Diem Nutrition
Center for Child Justice – Family Services Incorporated
Center for Mind, Body, and Wellness, Inc.
Delco Unplugged
Half A Million Kids
Luzerne County Child Advocacy Center
Native Clinics
PA Unplugged
Pennsylvania Nutrition Counseling, LLC
Promise of Life Network
Walk Her Home

Rhode Island

Leaders of the Former Together With Love
New Englanders Against Sexual Exploitation, RI Chapter
Tin Man Ministries

South Carolina

Born2Fly International, Inc.
Greenville Nutrition Therapy
Greenway Recovery
Less Than 3
South Carolina Legislative Roundtable on Human Trafficking

South Dakota

Victus Counseling
Compassionate Nutrition

Tennessee

Aristevi
Balance Nutrition Counseling
Forgiven Much Ministries
Fowler Nutrition PLLC
Freedom Forever
Heart of Intercession Ministry
Parents Who Fight
Riverside Entertainment

#PassKOSA!



NATIONAL
CENTER ON
SEXUAL
EXPLOITATION

Sarah Torti Counseling
Thistle Farms

Texas

A Butterfly Gets Its Wings
AK Chase Consulting
Allies Against Slavery
Carly Ryan Foundation
Child Advocates of Montgomery County
David's Legacy Foundation
Houston 20
Human Trafficking Abolitionists
Justice Society
MasterWord Services
Not on Our Watch
No Trafficking Zone
Redeemed Ministries
Reflection Ministries of TX
SB Nutrition Therapy
Talk More. Tech Less.
Texas Society for Clinical Social Work
Thoughtful Nutrition
Unbound Now
Wellspring
Wilco Therapist

Utah

Digital Childhood Institute
Fight the New Drug
PHASE Alliance

Vermont

New Englanders Against Sexual Exploitation (NEASE), VT Chapter
Northwest Unit for Special Investigations
Vermont Children's Alliance

Virginia

Courage to Nourish
Emily Harrison Consulting
Light of Life Ministries
Maternal Mental Health Leadership Alliance
Lisa Nava, Ph.D. & Associates, LLC
Maternal Mental Health Leadership Alliance

#PassKOSA!



Mood Balance Nutrition
New Creation
Prosperity Eating Disorders and Wellness
Rock Recovery
Tidal Counseling, PLC
Wealth Management Ministries – Prevention Works Joint Task Force and Coalition
Latisha's House

Washington

Andrea Broadwater Counseling and Consulting LLC
Bravespace Nutrition
Center for Online Safety
Emily RH Benedict Counseling
iSeeYouInitiative
The Seattle Clinic

West Virginia

Logan & Mingo Child Advocacy Centers
Harmony House, Inc.
West Virginia University School of Medicine
West Virginia Child Advocacy Network

Wisconsin

Fight to End Exploitation
Just Talk to Them
LOVE>hate Project
Mastarlarz Counseling, LLC
The Women's Community
Willow Tree CAC

Wyoming

Uprising

Common Sense Media Opposition Letter

Ahead of Tuesday's subcommittee hearing on the 19 kids' online safety bills, we wanted to highlight that Common Sense Media - which has long championed KOSA and COPPA - has serious concerns about the newly released House versions of both measures.

Below, you'll find a statement released today by our Founder and CEO, Jim Steyer, along with a brief analysis of the House version of COPPA 2.0. I've also attached to this email a set of potential questions that your boss may wish to consider using during the hearing. Common Sense Media Founder and CEO James P. Steyer released the following statement in advance of the December 2, 2025, hearing:

"Common Sense Media is deeply disappointed that critical kids' online safety bills being considered in a key House committee are significantly weaker than those passed by the Senate on a near-unanimous bipartisan basis. Last year, KOSA and COPPA 2.0 earned overwhelming support from parents across the country and passed the Senate by a vote of 91-3, with strong backing from both Republicans and Democrats.

"The House's versions of KOSA and COPPA 2.0, released just before Thanksgiving and being heard just days after, erode the safety and privacy protections our children desperately need. If Congress is serious about protecting kids online, this is a non-starter.

"We are particularly concerned that preemption language in both House bills may not just dilute protections already passed by the Senate but erase protections currently in law in both red and blue states. As written, these House bills seem to offer greater protections for the tech industry than they do for kids.

"America's kids and their families need strong protections from the harms that the tech industry and Congress know children and teens face online every day. We look forward to the hearing on Tuesday, where these and other bills will be subject to questions and discussion, and to working with the Committee and its Members to ensure that any final legislation that Congress approves will give children and families the protection they deserve."

Common Sense Media analysis of the House version of COPPA 2.0:

There are several serious problems with the just-unveiled House version of COPPA 2.0. For example:

- The sweeping preemptive language would prevent states from stepping in to protect kids and teens and responding to threats that emerge and change quickly. It has been over 25 years since Congress last passed a children's privacy law, COPPA. Congress cannot be trusted to move with haste.
- In addition, the preemption clause is so sweeping that it could cause children throughout the country to lose privacy and safety protections already put in place by state lawmakers (from across the political spectrum).
- And, the knowledge standard proposed is a step backwards. In court case after court case, documents are revealed that show tech companies know how old their young users are, but turn a blind eye, nonetheless. It is critical that companies be held accountable when they know or should have known—or have objective indicia of—young users. Further, start-ups and small companies can be just as problematic and dangerous for young users, who often jump on trends before adults do. No company should be able to turn a blind eye to kids.

Please feel free to draw on any of this material tomorrow and thank you for your attention to our concerns.

Best regards,

Holly

--

Holly Grosshans

Senior Counsel, Tech Policy | Common Sense Media

e: hgrosshans@commonsense.org

Follow Our Blog



Kids Online Safety Act House Discussion Draft
December 1, 2025

[ParentsSOS](#) is a coalition of over 20 families who have lost their children to online harms. We have been advocating for the Kids Online Safety Act in Congress for over three years. We have held hundreds of meetings on Capitol Hill sharing our stories with lawmakers, and our advocacy was critical to KOSA's 91-3 passage in the Senate last year.

We have significant concerns about the House's latest [KOSA discussion draft](#). Parent advocates have conveyed their willingness to compromise to Committee leadership and Representative Bilirakis, but the priorities we shared are not reflected in this discussion draft. Our foremost concerns include:

1. **The discussion draft contains overbroad preemption language that would undo critical work we have done in our home states to protect kids.** Parents refuse to preempt the states' ability to pass kids online safety legislation.
2. **The discussion draft has no Duty of Care to hold companies responsible for prioritizing profit over safety and wellbeing.** As we wait for Congress to act to protect children online, Big Tech continues to make decisions to maximize for kids' engagement instead of protecting their safety. Just over a week ago, a new filing in the multi-district litigation against major social media platforms [revealed new evidence](#) that Meta, Google, Snap, and ByteDance ignored clear evidence that design features — including beauty filters, autoplay, friend recommendations, and their algorithmic recommendations — harm kids and teens.
3. **It is unclear how the discussion draft's requirement that the platforms have reasonable policies, practices, and procedures to address some online harms will actually change Big Tech's conduct.** The harms enumerated in the discussion draft are mostly criminal acts and do not even include suicide. By contrast, S.B. 1748's Duty of Care covers mental health harms. In addition, the discussion draft only requires platforms to "address" harms through policies, practices and procedures, while S.B. 1748 requires operators to "prevent and mitigate" harms that are related to their platform's design.

4. **S.B. 1748 addresses both current and future design-caused harms.** The Senate's KOSA language defines "design features" as "including but not limited to" a list, while the House discussion draft omits the "not limited to" language. As a result, it is not clear the discussion draft will cover new design techniques developed and deployed by Big Tech in the future to maximize kids' online engagement.

5. **The discussion draft has a more limited scope than S.B. 1748.** S.B. 1748 holds companies responsible for protecting a user when they have "actual knowledge or knowledge fairly implied on the basis of objective circumstances" that a user is a minor. By contrast, the House discussion draft defines knowledge of a user's age as "actual knowledge or to have acted in willful disregard." It is unclear what the companies must not "willfully disregard" under this definition. Platforms must be held responsible for basing compliance on all of the information they have and infer about a user's age. In addition, the discussion draft does not include all online gaming platforms in the definition of "covered platform," unlike the S.B. 1748.

The House's decision to introduce a large package of bills, including many discussion drafts and bills that do not have Senate companions, will further delay what families have been asking of Congress for years: Real accountability to protect children online. **ParentsSOS is asking members of the Commerce, Manufacturing and Trade Subcommittee to support a strong KOSA that has a Duty of Care and no federal ceiling preemption.**

Social Media and Youth Mental Health

2023

The U.S. Surgeon General's Advisory



Contents



About the Advisory	3
Social Media and Youth Mental Health	4
Social Media Has Both Positive and Negative Impacts on Children and Adolescents	5
The Potential Benefits of Social Media Use Among Children and Adolescents	6
The Potential Harms of Social Media Use Among Children and Adolescents	6
What Drives Mental Health and Well-Being Concerns: A Snapshot of the Scientific Evidence	8
Potential Risk of Harm from Content Exposure	8
Potential Risk of Harm from Excessive and Problematic Use	9
Critical Questions Remain Unanswered	11
Known Evidence Gaps	11
We Must Take Action: A Way Forward	13
What Policymakers Can Do	15
What Technology Companies Can Do	16
What Parents and Caregivers Can Do	17
What Children and Adolescents Can Do	18
What Researchers Can Do	19
Acknowledgments	20
Endnotes	21

About the Advisory



A Surgeon General's Advisory is a public statement that calls the American people's attention to an urgent public health issue and provides recommendations for how it should be addressed. Advisories are reserved for significant public health challenges that require the nation's immediate awareness and action.

This Advisory calls attention to the growing concerns about the effects of social media on youth mental health. It explores and describes the current evidence on the positive and negative impacts of social media on children and adolescents, some of the primary areas for mental health and well-being concerns, and opportunities for additional research to help understand the full scope and scale of social media's impact. This document is not an exhaustive review of the literature. Rather, it was developed through a substantial review of the available evidence, primarily found via electronic searches of research articles published in English and resources suggested by a wide range of subject matter experts, with priority given to, but not limited to, meta-analyses and systematic literature reviews. It also offers actionable recommendations for the institutions that can shape online environments — policymakers and technology companies — as well as for what parents and caregivers, young people, and researchers can do.

For additional background and to read other Surgeon General's Advisories, visit **[SurgeonGeneral.gov](https://www.surgeongeneral.gov)**



Social Media and Youth Mental Health

Social media¹ use by youth is nearly universal. Up to 95% of youth ages 13–17 report using a social media platform, with more than a third saying they use social media “almost constantly.”² Although age 13 is commonly the required minimum age used by social media platforms in the U.S.,³ nearly 40% of children ages 8–12 use social media.⁴ Despite this widespread use among children and adolescents, robust independent safety analyses on the impact of social media on youth have not yet been conducted. There are increasing concerns among researchers, parents and caregivers, young people, healthcare experts, and others about the impact of social media on youth mental health.^{5,6}

More research is needed to fully understand the impact of social media; however, the current body of evidence indicates that while social media may have benefits for some children and adolescents, there are ample indicators that social media can also have a profound risk of harm to the mental health and well-being of children and adolescents. At this time, we do not yet have enough evidence to determine if social media is sufficiently safe for children and adolescents. We must acknowledge the growing body of research about potential harms, increase our collective understanding of the risks associated with social media use, and urgently take action to create safe and healthy digital environments that minimize harm and safeguard children’s and adolescents’ mental health and well-being during critical stages of development.

Up to 95% of youth ages 13–17 report using a social media platform, with more than a third saying they use social media “almost constantly.”

Social Media Has Both Positive and Negative Impacts on Children and Adolescents



The influence of social media on youth mental health is shaped by many complex factors, including, but not limited to, the amount of time children and adolescents spend on platforms, the type of content they consume or are otherwise exposed to, the activities and interactions social media affords, and the degree to which it disrupts activities that are essential for health like sleep and physical activity.⁶ Importantly, different children and adolescents are affected by social media in different ways, based on their individual strengths and vulnerabilities, and based on cultural, historical, and socio-economic factors.^{7,8} There is broad agreement among the scientific community that social media has the potential to both benefit and harm children and adolescents.^{6,9}

Brain development is a critical factor to consider when assessing the risk for harm. Adolescents, ages 10 to 19, are undergoing a highly sensitive period of brain development.^{10,11} This is a period when risk-taking behaviors reach their peak, when well-being experiences the greatest fluctuations, and when mental health challenges such as depression typically emerge.^{12,13,14} Furthermore, in early adolescence, when identities and sense of self-worth are forming, brain development is especially susceptible to social pressures, peer opinions, and peer comparison.^{11,13} Frequent social media use may be associated with distinct changes in the developing brain in the amygdala (important for emotional learning and behavior) and the prefrontal cortex (important for impulse control, emotional regulation, and moderating social behavior), and could increase sensitivity to social rewards and punishments.^{15,16} As such, adolescents may experience heightened emotional sensitivity to the communicative and interactive nature of social media.¹⁶ Adolescent social media use is predictive of a subsequent decrease in life satisfaction for certain developmental stages including for girls 11–13 years old and boys 14–15 years old.¹⁷ Because adolescence is a vulnerable period of brain development, social media exposure during this period warrants additional scrutiny.



The Potential Benefits of Social Media Use Among Children and Adolescents

Social media can provide benefits for some youth by providing positive community and connection with others who share identities, abilities, and interests. It can provide access to important information and create a space for self-expression.⁹ The ability to form and maintain friendships online and develop social connections are among the positive effects of social media use for youth.^{18, 19} These relationships can afford opportunities to have positive interactions with more diverse peer groups than are available to them offline and can provide important social support to youth.¹⁸ The buffering effects against stress that online social support from peers may provide can be especially important for youth who are often marginalized, including racial, ethnic, and sexual and gender minorities.^{20, 21, 22} For example, studies have shown that social media may support the mental health and well-being of lesbian, gay, bisexual, asexual, transgender, queer, intersex and other youths by enabling peer connection, identity development and management, and social support.²³ Seven out of ten adolescent girls of color report encountering positive or identity-affirming content related to race across social media platforms.²⁴ A majority of adolescents report that social media helps them feel more accepted (58%), like they have people who can support them through tough times (67%), like they have a place to show their creative side (71%), and more connected to what's going on in their friends' lives (80%).²⁵ In addition, research suggests that social media-based and other digitally-based mental health interventions may also be helpful for some children and adolescents by promoting help-seeking behaviors and serving as a gateway to initiating mental health care.^{8, 26, 27, 28, 29}

The Potential Harms of Social Media Use Among Children and Adolescents

Over the last decade, evidence has emerged identifying reasons for concern about the potential negative impact of social media on children and adolescents.

A longitudinal cohort study of U.S. adolescents aged 12–15 (n=6,595) that adjusted for baseline mental health status found that adolescents who spent more than 3 hours per day on social media faced double the risk of experiencing poor mental health outcomes including symptoms of depression and anxiety.³⁰



As of 2021, 8th and 10th graders now spend an average of 3.5 hours per day on social media.³¹ In a unique natural experiment that leveraged the staggered introduction of a social media platform across U.S. colleges, the roll-out of the platform was associated with an increase in depression (9% over baseline) and anxiety (12% over baseline) among college-aged youth (n = 359,827 observations).³² The study's co-author also noted that when applied across the entirety of the U.S. college population, the introduction of the social media platform may have contributed to more than 300,000 new cases of depression.^{32, 33} If such sizable effects occurred in college-aged youth, these findings raise serious concerns about the risk of harm from social media exposure for children and adolescents who are at a more vulnerable stage of brain development.

Limits on the use of social media have resulted in mental health benefits for young adults and adults. A small, randomized controlled trial in college-aged youth found that limiting social media use to 30 minutes daily over three weeks led to significant improvements in depression severity.³⁴ This effect was particularly large for those with high baseline levels of depression who saw an improvement in depression scores by more than 35%.³⁵ Another randomized controlled trial among young adults and adults found that deactivation of a social media platform for four weeks improved subjective well-being (i.e., self-reported happiness, life satisfaction, depression, and anxiety) by about 25–40% of the effect of psychological interventions like self-help therapy, group training, and individual therapy.³⁶

In addition to these recent studies, correlational research on associations between social media use and mental health has indicated reason for concern and further investigation. These studies point to a higher relative concern of harm in adolescent girls and those already experiencing poor mental health,^{37, 38, 39} as well as for particular health outcomes like cyberbullying-related depression,⁴⁰ body image and disordered eating behaviors,⁴¹ and poor sleep quality linked to social media use.⁴² For example, a study conducted among 14-year-olds (n = 10,904) found that greater social media use predicted poor sleep, online harassment, poor body image, low self-esteem, and higher depressive symptom scores with a larger association for girls than boys.⁴³ A majority of parents of adolescents say they are somewhat, very, or extremely worried that their child's use of social media could lead to problems with anxiety or depression (53%), lower self-esteem (54%), being harassed or bullied by others (54%), feeling pressured to act a certain way (59%), and exposure to explicit content (71%).⁴⁴

What Drives Mental Health and Well-Being Concerns: A Snapshot of the Scientific Evidence



Scientific evidence suggests that harmful content exposure as well as excessive and problematic social media use are primary areas for concern.

Potential Risk of Harm from Content Exposure

Extreme, inappropriate, and harmful content continues to be easily and widely accessible by children and adolescents. This can be spread through direct pushes, unwanted content exchanges, and algorithmic designs. In certain tragic cases, childhood deaths have been linked to suicide- and self-harm-related content and risk-taking challenges on social media platforms.^{45, 46} This content may be especially risky for children and adolescents who are already experiencing mental health difficulties.⁴⁷ Despite social media providing a sense of community for some, a systematic review of more than two dozen studies found that some social media platforms show live depictions of self-harm acts like partial asphyxiation, leading to seizures, and cutting, leading to significant bleeding.⁴⁸ Further, these studies found that discussing or showing this content can normalize such behaviors, including through the formation of suicide pacts and posting of self-harm models for others to follow.

Social media may also perpetuate body dissatisfaction, disordered eating behaviors, social comparison, and low self-esteem, especially among adolescent girls.^{49, 50, 51, 52} A synthesis of 20 studies demonstrated a significant relationship between social media use and body image concerns and eating disorders, with social comparison as a potential contributing factor.⁴¹ Social comparison driven by social media is associated with body dissatisfaction, disordered eating, and depressive symptoms.^{53, 54, 55, 56} When asked about the impact of social media on their body image, nearly half (46%) of adolescents aged 13–17 said social media makes them feel worse, 40% said it makes them feel neither better nor worse, and only 14% said it makes them feel better.⁵⁷

Additionally, roughly two-thirds (64%) of adolescents are “often” or “sometimes” exposed to hate-based content.⁵⁸ Among adolescent girls of color, one-third or more report exposure to racist content or language on social media platforms



at least monthly.²⁴ In a review of 36 studies, a consistent relationship was found between cyberbullying via social media and depression among children and adolescents,⁴⁰ with adolescent females and sexual minority youth more likely to report experiencing incidents of cyberbullying.^{59, 60} Nearly 75% of adolescents say social media sites are only doing a fair to poor job of addressing online harassment and cyberbullying.⁶¹

In addition, social media platforms can be sites for predatory behaviors and interactions with malicious actors who target children and adolescents (e.g., adults seeking to sexually exploit children, to financially extort them through the threat or actual distribution of intimate images, or to sell illicitly manufactured fentanyl).^{62, 63, 64} Adolescent girls and transgender youth are disproportionately impacted by online harassment and abuse, which is associated with negative emotional impacts (e.g., feeling sad, anxious or worried).^{65, 66} Nearly 6-in-10 adolescent girls say they've been contacted by a stranger on certain social media platforms in ways that make them feel uncomfortable.²⁴

Potential Risk of Harm from Excessive and Problematic Use

Excessive and problematic use of social media can harm children and adolescents by disrupting important healthy behaviors. Social media platforms are often designed to maximize user engagement, which has the potential to encourage excessive use and behavioral dysregulation.^{67, 68, 69,} ⁷⁰ Push notifications, autoplay, infinite scroll, quantifying and displaying popularity (i.e., 'likes'), and algorithms that leverage user data to serve content recommendations are some examples of these features that maximize engagement. According to one recent model, nearly a third (31%) of social media use may be attributable to self-control challenges magnified by habit formation.⁷¹ Further, some researchers believe that social media exposure can overstimulate the reward center in the brain and, when the stimulation becomes excessive, can trigger pathways comparable to addiction.^{68, 72} Small studies have shown that people with frequent and problematic social media use can experience changes in brain structure similar to changes seen in individuals with substance use or gambling addictions.^{73, 74} In a nationally representative survey of girls aged 11–15, one-third or more say they feel “addicted” to a social media platform.²⁴ Over half of teenagers report that it would be hard to give



up social media.² Nearly 3-in-4 teenagers believe that technology companies manipulate users to spend more time on their devices.⁶⁸ In addition, according to a survey of 8th and 10th graders, the average time spent on social media is 3.5 hours per day, 1-in-4 spend 5+ hours per day and 1-in-7 spend 7+ hours per day on social media.³¹

Excessive and problematic social media use, such as compulsive or uncontrollable use, has been linked to sleep problems, attention problems, and feelings of exclusion among adolescents.^{43, 75, 76, 77} Sleep is essential for the healthy development of adolescents. A systematic review of 42 studies on the effects of excessive social media use found a consistent relationship between social media use and poor sleep quality, reduced sleep duration, sleep difficulties, and depression among youth.⁴² Poor sleep has been linked to altered neurological development in adolescent brains, depressive symptoms, and suicidal thoughts and behaviors.^{78, 79, 80} On a typical weekday, nearly 1-in-3 adolescents report using screen media until midnight or later.⁵⁸ While screen media use encompasses various digital activities, social media applications are the most commonly used applications by adolescents.⁵⁸

In a recent narrative review of multiple studies, problematic social media use has also been linked to both self-reported and diagnosed attention-deficit/hyperactivity disorder (ADHD) in adolescents, although more research is necessary to understand whether one causes the other.⁸¹ A longitudinal prospective study of adolescents without ADHD symptoms at the beginning of the study found that, over a 2-year follow-up, high-frequency use of digital media, with social media as one of the most common activities, was associated with a modest yet statistically significant increased odds of developing ADHD symptoms (OR 1.10; 95% CI, 1.05-1.15).⁸² Additionally, social media-induced fear of missing out, or “the pervasive apprehension that others might be having rewarding experiences from which one is absent,”⁸³ has been associated with depression, anxiety, and neuroticism.⁸⁴



Nearly every teenager in America uses social media, and yet we do not have enough evidence to conclude that it is sufficiently safe for them. Our children have become unknowing participants in a decades-long experiment. It is critical that independent researchers and technology companies work together to rapidly advance our understanding of the impact of social media on children and adolescents. This section describes the known gaps and proposes additional areas for research that warrant urgent consideration.

Known Evidence Gaps

The relationship between social media and youth mental health is complex and potentially bidirectional.¹⁹ There is broad concern among the scientific community that a lack of access to data and lack of transparency from technology companies have been barriers to understanding the full scope and scale of the impact of social media on mental health and well-being. Most prior research to date has been correlational, focused on young adults or adults, and generated a range of results.⁸⁵ Critical areas of research have been proposed to fill knowledge gaps and create evidence-based interventions, resources, and tools to support youth mental health.⁸⁶ Thus, there is an urgent need for additional research including on, but not limited to, the following questions:

- How do in-person vs. digital social interactions differ in terms of the impact on health, and what are the unique contributions of social media behavior to social connectedness, social isolation, and mental health symptoms?
- What are the potential pathways through which social media may cause harm to children's and adolescents' mental health and well-being? For example:
 - » How does social comparison affect one's sense of life satisfaction and in-person relationships?
 - » How does the use of social media, including specific designs and features, relate to dopamine pathways involved in motivation, reward, and addiction?
- What type of content, and at what frequency and intensity, generates the most harm? Through which modes of social media access (e.g., smartphone, computer) and design features? For which users and why?



- What are the beneficial effects of social media? For whom are the benefits greatest? In what ways, and under what circumstances?
- What individual-, community-, and societal-level factors may protect youth from the negative effects of social media?
- What types of strategies and approaches are effective in protecting the mental health and well-being of children and adolescents on social media (e.g., programs, policies, design features, interventions, norms)?
- How does social media use interact with a person's developmental stage for measuring risk of mental health impact?

It is critical that independent researchers and technology companies work together to rapidly advance our understanding of the impact of social media on children and adolescents.

We Must Take Action: A Way Forward



Our children and adolescents don't have the luxury of waiting years until we know the full extent of social media's impact. Their childhoods and development are happening now. While social media use can have positive impacts for some children, the evidence noted throughout this Surgeon General's Advisory necessitates significant concern with the way it is currently designed, deployed, and utilized. Child and adolescent use of platforms designed for adults places them at high risk of "unsupervised, developmentally inappropriate, and potentially harmful" use according to the National Scientific Council on Adolescence.⁸⁷ At a moment when we are experiencing a national youth mental health crisis, now is the time to act swiftly and decisively to protect children and adolescents from risk of harm.

To date, the burden of protecting youth has fallen predominantly on children, adolescents, and their families. Parents face significant challenges in managing children and adolescents' use of social media applications, and youth are using social media at increasingly earlier ages.^{4,88} Nearly 70% of parents say parenting is now more difficult than it was 20 years ago, with technology and social media as the top two cited reasons.⁸⁹ While nearly all parents believe they have a responsibility to protect their children from inappropriate content online,⁸⁹ the entire burden of mitigating the risk of harm of social media cannot be placed on the shoulders of children and parents. Nearly 80% of parents believe technology companies have a responsibility to protect children from inappropriate content as well.⁸⁹

We must provide children and their families with the information and tools to navigate the changing digital environment, but this burden to support our children must be further shared. There are actions technology companies can take to make their platforms safer for children and adolescents. There are actions researchers can take to develop the necessary research base to support further safeguards. And there is a role for local, state, and federal policy to implement protections for our children and adolescents.

The U.S. has a strong history of taking action in such circumstances. In the case of toys, transportation, and medications — among other sectors that have



widespread adoption and impact on children — the U.S. has often adopted a safety-first approach to mitigate the risk of harm to consumers. According to this principle, a basic threshold for safety must be met, and until safety is demonstrated with rigorous evidence and independent evaluation, protections are put in place to minimize the risk of harm from products, services, or goods. For example, the Consumer Product Safety Commission requires toy manufacturers to undergo third-party testing and be certified through a Children's Product Certificate as compliant with the federal toy safety standard for toys intended for use by children.⁹⁰ To reduce the risk of injury from motor vehicle accidents, the National Highway Traffic Safety Administration requires manufacturers to fit new motor vehicles with standard airbags and seat belts, among other safety features, and conduct crash tests to be compliant with the Federal Motor Vehicle Safety Standards.⁹¹ Medications must demonstrate safety to the Food and Drug Administration before being made available and marketed for use.⁹² Given the mounting evidence for the risk of harm to some children and adolescents from social media use, a safety-first approach should be applied in the context of social media products.

To better safeguard the mental health and well-being of children and adolescents, policymakers, technology companies, researchers, families, and young people must all engage in a proactive and multifaceted approach. Through the recommendations below, we can provide more resources and tools to children and families, we can gain a better understanding of the full impact of social media, and we can maximize the benefits and minimize the harms of social media platforms to create safer, healthier online environments for children.

We can maximize the benefits and minimize the harms of social media platforms to create safer, healthier online environments for children.

What Policymakers Can Do



Policymakers play an important role in addressing the complex and multifaceted issues related to social media use and in protecting youth from harm.

- **Strengthen protections to ensure greater safety for children interacting with all social media platforms**, in collaboration with governments, academic organizations, public health experts, and technology companies.
 - » **Develop age-appropriate health and safety standards** for technology platforms. Such standards may include designing technology that is appropriate and safe for a child's developmental stage; protecting children and adolescents from accessing harmful content (e.g., content that encourages eating disorders, violence, substance abuse, sexual exploitation, and suicide or discusses suicide means); limiting the use of features that attempt to maximize time, attention, and engagement; developing tools that protect activities that are essential for healthy development like sleep; and regularly assessing and mitigating risks to children and adolescents.
 - » **Require a higher standard of data privacy for children** to protect them from potential harms like exploitation and abuse. Six-in-ten adolescents say they think they have little or no control over the personal information that social media companies collect about them.³²
 - » **Pursue policies that further limit access — in ways that minimize the risk of harm — to social media for all children**, including strengthening and enforcing age minimums.
- **Ensure technology companies share data relevant to the health impact of their platforms** with independent researchers and the public in a manner that is timely, sufficiently detailed, and protects privacy.
- **Support the development, implementation, and evaluation of digital and media literacy curricula in schools and within academic standards.** Digital and media literacy provides children and educators with digital skills to strengthen digital resilience, or the ability to recognize, manage, and recover from online risks (e.g., cyberbullying and other forms of online harassment and abuse, as well as excessive social media use).
- **Support increased funding for future research** on both the benefits and harms of social media use and other technology and digital media use for children, adolescents, and families.
- **Engage with international partners** working to protect children and adolescents against online harm to their health and safety.

What Technology Companies Can Do



Technology companies play a central role and have a fundamental responsibility in designing safe online environments and in preventing, minimizing, and addressing the risks associated with social media.

- **Conduct and facilitate transparent and independent assessments of the impact of social media products and services on children and adolescents.** Assume responsibility for the impact of products on different subgroups and ages of children and adolescents, regardless of the intent behind them.
 - » **Be transparent and share assessment findings and underlying data** with independent researchers and the public in a privacy protecting manner.
 - » **Assess the potential risks of online interactions and take active steps to prevent potential misuse**, reducing exposure to harms. When proactive responses fail, take immediate action to mitigate unintended negative effects.
 - » **Establish scientific advisory committees to inform approaches and policies** aimed at creating safe online environments for children. Scientific advisory committees should be comprised of independent experts and members of user subgroups, including youth.
- **Prioritize user health and safety in the design and development of social media products and services.**^{93, 94, 95, 96} Prioritize and leverage expertise in developmental psychology and user mental health and well-being in product teams to minimize risks of harm to children and adolescents.
 - » **Ensure default settings for children are set to highest safety and privacy standards.** Provide easy-to-read and highly visible information about policies regarding use by children.
 - » **Adhere to and enforce age minimums** in ways that respect the privacy of youth users.
- **Design, develop, and evaluate platforms, products, and tools that foster safe and healthy online environments for youth**, keeping in mind the needs of girls, racial, ethnic, and sexual and gender minorities. The platform design and algorithms should prioritize health and safety as the first principle, seek to maximize the potential benefits, and avoid design features that attempt to maximize time, attention, and engagement.
- **Share data relevant to the health impact of platforms and strategies employed to ensure safety and well-being** with independent researchers and the public in a manner that is timely and protects privacy.
- **Create effective and timely systems and processes to adjudicate requests and complaints from young people, families, educators, and others** to address online abuse, harmful content and interactions, and other threats to children's health and safety. Social media platforms should take these complaints seriously, thoroughly investigate and consider them, and respond in a timely and transparent manner.

What Parents and Caregivers Can Do



The onus of mitigating the potential harms of social media should not be placed solely on the shoulders of parents and caregivers, but there are steps they can take to help protect and support children and adolescents against the risk of harm.

- **Create a family media plan.**⁹⁷ Agreed-upon expectations can help establish healthy technology boundaries at home—including social media use. A family media plan can promote open family discussion and rules about media use and include topics such as balancing screen/online time, content boundaries, and not disclosing personal information. For information on creating a family media plan, visit www.healthychildren.org/MediaUsePlan.
- **Create tech-free zones and encourage children to foster in-person friendships.**⁹⁸ Since electronics can be a potential distraction after bedtime and can interfere with sleep, consider restricting the use of phones, tablets, and computers for at least 1 hour before bedtime and through the night. Consider keeping family mealtimes and in-person gatherings device-free to build social bonds and engage in a two-way conversation. Help your child develop social skills and nurture his or her in-person relationships by encouraging unstructured and offline connections with others and making unplugged interactions a daily priority. See the American Academy of Pediatrics (AAP) [guidelines for media use](#).
- **Model responsible social media behavior.** As children often learn behaviors and habits from what they see around them, try to model the behavior you want to see.^{97,99} Parents can set a good example of what responsible and healthy social media use looks like by limiting their own use, being mindful of social media habits (including when and how parents share information or content about their child), and modeling positive behavior on your social media accounts.
- **Teach kids about technology and empower them to be responsible online participants at the appropriate age.**¹⁰⁰ Discuss with children the benefits and risks of social media as well as the importance of respecting privacy and protecting personal information in age-appropriate ways. Have conversations with children about who they are connecting with, their privacy settings, their online experiences, and how they are spending their time online. Empower and encourage them to seek help should they need it. Learn more about the benefits and risks of social media use and get guidance from experts at AAP's [Center of Excellence on Social Media and Youth Mental Health](#) and from the American Psychological Association's [Health Advisory on Social Media Use in Adolescence](#).
- **Report cyberbullying and online abuse and exploitation.** Talk to your child about their reporting options, and provide support, without judgment, if he or she tells or shows you that they (a) are being harassed through email, text message, online games, or social media or (b) have been contacted by an adult seeking private images or asking them to perform intimate or sexual acts. You or your child can report cyberbullying to the school and/or the online platform, or your local law enforcement.¹⁰¹ Visit [CyberTipline](#), [Take it Down](#), or contact your local law enforcement to report any instances of online exploitation.
- **Work with other parents to help establish shared norms and practices and to support programs and policies around healthy social media use.** Such norms and practices among parents facilitate collective action and can make it easier to set and implement boundaries on social media use for children.

What Children and Adolescents Can Do



The burden of mitigating the potential harms of social media does not rest solely on the shoulders of children and adolescents, but there are measures they can take to navigate social media in a safe and healthy way.

- **Reach out for help.** If you or someone you know is being negatively affected by social media, reach out to a trusted friend or adult for help. For information from experts, visit AAP's [Center of Excellence on Social Media and Youth Mental Health](#). If you or someone you know is experiencing a mental health crisis, contact the 988 Suicide and Crisis Lifeline by calling or texting 988 for immediate help.
- **Create boundaries to help balance online and offline activities.** Limit the use of phones, tablets, and computers for at least 1 hour before bedtime and through the night to enable sufficient and quality sleep. Keep mealtimes and in-person gatherings device-free to help build social bonds and engage in two-way conversations with others. Nurture your in-person relationships by connecting with others and making unplugged interactions a daily priority.
- **Develop protective strategies and healthy practices** such as tracking the amount of time you spend online, blocking unwanted contacts and content, learning about and using available privacy and safety settings, learning and utilizing digital media literacy skills to help tell the difference between fact and opinion, and ensuring you are connecting with peers in-person. See this [Tip Sheet on Social Media Use and Mental Health](#) for healthy social media use created for and by young people.
- **Be cautious about what you share.** Personal information about you has value. Be selective with what you post and share online and with whom, as it is often public and can be stored permanently. If you aren't sure if you should post something, it's usually best if you don't. Talk to a family member or trusted adult to see if you should.
- **Protect yourself and others.** Harassment that happens in email, text messaging, direct messaging, online games, or on social media is harmful and can be cyberbullying. It might involve trolling, rumors, or photos passed around for others to see –and it can leave people feeling angry, sad, ashamed, or hurt. If you or someone you know is the victim of cyberbullying or other forms of online harassment and abuse:
 - » **Don't keep online harassment or abuse a secret.** Reach out to at least one person you trust, such as a close friend, family member, counselor, or teacher, who can give you the help and support you deserve. Visit stopbullying.gov for helpful tips on how to report cyberbullying. If you have experienced online harassment and abuse by a dating partner, contact an expert at [Love is Respect](#) for support or if your private images have been taken and shared online without your permission, visit [Take it Down](#) to help get them removed.
 - » **Don't take part in online harassment or abuse.** Avoid forwarding or sharing messages or images and tell others to stop. Another way is to report offensive content to the site or network where you saw it.

What Researchers Can Do



Researchers play a critical role in helping to gain a better understanding of the full impact of social media on mental health and well-being and informing policy, best practices, and effective interventions.

- **Establish the impact of social media on youth mental health as a research priority and develop a shared research agenda.**¹⁰² Research should include but not be limited to:
 - » **Rigorous evaluation of social media's impact** on youth mental health and well-being, including longitudinal and experimental studies. This could also include research on specific outcomes and clinical diagnoses (e.g., sleep duration and quality, attention, depression, anxiety, and body image), among specific populations (e.g., racial, ethnic, and sexual and gender minorities), and based on specific aspects of social media (e.g., designs, features, and algorithms).
 - » **Role of age, developmental stage, cohort processes, and the in-person environment** in influencing the onset and progression of poor mental health outcomes among social media users.
 - » **Benefits and risks associated** with specific social media designs, features, and content.
 - » **Long-term effects on adults** of social media use during childhood and adolescence.
- **Develop and establish standardized definitions and measures** for social media and mental health outcomes that are regularly evaluated and can be applied across basic research, population surveillance, intervention evaluation, and other contexts.
- **Evaluate best practices for healthy social media use** in collaboration with experts including healthcare providers, parents, and youth.^{94, 103, 104}
- **Enhance research coordination and collaboration.** Example opportunities include developing an accessible evidence database and forming a consortium of researchers focused on examining the positive and negative effects of social media on mental health and well-being. Researchers should work with community partners to make research findings publicly accessible and digestible.

Acknowledgments



We are grateful to all of the experts, academic researchers, associations, and community-based organizations across the country who shared their insights.

The U.S. Surgeon General's Advisory on Social Media and Youth Mental Health was prepared by the Office of the Surgeon General with valuable contributions from partners across the U.S. Government, including but not limited to:

Office of the Assistant Secretary for Health (OASH)

Office of the General Counsel (OGC)

Office of the Assistant Secretary for Planning and Evaluation (ASPE)

Centers for Disease Control and Prevention (CDC)

Office of the Director

National Center for Injury Prevention and Control (NCIPC)

National Center for HIV, Viral Hepatitis, STD, and TB Prevention, Division of Adolescent and School Health (DASH)

Health Resources and Services Administration (HRSA)

National Institutes of Health (NIH)

***Eunice Kennedy Shriver* National Institute of Child Health and Human Development (NICHD)**

National Institute of Mental Health (NIMH)

Substance Abuse and Mental Health Services Administration (SAMHSA)

Endnotes

1. The definition of social media has been highly debated over the past few decades. As a result, there isn't a single, widely-accepted scholarly definition of social media. (Aichner et al., 2021) The definition may vary from the cited research in this document based on the methods used in each study. In making conclusions and recommendations, this document regards social media as "internet-based channels that allow users to opportunistically interact and selectively self-present, either in real-time or asynchronously, with both broad and narrow audiences who derive value from user-generated content and the perception of interaction with others." (Carr & Hayes, 2015) For the purposes of this product, we did not include studies specific to online gaming or e-sports. **Source:** Aichner, T., Grünfelder, M., Maurer, O., & Jegeni, D. (2021). Twenty-Five Years of Social Media: A Review of Social Media Applications and Definitions from 1994 to 2019. *Cyberpsychology, Behavior And Social Networking*, 24(4), 215–222. <https://doi.org/10.1089/cyber.2020.0134> **Source:** Carr, C. T., & Hayes, R. A. (2015). Social Media: Defining, Developing, and Divining. *Atlantic Journal of Communication*, 23:1, 46-65. <https://doi.org/10.1080/15456870.2015.972282>
2. Vogels, E., Gelles-Watnick, R. & Massarat, N. (2022). Teens, Social Media and Technology 2022. Pew Research Center: Internet, Science & Tech. United States of America. Retrieved from <https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/>
3. The minimum required age set by social media platforms is informed by the Children's Online Privacy Protection Act that requires social media platforms to collect verifiable parental consent before collecting, storing, and sharing data from children under age 13. **Source:** Federal Trade Commission. (n.d.). Children's Online Privacy Protection Act ("COPPA"). Federal Trade Commission. Retrieved from <https://www.ftc.gov/legal-library/browse/statutes/childrens-online-privacy-protection-act>
4. Rideout, V., Peebles, A., Mann, S., & Robb, M. B. (2022). Common Sense Census: Media use by tweens and teens, 2021. San Francisco, CA: Common Sense. Retrieved from https://www.common SenseMedia.org/sites/default/files/research/report/8-18-census-integrated-report-final-web_0.pdf
5. It is important to note that many factors can shape mental health, and a comprehensive approach, including prevention strategies, will be needed to support and protect the mental health of children and adolescents. **Source:** Office of the Surgeon General (OSG). (2021). Protecting Youth Mental Health: The U.S. Surgeon General's Advisory. US Department of Health and Human Services. Retrieved from <https://www.hhs.gov/sites/default/files/surgeon-general-youth-mental-health-advisory.pdf>
6. American Psychological Association. (2023). Health Advisory on Social Media Use in Adolescence. American Psychological Association. Retrieved from <https://www.apa.org/topics/social-media-internet/health-advisory-adolescent-social-media-use.pdf>
7. Beyens, I., Pouwels, J. L., van Driel, I. I., Keijsers, L., & Valkenburg, P. M. (2020). The effect of social media on well-being differs from adolescent to adolescent. *Scientific reports*, 10(1), 10763. <https://doi.org/10.1038/s41598-020-67727-7>
8. Hollis, C., Livingstone, S., & Sonuga-Barke, E. (2020). Editorial: The role of digital technology in children and young people's mental health - a triple-edged sword?. *Journal of child psychology and psychiatry, and allied disciplines*, 61(8), 837–841. <https://doi.org/10.1111/jcpp.13302>
9. Uhls, Y. T., Ellison, N. B., & Subrahmanyam, K. (2017). Benefits and Costs of Social Media in Adolescence. *Pediatrics*, 140(Suppl 2), S67–S70. <https://doi.org/10.1542/peds.2016-1758E>
10. Fuhrmann, D., Knoll, L. J., & Blakemore, S. J. (2015). Adolescence as a Sensitive Period of Brain Development. *Trends in cognitive sciences*, 19(10), 558–566. <https://doi.org/10.1016/j.tics.2015.07.008>
11. Blakemore, S. J., & Mills, K. L. (2014). Is adolescence a sensitive period for sociocultural processing?. *Annual review of psychology*, 65, 187–207. <https://doi.org/10.1146/annurev-psych-010213-115202>
12. Romer D. (2010). Adolescent risk taking, impulsivity, and brain development: implications for prevention. *Developmental psychobiology*, 52(3), 263–276. <https://doi.org/10.1002/dev.20442>
13. National Academies of Sciences, Engineering, and Medicine (NASEM). (2019). The Promise of Adolescence: Realizing Opportunity for All Youth. Washington, DC: The National Academies Press. <https://doi.org/10.17226/25388>
14. Kessler, R. C., Amminger, G. P., Aguilar-Gaxiola, S., Alonso, J., Lee, S., & Ustün, T. B. (2007). Age of onset of mental disorders: a review of recent literature. *Current opinion in psychiatry*, 20(4), 359–364. <https://doi.org/10.1097/YCO.0b013e32816ebc8c>
15. Maza, M. T., Fox, K. A., Kwon, S. J., Flannery, J. E., Lindquist, K. A., Prinstein, M. J., & Telzer, E. H. (2023). Association of Habitual Checking Behaviors on Social Media With Longitudinal Functional Brain Development. *JAMA pediatrics*, 177(2), 160–167. <https://doi.org/10.1001/jamapediatrics.2022.4924>
16. Crone, E. A., & Konijn, E. A. (2018). Media use and brain development during adolescence. *Nature communications*, 9(1), 588. <https://doi.org/10.1038/s41467-018-03126-x>

17. Orben, A., Przybylski, A. K., Blakemore, S. J., & Kievit, R. A. (2022). Windows of developmental sensitivity to social media. *Nature communications*, 13(1), 1649. <https://doi.org/10.1038/s41467-022-29296-3>
18. Anderson, M. & Jiang, J. (2018). Teens' Social Media Habits and Experiences. Pew Research Center: Internet, Science & Tech. United States of America. Retrieved from <https://www.pewresearch.org/internet/2018/11/28/teens-social-media-habits-and-experiences/>
19. Seabrook, E. M., Kern, M. L., & Rickard, N. S. (2016). Social Networking Sites, Depression, and Anxiety: A Systematic Review. *JMIR mental health*, 3(4), e50. <https://doi.org/10.2196/mental.5842>
20. According to the National Institutes of Health, sexual and gender minority (SGM) populations include, but are not limited to, individuals who identify as lesbian, gay, bisexual, asexual, transgender, Two-Spirit, queer, and/or intersex. Individuals with same-sex or -gender attractions or behaviors and those with a difference in sex development are also included. These populations also encompass those who do not self-identify with one of these terms but whose sexual orientation, gender identity or expression, or reproductive development is characterized by non-binary constructs of sexual orientation, gender, and/or sex. **Source:** U.S. Department of Health and Human Services. National Institutes of Health. (2022, December 8). Sex, gender, and Sexuality. National Institutes of Health. <https://www.nih.gov.nih-style-guide/sex-gender-sexuality>
21. Charmaraman, L., Hernandez, J., & Hodes, R. (2022). Marginalized and Understudied Populations Using Digital Media. In J. Nesi, E. Telzer, & M. Prinstein (Eds.), *Handbook of Adolescent Digital Media Use and Mental Health* (pp. 188-214). Cambridge: Cambridge University Press. <https://doi.org/10.1017/9781108976237.011>
22. Ybarra, M. L., Mitchell, K. J., Palmer, N. A., & Reisner, S. L. (2015). Online social support as a buffer against online and offline peer and sexual victimization among U.S. LGBT and non-LGBT youth. *Child abuse & neglect*, 39, 123-136. <https://doi.org/10.1016/j.chiabu.2014.08.006>
23. Berger, M. N., Taba, M., Marino, J. L., Lim, M. S. C., & Skinner, S. R. (2022). Social Media Use and Health and Well-being of Lesbian, Gay, Bisexual, Transgender, and Queer Youth: Systematic Review. *Journal of medical Internet research*, 24(9), e38449. <https://doi.org/10.2196/38449>
24. Nesi, J., Mann, S. and Robb, M. B. (2023). Teens and mental health: How girls really feel about social media. San Francisco, CA: Common Sense. Retrieved from https://www.common SenseMedia.org/sites/default/files/research/report/how-girls-really-feel-about-social-media-researchreport_final_1.pdf
25. Vogels, E., & Gelles-Watnick, R. (2023). Teens and social media: Key findings from Pew Research Center surveys. Pew Research Center: Internet, Science & Tech. United States of America. Retrieved from <https://www.pewresearch.org/short-reads/2023/04/24/teens-and-social-media-key-findings-from-pew-research-center-surveys/>
26. Kauer, S. D., Mangan, C., & Sanci, L. (2014). Do online mental health services improve help-seeking for young people? A systematic review. *Journal of medical Internet research*, 16(3), e66. <https://doi.org/10.2196/jmir.3103>
27. Rice, S. M., Goodall, J., Hetrick, S. E., Parker, A. G., Gilbertson, T., Amminger, G. P., Davey, C. G., McGorry, P. D., Gleeson, J., & Alvarez-Jimenez, M. (2014). Online and social networking interventions for the treatment of depression in young people: a systematic review. *Journal of medical Internet research*, 16(9), e206. <https://doi.org/10.2196/jmir.3304>
28. Ridout, B., & Campbell, A. (2018). The Use of Social Networking Sites in Mental Health Interventions for Young People: Systematic Review. *Journal of medical Internet research*, 20(12), e12244. <https://doi.org/10.2196/12244>
29. Kruzan, K. P., Williams, K. D. A., Meyerhoff, J., Yoo, D. W., O'Dwyer, L. C., De Choudhury, M., & Mohr, D. C. (2022). Social media-based interventions for adolescent and young adult mental health: A scoping review. *Internet interventions*, 30, 100578. <https://doi.org/10.1016/j.invent.2022.100578>
30. Riehm, K. E., Feder, K. A., Tormohlen, K. N., Crum, R. M., Young, A. S., Green, K. M., Pacek, L. R., La Flair, L. N., & Mojtabai, R. (2019). Associations Between Time Spent Using Social Media and Internalizing and Externalizing Problems Among US Youth. *JAMA psychiatry*, 76(12), 1266-1273. <https://doi.org/10.1001/jamapsychiatry.2019.2325>
31. Miech, R. A., Johnston, L. D., Bachman, J. G., O'Malley, P. M., Schulenberg, J. E., and Patrick, M. E. (2022). Monitoring the Future: A Continuing Study of American Youth (8th-and 10th-Grade Surveys), 2021. Inter-university Consortium for Political and Social Research [distributor]. <https://doi.org/10.3886/ICPSR38502.v1>
32. Braghieri, L., Levy, R., & Makarin, A. (2022). Social Media and Mental Health. *American Economic Review*, 112(11), 3660-3693. <https://pubs.aeaweb.org/doi/abs/10.1257/aer.20211218>
33. Doucleff, M. (2023, April 25). The Truth About Teens, Social Media and the Mental Health Crisis. NPR. Retrieved May 2, 2023, from <https://www.npr.org/sections/health-shots/2023/04/25/1171773181/social-media-teens-mental-health>
34. Hunt, M. G., Marx, R., Lipson, C., & Young, J. (2018). No more FOMO: Limiting social media decreases loneliness and depression. *Journal of Social and Clinical Psychology*, 37(10), 751-768. <https://doi.org/10.1521/jscp.2018.37.10.751>
35. From a mean Beck Depression Inventory (BDI) of 23 at baseline to a mean BDI of 14.5 at Week 4.
36. Allcott, H., Braghieri, L., Eichmeyer, S., & Gentzkow, M. (2020). The Welfare Effects of Social Media. *American Economic Review*, 110(3), 629-76. DOI: 10.1257/aer.20190658
37. Abi-Jaoude, E., Naylor, K. T., & Pignatiello, A. (2020). Smartphones, social media use and youth mental health. *Canadian Medical Association journal*, 192(6), E136-E141. <https://doi.org/10.1503/cmaj.190434>

38. Orben, A., & Przybylski, A. K. (2020). Reply to: Underestimating digital media harm. *Nature human behaviour*, 4(4), 349–351. <https://doi.org/10.1038/s41562-020-0840-y>
39. Twenge, J. M., Haidt, J., Lozano, J., & Cummins, K. M. (2022). Specification curve analysis shows that social media use is linked to poor mental health, especially among girls. *Acta psychologica*, 224, 103512. <https://doi.org/10.1016/j.actpsy.2022.103512>
40. Hamm, M. P., Newton, A. S., Chisholm, A., Shulhan, J., Milne, A., Sundar, P., Ennis, H., Scott, S. D., & Hartling, L. (2015). Prevalence and Effect of Cyberbullying on Children and Young People: A Scoping Review of Social Media Studies. *JAMA pediatrics*, 169(8), 770–777. <https://doi.org/10.1001/jamapediatrics.2015.0944>
41. Holland, G., & Tiggemann, M. (2016). A systematic review of the impact of the use of social networking sites on body image and disordered eating outcomes. *Body image*, 17, 100–110. <https://doi.org/10.1016/j.bodyim.2016.02.008>
42. Alonzo, R., Hussain, J., Stranges, S., & Anderson, K. K. (2021). Interplay between social media use, sleep quality, and mental health in youth: A systematic review. *Sleep medicine reviews*, 56, 101414. <https://doi.org/10.1016/j.smrv.2020.101414>
43. Kelly, Y., Zilanawala, A., Booker, C., & Sacker, A. (2019). Social Media Use and Adolescent Mental Health: Findings From the UK Millennium Cohort Study. *EClinicalMedicine*, 6, 59–68. <https://doi.org/10.1016/j.eclinm.2018.12.005>
44. Gelles-Watnick, R. (2022). Explicit Content, Time-wasting Are Key Social Media Worries For Parents Of U.S. Teens. Pew Research Center. United States of America. Retrieved from <https://www.pewresearch.org/fact-tank/2022/12/15/explicit-content-time-wasting-are-key-social-media-worries-for-parents-of-u-s-teens/>
45. Dyer C. (2022). Social media content contributed to teenager's death "in more than a minimal way," says coroner. *BMJ* (Clinical research ed.), 379, o2374. <https://doi.org/10.1136/bmj.o2374>
46. Carville, O. (2022, November 30). TikTok's Viral Challenges Keep Luring Young Kids to Their Deaths. Bloomberg. Retrieved from <https://www.bloomberg.com/news/features/2022-11-30/is-tiktok-responsible-if-kids-die-doing-dangerous-viral-challenges>
47. Sumner, S. A., Ferguson, B., Bason, B., Dink, J., Yard, E., Hertz, M., Hilker, B., Holland, K., Mercado-Crespo, M., Tang, S., & Jones, C. M. (2021). Association of Online Risk Factors With Subsequent Youth Suicide-Related Behaviors in the US. *JAMA network open*, 4(9), e2125860. <https://doi.org/10.1001/jamanetworkopen.2021.25860>
48. Dyson, M. P., Hartling, L., Shulhan, J., Chisholm, A., Milne, A., Sundar, P., Scott, S. D., & Newton, A. S. (2016). A Systematic Review of Social Media Use to Discuss and View Deliberate Self-Harm Acts. *PLoS one*, 11(5), e0155813. <https://doi.org/10.1371/journal.pone.0155813>
49. Lonergan, A. R., Bussey, K., Fardouly, J., Griffiths, S., Murray, S. B., Hay, P., Mond, J., Trompeter, N., & Mitchison, D. (2020). Protect me from my selfie: Examining the association between photo-based social media behaviors and self-reported eating disorders in adolescence. *The International journal of eating disorders*, 53(5), 485–496. <https://doi.org/10.1002/eat.23256>
50. Meier, E. P., & Gray, J. (2014). Facebook photo activity associated with body image disturbance in adolescent girls. *Cyberpsychology, behavior and social networking*, 17(4), 199–206. <https://doi.org/10.1089/cyber.2013.0305>
51. Thai, H., Davis, C. G., Mahboob, W., Perry, S., Adams, A., & Goldfield, G. S. (2023). Reducing Social Media Use Improves Appearance and Weight Esteem in Youth With Emotional Distress. *Psychology of Popular Media*. 10.1037/ppm0000460.
52. Vogel, E. A., Rose, J. P., Roberts, L. R., & Eckles, K. (2014). Social comparison, social media, and self-esteem. *Psychology of Popular Media Culture*, 3(4), 206–222. <https://doi.org/10.1037/ppm0000047>
53. Nesi, J., & Prinstein, M. J. (2015). Using Social Media for Social Comparison and Feedback-Seeking: Gender and Popularity Moderate Associations with Depressive Symptoms. *Journal of abnormal child psychology*, 43(8), 1427–1438. <https://doi.org/10.1007/s10802-015-0020-0>
54. Appel, H., Gerlach, A. L., & Crusius, J. (2016). The Interplay Between Facebook Use, Social Comparison, Envy, And Depression. *Current Opinion in Psychology*, 9, 44–49. <https://doi.org/10.1016/j.copsyc.2015.10.006>
55. Kleemans, M., Daalmans, S., Carbaat, I., & Anschütz, D. (2018). Picture Perfect: The Direct Effect Of Manipulated Instagram Photos On Body Image In Adolescent Girls. *Media Psychology*, 21(1), 93–110. <https://doi.org/10.1080/15213269.2016.1257392>
56. Mabe, A. G., Forney, K. J., & Keel, P. K. (2014). Do You “Like” My Photo? Facebook Use Maintains Eating Disorder Risk. *The International journal of eating disorders*, 47(5), 516–523. <https://doi.org/10.1002/eat.22254>
57. Bickham, D.S., Hunt, E., Bediou, B., & Rich, M. (2022). Adolescent Media Use: Attitudes, Effects, and Online Experiences. Boston, MA: Boston Children's Hospital Digital Wellness Lab. Retrieved from https://digitalwellnesslab.org/wp-content/uploads/Pulse-Survey_Adolescent-Attitudes-Effects-and-Experiences.pdf
58. Rideout, V., & Robb, M. B. (2018). Social media, social life: Teens reveal their experiences. San Francisco, CA: Common Sense Media. Retrieved from <https://www.common Sense Media.org/sites/default/files/research/report/2018-social-media-social-life-executive-summary-web.pdf>
59. Alhajji, M., Bass, S., & Dai, T. (2019). Cyberbullying, Mental Health, and Violence in Adolescents and Associations With Sex and Race: Data From the 2015 Youth Risk Behavior Survey. *Global pediatric health*, 6, 2333794X19868887. <https://doi.org/10.1177/2333794X19868887>

60. Rice, E., Petering, R., Rhoades, H., Winetrobe, H., Goldbach, J., Plant, A., Montoya, J., & Kordic, T. (2015). Cyberbullying perpetration and victimization among middle-school students. *American journal of public health*, 105(3), e66–e72. <https://doi.org/10.2105/AJPH.2014.302393>
61. Vogels, E. (2022). Teens and Cyberbullying 2022. Pew Research Center: Internet, Science & Tech. United States of America. Retrieved from <https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/>
62. Wolak, J., Finkelhor, D., Walsh, W., & Treitman, L. (2018). Sextortion of Minors: Characteristics and Dynamics. *The Journal of adolescent health*, 62(1), 72–79. <https://doi.org/10.1016/j.jadohealth.2017.08.014>
63. Federal Bureau of Investigations. (2022, December 19). FBI and Partners Issue National Public Safety Alert on Financial Sextortion Schemes. FBI. Retrieved from <https://www.fbi.gov/news/press-releases/fbi-and-partners-issue-national-public-safety-alert-on-financial-sex-tortion-schemes>
64. U.S. Drug Enforcement Administration. (2021, July 23). DEA Washington warns of deadly counterfeit drugs on social media. DEA. Retrieved from <https://www.dea.gov/stories/2021/2021-07/2021-07-23/counterfeit-drugs-social-media>
65. Finkelhor, D., Turner, H.A., & Colburn, D. (2023). Which dynamics make online child sexual abuse and cyberstalking more emotionally impactful: Perpetrator identity and images? *Child Abuse & Neglect*, 137, 106020. <https://doi.org/10.1016/j.chiabu.2023.106020>
66. Finkelhor, D., Turner, H., & Colburn, D. (2022). Prevalence of Online Sexual Offenses Against Children in the US. *JAMA network open*, 5(10), e2234471. <https://doi.org/10.1001/jamanetworkopen.2022.34471>
67. 5Rights Foundation. (2021). Pathways: How Digital Design Puts Children At Risk. Retrieved from <https://5rightsfoundation.com/uploads/Pathways-how-digital-design-puts-children-at-risk.pdf>
68. Kuss, D. J., & Griffiths, M. D. (2011). Online social networking and addiction--a review of the psychological literature. *International journal of environmental research and public health*, 8(9), 3528–3552. <https://doi.org/10.3390/ijerph8093528>
69. Griffiths, M.D. (2018). Adolescent social networking: How do social media operators facilitate habitual use? *Education and Health*, 36(3), 66–69. Retrieved from <https://sheu.org.uk/sheux/EH/eh363mdg.pdf>
70. Marino, C., Gini, G., Vieno, A., & Spada, M. M. (2018). The associations between problematic Facebook use, psychological distress and well-being among adolescents and young adults: A systematic review and meta-analysis. *Journal of affective disorders*, 226, 274–281. <https://doi.org/10.1016/j.jypmed.2020.106270>
71. Allcott, H., Gentzkow, M., & Song, L. (2022). Digital Addiction. *American Economic Review*, 112 (7): 2424–63. <https://doi.org/10.1257/aer.20210867>
72. Andreassen, C. S. (2015). Online Social Network Site Addiction: A Comprehensive Review. *Current Addiction Reports*, 2, 175–184. <https://doi.org/10.1007/s40429-015-0056-9>
73. He, Q., Turel, O., & Bechara, A. (2017). Brain anatomy alterations associated with Social Networking Site (SNS) addiction. *Scientific reports*, 7, 45064. <https://doi.org/10.1038/srep45064>
74. Montag, C., Markowitz, A., Blaszkiewicz, K., Andone, I., Lachmann, B., Sariyska, R., Trendafilov, B., Eibes, M., Kolb, J., Reuter, M., Weber, B., & Markett, S. (2017). Facebook Usage On Smartphones And Gray Matter Volume Of The Nucleus Accumbens. *Behavioural Brain Research*, 329, 221–228. <https://doi.org/10.1016/j.bbr.2017.04.035>
75. Shannon, H., Bush, K., Villeneuve, P. J., Hellemans, K. G., & Guimond, S. (2022). Problematic Social Media Use in Adolescents and Young Adults: Systematic Review and Meta-analysis. *JMIR mental health*, 9(4), e33450. <https://doi.org/10.2196/33450>
76. Boer, M., Stevens, G., Finkenauer, C., & van den Eijnden, R. (2020). Attention deficit hyperactivity disorder-symptoms, social media use intensity, and social media use problems in adolescents: Investigating directionality. *Child Development*, 91(4), e853–e865. <https://doi.org/10.1111/cdev.13334>
77. Franchina, V., Vanden Abeele, M., van Rooij, A. J., Lo Coco, G., & De Marez, L. (2018). Fear of Missing Out as a Predictor of Problematic Social Media Use and Phubbing Behavior among Flemish Adolescents. *International Journal Of Environmental Research And Public Health*, 15(10), 2319. <https://doi.org/10.3390/ijerph15102319>
78. Telzer, E. H., Goldenberg, D., Fuligni, A. J., Lieberman, M. D., & Gálvan, A. (2015). Sleep variability in adolescence is associated with altered brain development. *Developmental cognitive neuroscience*, 14, 16–22. <https://doi.org/10.1016/j.dcn.2015.05.007>
79. Liu, R. T., Steele, S. J., Hamilton, J. L., Do, Q. B. P., Furbish, K., Burke, T. A., Martinez, A. P., & Gerlus, N. (2020). Sleep and suicide: A systematic review and meta-analysis of longitudinal studies. *Clinical psychology review*, 81, 101895. <https://doi.org/10.1016/j.cpr.2020.101895>
80. Shochat, T., Cohen-Zion, M., & Tzischinsky, O. (2014). Functional consequences of inadequate sleep in adolescents: a systematic review. *Sleep medicine reviews*, 18(1), 75–87. <https://doi.org/10.1016/j.smrv.2013.03.005>
81. Dekkers, T. J., & van Hoorn, J. (2022). Understanding Problematic Social Media Use in Adolescents with Attention-Deficit/Hyperactivity Disorder (ADHD): A Narrative Review and Clinical Recommendations. *Brain Sciences*, 12(12), 1625. <https://doi.org/10.3390/brainsci12121625>
82. Ra, C. K., Cho, J., Stone, M. D., De La Cerda, J., Goldenson, N. I., Moroney, E., Tung, I., Lee, S. S., & Leventhal, A. M. (2018). Association of Digital Media Use With Subsequent Symptoms of Attention-Deficit/Hyperactivity Disorder Among Adolescents. *JAMA*, 320(3), 255–263. <https://doi.org/10.1001/jama.2018.8931>
83. Przybylski A. K., Murayama K., DeHaan C.R., & Gladwell V. (2013). Motivational, emotional, and behavioral correlates of fear of missing out. *Computers in Human Behavior*; 29:1841–1848.

84. Fioravanti, G., Casale, S., Benucci, S.B., Probst, A., Falone, A., Ricca, V., & Rotella, F. (2021). Fear of missing out and social networking sites use and abuse: A meta-analysis. *Computers in Human Behavior*, 122, 106839. <https://doi.org/10.1016/j.chb.2021.106839>
85. Odgers, C. L., & Jensen, M. R. (2020). Annual Research Review: Adolescent mental health in the digital age: facts, fears, and future directions. *Journal of Child Psychology and Psychiatry*, and Allied Disciplines, 61(3), 336–348. <https://doi.org/10.1111/jcpp.13190>
86. Office of the Surgeon General (OSG). (2021). Protecting Youth Mental Health: The U.S. Surgeon General's Advisory. U.S. Department of Health and Human Services. Retrieved from <https://www.hhs.gov/sites/default/files/surgeon-general-youth-mental-health-advisory.pdf>
87. Odgers, C.L., Allen, N.B., Pfeifer, J.H., Dahl, R.E., Nesi, J., Schueller, S.M., Williams, J. L., & the National Scientific Council on Adolescence (2022). Engaging, safe, and evidence-based: What science tells us about how to promote positive development and decrease risk in online spaces, Council Report No 2. doi: 10.31234/osf.io/rvn8q
88. Clark, S. J., Schultz, S. L., Gebremariam, A., Singer, D. C., & Freed, G. L. (2021). Sharing too soon? Children and social media apps. C.S. Mott Children's Hospital National Poll on Children's Health, University of Michigan, 39(4). Retrieved from https://mottpoll.org/sites/default/files/documents/101821_SocialMedia.pdf
89. Auxier, B., Anderson, M., Perrin, A., & Turner, E. (2020). Parenting Children in the Age of Screens. Pew Research Center: Internet, Science & Tech. Retrieved from <https://www.pewresearch.org/internet/2020/07/28/parenting-children-in-the-age-of-screens/>
90. U.S. Consumer Product Safety Commission. (n.d.). Toy Safety Business Guidance & Small Entity Compliance Guide. U.S. Consumer Product Safety Commission. Retrieved from <https://www.cpsc.gov/Business--Manufacturing/Business-Education/Toy-Safety-Business-Guidance-and-Small-Entity-Compliance-Guide>
91. United States Department of Transportation. (n.d.). National Highway Traffic Safety Administration. Retrieved from <https://www.nhtsa.gov/>
92. U.S. Food and Drug Administration. (n.d.). Center for Drug Evaluation and Research. U.S. Food and Drug Administration. Retrieved from <https://www.fda.gov/drugs>
93. Australian Government, eSafety Commissioner. (nd). Safety by Design. Retrieved from <https://www.esafety.gov.au/industry/safety-by-design>
94. Information Commissioner's Office. (nd). Introduction To The Age Appropriate Design Code. Retrieved from <https://ico.org.uk/for-organisations/childrens-code-hub/>
95. Perrino, J. (2022, July 27). Using "Safety By Design" To Address Online Harms. Brookings Institute. <https://www.brookings.edu/techstream/using-safety-by-design-to-address-online-harms/>
96. Lenhart, A., & Owens, K. (2021). The Unseen Teen: The Challenges of Building Healthy Tech for Young People. Data & Society. Retrieved from <https://datasociety.net/library/the-unseen-teen/>
97. American Academy of Pediatrics (AAP). (2018, October 8). Kids & Tech: Tips for parents in the Digital age. *HealthyChildren.org*. Retrieved from <https://www.healthychildren.org/English/family-life/Media/Pages/Tips-for-Parents-Digital-Age.aspx>
98. Morgan Stanley Alliance For Children's Mental Health & Child Mind Institute. (2022, May). How to set limits on screen time and internet use. Retrieved from <https://www.morganstanley.com/assets/pdfs/setting-limits-on-screen-time-tip-sheet.pdf>
99. Ehmke, R. (2023, March 13). How using social media affects teenagers. Child Mind Institute. Retrieved from <https://childmind.org/article/how-using-social-media-affects-teenagers/>
100. American Psychological Association. (2019, December 12). Digital Guidelines: Promoting healthy technology use for children. American Psychological Association. Retrieved from <https://www.apa.org/topics/social-media-internet/technology-use-children>
101. US Department of Health and Human Services, Assistant Secretary for Public Affairs (ASPA). (2021, November 10). Prevent cyberbullying. *StopBullying.gov*. Retrieved from <https://www.stopbullying.gov/cyberbullying/prevention> <https://www.stopbullying.gov/cyberbullying/how-to-report>
102. National Academies of Sciences, Engineering, and Medicine (NASEM). (n.d.). Assessment of the Impact of Social Media on the Health and Wellbeing of Adolescents and Children. Retrieved from <https://www.nationalacademies.org/our-work/assessment-of-the-impact-of-social-media-on-the-health-and-wellbeing-of-adolescents-and-children>
103. American Academy of Pediatrics. (2023, February 7). Center of Excellence on Social Media and Youth Mental Health. Retrieved from <https://www.aap.org/en/patient-care/media-and-children/center-of-excellence-on-social-media-and-youth-mental-health/#:~:text=What%20We%20Do,protect%20youth%20mental%20health%20online>
104. American Academy of Pediatrics. (2017). *Bright Futures Guidelines for Health Supervision of Infants, Children, and Adolescents* (4th ed., pp. 229-234). American Academy of Pediatrics. https://downloads.aap.org/AAP/PDF/Bright%20Futures/BF4_HealthySocialMedia.pdf



AMERICAN
PSYCHOLOGICAL
ASSOCIATION

AMERICAN PSYCHOLOGICAL ASSOCIATION

Health Advisory on Social Media Use in Adolescence

MAY 2023



Psychological scientists examine potential beneficial and harmful effects of social media^a use on adolescents' social, educational, psychological, and neurological development. This is a rapidly evolving and growing area of research with implications for many stakeholders (e.g., youth, parents, caregivers, educators, policymakers, practitioners, and members of the tech industry) who share responsibility to ensure adolescents' well-being.^b Officials and policymakers including the U.S. Surgeon General Dr. Vivek Murthy have documented the importance of this issue and are actively seeking science-informed input.^c The recommendations below are based on the scientific evidence to date, and the following considerations.

- A. Using social media is not inherently beneficial or harmful to young people. Adolescents' lives online both reflect and impact their offline lives. In most cases, the effects of social media are dependent on adolescents' own personal and psychological characteristics and social circumstances—intersecting with the specific content, features, or functions that are afforded within many social media platforms. In other words, the effects of social media likely depend on what teens can do and see online, teens' pre-existing strengths or vulnerabilities, and the contexts in which they grow up.³
- B. Adolescents' experiences online are affected by both 1) how they shape their own social media experiences (e.g., they choose whom to like and follow); and 2) both visible and unknown features built into social media platforms.
- C. Not all findings apply equally to all youth. Scientific findings offer one piece of information that can be used along with knowledge of specific youths' strengths, weaknesses, and context to make decisions that are tailored for each teen, family, and community.⁴
- D. Adolescent development is gradual and continuous, beginning with biological and neurological changes occurring before puberty is observable (i.e., approximately beginning at 10 years of age), and lasting at least until dramatic changes in youths' social environment (e.g., peer, family, and school context) and neurological changes have completed (i.e., until approximately 25 years of age).⁵ Age-appropriate use of social media should be based on each adolescent's level of maturity (e.g., self-regulation skills, intellectual development, comprehension of risks) and home environment.⁶ Because adolescents mature at different rates, and because there are no data available to indicate that children become unaffected by the potential risks and opportunities posed by social media usage at a specific age, research is in development to specify a single time or age point for many of these recommendations. In general, potential risks are likely to be greater in early adolescence—a period of greater biological, social, and psychological transitions, than in late adolescence and early adulthood.^{7,8}
- E. As researchers have found with the internet more broadly, racism (i.e., often reflecting perspectives of those building technology) is built into social media platforms. For example, algorithms (i.e., a set of mathematical instructions that direct users' everyday experiences down to the posts that they see) can often have centuries of racist policy and discrimination encoded.⁹ Social media can become an incubator, providing community and training that fuel racist hate.¹⁰ The resulting potential impact is far reaching, including physical violence offline, as well as threats to well-being.¹¹
- F. These recommendations are based on psychological science and related disciplines at the time of this writing (April 2023). Collectively, these studies were conducted with thousands of adolescents who completed standardized assessments of social, behavioral, psychological, and/or neurological functioning, and also reported (or were observed) engaging with specific social media functions or content. However, these studies do have limitations. First, findings suggesting causal associations are rare, as the data required to make cause-and-effect conclusions are challenging to collect and/or may be available within technology companies, but have not been made accessible to independent scientists. Second, *long-term* (i.e., multi-year) longitudinal research often is unavailable; thus, the associations between adolescents' social media use and long-term outcomes (i.e., into adulthood) are largely unknown. Third, relatively few studies have been conducted with marginalized populations of youth, including those from marginalized racial, ethnic, sexual, gender, socioeconomic backgrounds, those who are differently abled, and/or youth with chronic developmental or health conditions.

a These recommendations do not address the use of all technology among youth, including educationally-based platforms or digital interventions that use evidence-based approaches to promote adaptive health outcomes. Rather, these recommendations reflect the literature on social media specifically, which is defined as technologically-based applications, platforms, or communication systems using online architecture that promotes asynchronous, unilateral, permanent, public, continually-accessible, social cue-restricted, quantifiable, visually-based, or algorithmic-based social interactions.^{1,2}

b These recommendations enact policies and resolutions approved by the APA Council of Representatives including the [APA Resolution on Child and Adolescent Mental and Behavioral Health](#) and the [APA Resolution on Dismantling Systemic Racism](#) in contexts including social media. These are not professional practice guidelines but are intended to provide information based on psychological science.

c The U.S. Surgeon General released an [Advisory](#) in 2021 focused on Protecting Youth Mental Health that recognizes the importance of examining the impacts of social media on children.

RECOMMENDATIONS



Youth using social media should be encouraged to use functions that create opportunities for social support, online companionship, and emotional intimacy that can promote healthy socialization.

- Data suggest that youths' psychological development may benefit from this type of online social interaction, particularly during periods of social isolation, when experiencing stress, when seeking connection to peers with similar developmental and/or health conditions, and perhaps especially for youth who experience adversity or isolation in offline environments.^{12,13,14,15}
- Youth with symptoms of mental illness, such as adolescents with social anxiety, depression, or loneliness, for instance, may benefit from interactions on social media that allow for greater control, practice, and review of social interactions.¹⁶ Unfortunately, these populations may also be at higher risk for some of the negative facets of social media use as discussed below.¹⁷
- Social media offers a powerful opportunity for socialization of specific attitudes and behaviors, encouraging adolescents to follow the opinions and prosocial acts of others.¹⁸ The discussion of healthy behaviors online can promote or reinforce positive offline activity and healthy outcomes.
- Social media may be psychologically beneficial particularly among those experiencing mental health crises,¹⁹ or members of marginalized groups that have been disproportionately harmed in online contexts. For instance, access to peers that allows LGBTQIA+ and questioning adolescents to provide support to and share accurate health information with one another is beneficial to psychological development, and can protect youth from negative psychological outcomes when experiencing stress.²⁰ This may be especially important for topics that adolescents feel reluctant to or are unable to discuss with a parent or caregiver.

Access to peers that allows LGBTQIA+ and questioning adolescents to provide support to and share accurate health information with one another can protect youth from negative psychological outcomes when experiencing stress

Social media use, functionality, and permissions/consenting should be tailored to youths' developmental capabilities; designs created for adults may not be appropriate for children.

- Specific features (e.g., the “like” button, recommended content, unrestricted time limits, endless scrolling) and notices/alerts (e.g., regarding changes to privacy policies) should be tailored to the social and cognitive abilities and comprehension of adolescent users.²¹ As one example, adolescents should be informed explicitly and repeatedly, in age-appropriate ways, about the manner in which their behaviors on social media may yield data that can be used, stored, or shared with others, for instance, for commercial (and other) purposes.

In early adolescence (i.e., typically 10-14 years), adult monitoring (i.e., ongoing review, discussion, and coaching around social media content) is advised for most youths' social media use; autonomy may increase gradually as kids age and if they gain digital literacy skills. However, monitoring should be balanced with youths' appropriate needs for privacy.

- Brain regions associated with a desire for attention, feedback, and reinforcement from peers become increasingly sensitive beginning in early adolescence, and regions associated with mature self-control are not fully developed until adulthood.⁵ Parental monitoring (i.e., coaching and discussion) and developmentally appropriate limit-setting thus is critical, especially in early adolescence.
- Adults' own use of social media in youths' presence should also be carefully considered. Science demonstrates that adults' (e.g., caregivers') orientation and attitudes toward social media (e.g., using during interactions with their children, being distracted from in-person interactions by social media use) may affect adolescents' own use of social media.
- Preliminary research suggests that *a combination of* 1) social media limits and boundaries, and 2) adult-child discussion and coaching around social media use, leads to the best outcomes for youth.²²

Adolescents should be informed explicitly and repeatedly, in age-appropriate ways, about the manner in which their behaviors on social media may yield data that can be used, stored, or shared with others



RECOMMENDATIONS *(continued)*

To reduce the risks of psychological harm, adolescents' exposure to content on social media that depicts illegal or psychologically maladaptive behavior, including content that instructs or encourages youth to engage in health-risk behaviors, such as self-harm (e.g., cutting, suicide), harm to others, or those that encourage eating-disordered behavior (e.g., restrictive eating, purging, excessive exercise) should be minimized, reported, and removed²³; moreover, technology should not drive users to this content.

- Evidence suggests that exposure to maladaptive behavior may promote similar behavior among vulnerable youth, and online social reinforcement of these behaviors may be related to increased risk for serious psychological symptoms, even after controlling for offline influences.²⁴
- Reporting structures should be created to easily identify harmful content, and ensure it is deprioritized or removed.

To minimize psychological harm, adolescents' exposure to "cyberhate" including online discrimination, prejudice, hate, or cyberbullying especially directed toward a marginalized group (e.g., racial, ethnic, gender, sexual, religious, ability status),²² or toward an individual because of their identity or allyship with a marginalized group should be minimized.

- Research demonstrates that adolescents' exposure to online discrimination and hate predicts increases in anxiety and depressive symptoms, even after controlling for how much adolescents are exposed to similar experiences offline.²⁵ Similarly, research indicates that as compared to offline bullying, online bullying and harassment can be more severe, and thus damaging to psychological development.^{26,27,28} In other words, both online cyberhate and offline bullying can increase risk for adolescent mental health problems. Research suggests elevated risks both for the perpetrators and victims of cyberhate.^{29,30}
- Adolescents should be trained to recognize online structural racism and critique racist messages. Research shows that young people who are able to critique racism experience less psychological distress when they witness race-related traumatic events online.²⁵ As noted above, adults' monitoring and active discussion of online content can also reduce the effects of exposure to cyberhate on adolescents' psychological adjustment.²²



Research demonstrates that adolescents' exposure to online discrimination and hate predicts increases in anxiety and depressive symptoms.



Adolescents should be routinely screened for signs of “problematic social media use” that can impair their ability to engage in daily roles and routines, and may present risk for more serious psychological harms over time.

- Indicators of problematic social media use include a) a tendency to use social media even when adolescents want to stop, or realize it is interfering with necessary tasks; b) spending excessive effort to ensure continuous access to social media; c) strong cravings to use social media, or disruptions in other activities from missing social media use too much; d) repeatedly spending more time on social media than intended; e) lying or deceptive behavior to retain access to social media use; f) loss or disruption of significant relationships or educational opportunities because of media use.³¹
- Social media use should not restrict opportunities to practice in-person reciprocal social interactions, and should not contribute to psychological avoidance of in-person social interactions.

The use of social media should be limited so as to not interfere with adolescents’ sleep and physical activity.

- Research recommends adolescents get at least 8 hours of sleep each night and maintain regular sleep-wake schedules.³² Data indicate that technology use particularly within 1 hour of bedtime, and social media use in particular, is associated with sleep disruptions.^{33,34} Insufficient sleep is associated with disruptions to neurological development in adolescent brains, teens’ emotional functioning,^{35,36} and risk for suicide.^{37,38}
- Adolescents’ social media use also should not interfere with or reduce adolescents’ opportunities for physical activity and exercise.³⁹ Research demonstrates that physical activity is essential for both physical and psychological health (i.e., lower rates of depression).⁴⁰

Insufficient sleep is associated with disruptions to neurological development in adolescent brains, teens’ emotional functioning, and risk for suicide

RECOMMENDATIONS *(continued)*

Adolescents should limit use of social media for social comparison, particularly around beauty- or appearance-related content.

- Research suggests that using social media for social comparisons related to physical appearance, as well as excessive attention to and behaviors related to one's own photos and feedback on those photos, are related to poorer body image, disordered eating, and depressive symptoms, particularly among girls.^{41,42,43,44,45,46}

Adolescents' social media use should be preceded by training in *social media literacy* to ensure that users have developed psychologically-informed competencies and skills that will maximize the chances for balanced, safe, and meaningful social media use.

- Emerging science offers preliminary support for the efficacy of Digital Citizenship and Digital Literacy to increase the frequency of positive interactions online⁴⁷; however, more research is needed in this area.⁴⁸
- Additional competencies could also include: 1) questioning the accuracy and representativeness of social media content; 2) understanding the tactics used to spread mis- and disinformation; 3) limiting "overgeneralization" and "mises-timation" errors that lead users to incorrectly estimate others' behaviors or attitudes based on social media content (or reactions to content); 4) signs of problematic social media use; 5) how to build and nourish healthy online relationships; 6) how to solve conflicts that can emerge on social media platforms; 7) how to refrain from excessive social comparisons online and/or better understand how images and content can be manipulated; 8) as noted above, how to recognize online structural racism and critique racist messages; and 9) how to safely communicate about mental health online.⁴⁹

Substantial resources should be provided for continued scientific examination of the positive and negative effects of social media on adolescent development.

- A substantial investment in research funding is needed, including long-term longitudinal research, studies of younger children, and research on marginalized populations.
- Access to data among independent scientists (including data from tech companies) to more thoroughly examine the associations between social media use and adolescent development is needed.



A substantial investment in research funding is needed, including long-term longitudinal research, studies of younger children, and research on marginalized populations.

EXPERT ADVISORY PANEL

Co-Chairs

Mary Ann McCabe, PhD, ABPP, Member-at-large, Board of Directors, American Psychological Association; associate clinical professor of pediatrics, George Washington University School of Medicine

Mitchell J. Prinstein, PhD, ABPP, Chief science officer, American Psychological Association; John Van Seters Distinguished Professor of Psychology and Neuroscience, University of North Carolina at Chapel Hill

Members

Mary K. Alvord, PhD, director, Alvord, Baker & Associates; board president, Resilience Across Borders; adjunct associate professor of psychiatry and behavioral sciences, The George Washington University School of Medicine and Health Sciences

Dawn T. Bounds, PhD, PMHNP-BC, FAAN, assistant professor, Sue & Bill Gross School of Nursing, University of California, Irvine

Linda Charmaraman, PhD, Wellesley Centers for Women, Wellesley College

Sophia Choukas-Bradley, PhD, assistant professor, Department of Psychology, University of Pittsburgh

Dorothy L. Espelage, PhD, William C. Friday Distinguished Professor of Education, University of North Carolina at Chapel Hill

Joshua A. Goodman, PhD, assistant professor, Department of Psychology, Southern Oregon University

Jessica L. Hamilton, PhD, assistant professor, Department of Psychology, Rutgers University

Jacqueline Nesi, PhD, assistant professor, Department of Psychiatry and Human Behavior, Alpert Medical School of Brown University

Brendesha M. Tynes, PhD, Dean's Professor of Educational Equity, University of Southern California

L. Monique Ward, PhD, professor, Department of Psychology (Developmental), University of Michigan

Lucía Magis-Weinberg, MD, PhD, assistant professor, Department of Psychology, University of Washington

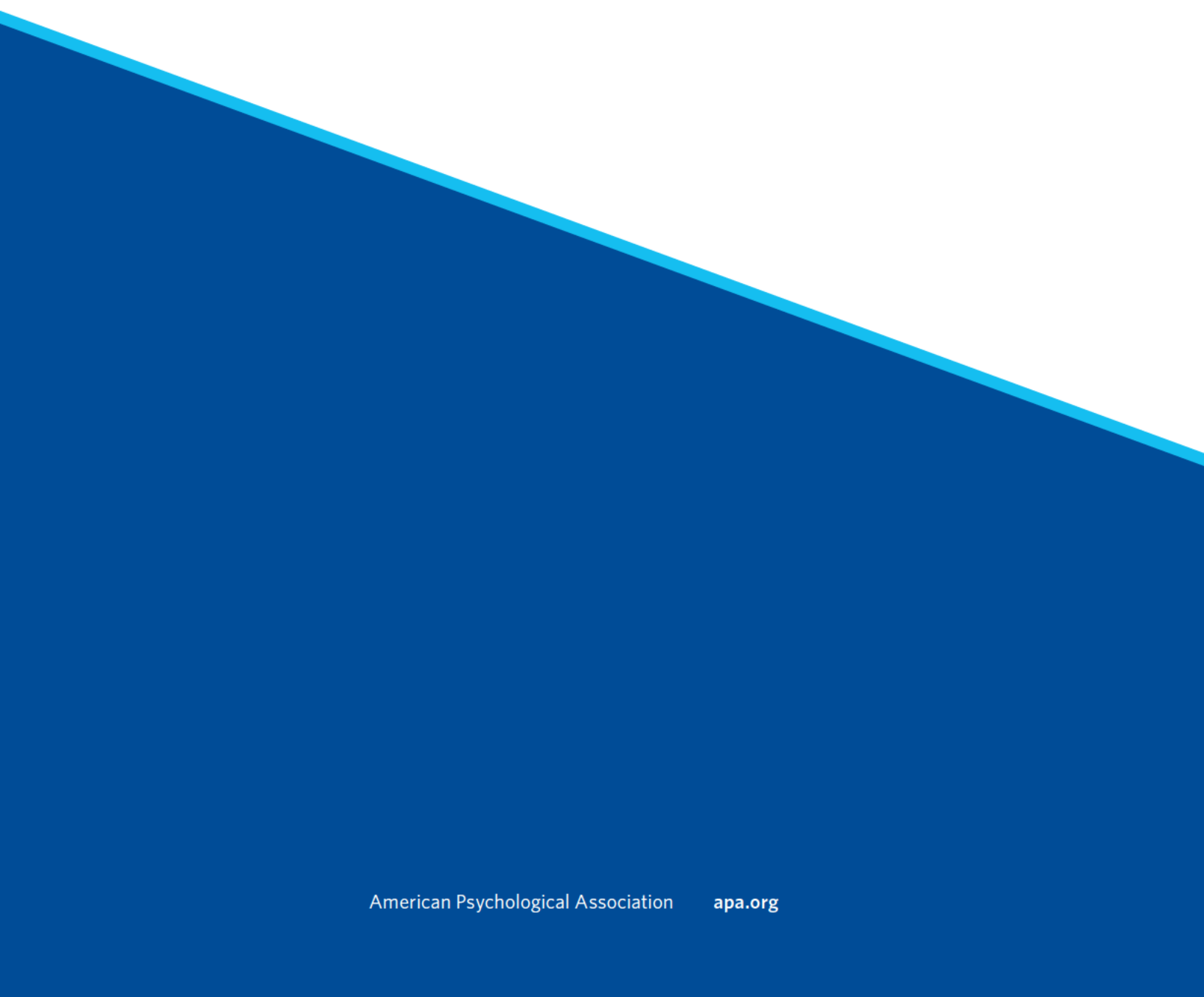
Acknowledgements

We wish to acknowledge the outstanding contributions to this report made by Corbin Evans, JD, Senior Director of Congressional & Federal Relations, American Psychological Association.

SELECTED PUBLICATIONS AND RESOURCES

- Nesi J, Choukas-Bradley S, Prinstein MJ. Transformation of Adolescent Peer Relations in the Social Media Context: Part 1-A Theoretical Framework and Application to Dyadic Peer Relationships. *Clin Child Fam Psychol Rev*. 2018;21(3):267-294. doi:10.1007/s10567-018-0261-x
- Nesi J, Dredge R, Maheux AJ, Roberts SR, Fox KA, Choukas-Bradley S. Peer experiences via social media. In: *Encyclopedia of Child and Adolescent Health*. Elsevier; 2023:182-195. doi:10.1016/B978-0-12-818872-9.00046-7
- Prinstein MJ, Nesi J, Telzer EH. Commentary: An updated agenda for the study of digital media use and adolescent development - future directions following Odgers & Jensen (2020). *J Child Psychol Psychiatry*. 2020;61(3):349-352. doi:10.1111/jcpp.13219
- Valkenburg PM, Peter J. The differential susceptibility to media effects model. *J Commun*. 2013;63(2):221-243. doi:10.1111/jcom.12024
- Somerville LH, Casey BJ. Developmental neurobiology of cognitive control and motivational systems. *Curr Opin Neurobiol*. 2010;20(2):236-241. doi:10.1016/j.conb.2010.01.006
- Orben A, Blakemore S-J. How social media affects teen mental health: a missing link. *Nature*. 2023;614(7948):410-412. doi:10.1038/d41586-023-00402-9
- Magis-Weinberg L, Ballonoff Suleiman A, Dahl RE. Context, development, and digital media: implications for very young adolescents in Imics. *Front Psychol*. 2021;12:632713. doi:10.3389/fpsyg.2021.632713
- Orben A, Przybylski AK, Blakemore S-J, Kievit RA. Windows of developmental sensitivity to social media. *Nat Commun*. 2022;13(1):1649. doi:10.1038/s41467-022-29296-3
- Noble SU. *Algorithms of Oppression: How Search Engines Reinforce Racism*. NYU Press; 2018. doi:10.2307/j.ctt1pwt9w5
- Relia K, Li Z, Cook SH, Chunara R. Race, Ethnicity and National Origin-Based Discrimination in Social Media and Hate Crimes across 100 U.S. Cities. *ICWSM*. 2019;13:417-427. doi:10.1609/icwsm.v13i01.3354
- Tynes BM, Willis HA, Stewart AM, Hamilton MW. Race-Related Traumatic Events Online and Mental Health Among Adolescents of Color. *J Adolesc Health*. 2019;65(3):371-377. doi:10.1016/j.jadohealth.2019.03.006
- Charmaraman L, Lynch AD, Richer AM, Zhai E. Examining Early Adolescent Positive and Negative Social Technology Behaviors and Well-being During the COVID-19 Pandemic. *Technology, Mind, and Behavior*. 2022;3(1). doi:10.1037/tmb0000062
- Magis-Weinberg L, Gys CL, Berger EL, Domoff SE, Dahl RE. Positive and Negative Online Experiences and Loneliness in Peruvian Adolescents During the COVID-19 Lockdown. *J Res Adolesc*. 2021;31(3):717-733. doi:10.1111/jora.12666
- Psihogios AM, Ahmed AM, McKelvey ER, et al. Social media to promote treatment adherence among adolescents and young adults with chronic health conditions: A topical review and TikTok application. *Clin Pract Pediatr Psychol*. 2022;10(4):440-451. doi:10.1037/cpp0000459
- Holtz BE, Kanthawala S. #T1DLooksLikeMe: Exploring Self-Disclosure, Social Support, and Type 1 Diabetes on Instagram. *Front Commun*. 2020;5. doi:10.3389/fcomm.2020.510278
- Chassiakos YLR, Radesky J, Christakis D, Moreno MA, Cross C, COUNCIL ON COMMUNICATIONS AND MEDIA. Children and adolescents and digital media. *Pediatrics*. 2016;138(5). doi:10.1542/peds.2016-2593
- Nesi, J., Mann, S. and Robb, M. B. (2023). Teens and mental health: How girls really feel about social media. San Francisco, CA: Common Sense
- Armstrong-Carter E, Telzer EH. Advancing measurement and research on youths' prosocial behavior in the digital age. *Child Dev Perspect*. 2021;15(1):31-36. doi:10.1111/cdep.12396
- Massing-Schaffer M, Nesi J, Telzer EH, Lindquist KA, Prinstein MJ. Adolescent Peer Experiences and Prospective Suicidal Ideation: The Protective Role of Online-Only Friendships. *J Clin Child Adolesc Psychol*. 2022;51(1):49-60. doi:10.1080/1537444.2020.1750019
- Craig SL, Eaton AD, McInroy LB, Leung VWY, Krishnan S. Can Social Media Participation Enhance LGBTQ+ Youth Well-Being? Development of the Social Media Benefits Scale. *Social Media + Society*. 2021;7(1):205630512198893. doi:10.1177/2056305121988931
- Introduction to the Age appropriate design code. (2022, October 17). Ico.org.uk. <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-code/#:~:text=The%20Children>
- Wachs S, Costello M, Wright MF, et al. "DNT LET 'EM H8 U!": Applying the routine activity framework to understand cyberhate victimization among adolescents across eight countries. *Comput Educ*. 2021;160:104026. doi:10.1016/j.compedu.2020.104026
- Tools and tips to help communicate safely online about suicide - #chatsafe - Orygen, Revolution in Mind. (n.d.). www.orygen.org.au. Retrieved April 20, 2023, from <https://www.orygen.org.au/chatsafe>.
- Nesi J, Rothenberg WA, Hussong AM, Jackson KM. Friends' Alcohol-Related Social Networking Site Activity Predicts Escalations in Adolescent Drinking: Mediation by Peer Norms. *J Adolesc Health*. 2017;60(6):641-647. doi:10.1016/j.jadohealth.2017.01.009
- Tynes BM, Giang MT, Williams DR, Thompson GN. Online racial discrimination and psychological adjustment among adolescents. *J Adolesc Health*. 2008;43(6):565-569. doi:10.1016/j.jadohealth.2008.08.021

26. Mitchell KJ, Ybarra ML, Jones LM, Espelage D. What features make online harassment incidents upsetting to youth? *J Sch Violence*. 2016;15(3):279-301. doi:10.1080/15388220.2014.990462
27. Li C, Wang P, Martin-Moratinos M, Bella-Fernández M, Blasco-Fontecilla H. Traditional bullying and cyberbullying in the digital age and its associated mental health problems in children and adolescents: a meta-analysis. *Eur Child Adolesc Psychiatry*. December 31, 2022. doi:10.1007/s00787-022-02128-x
28. Gini G, Espelage DL. Peer victimization, cyberbullying, and suicide risk in children and adolescents. *JAMA*. 2014;312(5):545-546. doi:10.1001/jama.2014.3212
29. Fulantelli G, Taibi D, Scifo L, Schwarze V, Eimler SC. Cyberbullying and Cyberhate as Two Interlinked Instances of Cyber-Aggression in Adolescence: A Systematic Review. *Front Psychol*. 2022;13:909299. doi:10.3389/fpsyg.2022.909299
30. Castaño-Pulgarín SA, Suárez-Betancur N, Vega LMT, López HHM. Internet, social media and online hate speech. Systematic review. *Aggress Violent Behav*. 2021;58:101608. doi:10.1016/j.avb.2021.101608
31. Boer M, Stevens GWJM, Finkenauer C, van den Eijnden RJJM. The course of problematic social media use in young adolescents: A latent class growth analysis. *Child Dev*. 2022;93(2):e168-e187. doi:10.1111/cdev.13712
32. Paruthi S, Brooks LJ, D'Ambrosio C, et al. Recommended amount of sleep for pediatric populations: A consensus statement of the american academy of sleep medicine. *J Clin Sleep Med*. 2016;12(6):785-786. doi:10.5664/jcsm.5866
33. Alonzo R, Hussain J, Stranges S, Anderson KK. Interplay between social media use, sleep quality, and mental health in youth: A systematic review. *Sleep Med Rev*. 2021;56:101414. doi:10.1016/j.smrv.2020.101414
34. Hamilton JL, Chand S, Reinhardt L, et al. Social media use predicts later sleep timing and greater sleep variability: An ecological momentary assessment study of youth at high and low familial risk for depression. *J Adolesc*. 2020;83:122-130. doi:10.1016/j.adolescence.2020.07.009
35. Perrault AA, Bayer L, Peuvrier M, et al. Reducing the use of screen electronic devices in the evening is associated with improved sleep and daytime vigilance in adolescents. *Sleep*. 2019;42(9). doi:10.1093/sleep/zsz125
36. Telzer EH, Goldenberg D, Fuligni AJ, Lieberman MD, Gálvan A. Sleep variability in adolescence is associated with altered brain development. *Dev Cogn Neurosci*. 2015;14:16-22. doi:10.1016/j.dcn.2015.05.007
37. Hamilton JL, Tsypes A, Zelazny J, et al. Sleep influences daily suicidal ideation through affective reactivity to interpersonal events among high-risk adolescents and young adults. *J Child Psychol Psychiatry*. 2023;64(1):27-38. doi:10.1111/jcpp.13651
38. Liu RT, Steele SJ, Hamilton JL, et al. Sleep and suicide: A systematic review and meta-analysis of longitudinal studies. *Clin Psychol Rev*. 2020;81:101895. doi:10.1016/j.cpr.2020.101895
39. Shimoga SV, Erlyana E, Rebello V. Associations of Social Media Use With Physical Activity and Sleep Adequacy Among Adolescents: Cross-Sectional Survey. *J Med Internet Res*. 2019;21(6):e14290. doi:10.2196/14290
40. Bustamante EE, Santiago-Rodríguez ME, Ramer JD. Unlocking the promise of physical activity for mental health promotion. *JAMA Pediatr*. 2023;177(2):111-113. doi:10.1001/jamapediatrics.2022.5096
41. Nesi J, Miller AB, Prinstein MJ. Adolescents' Depressive Symptoms and Subsequent Technology-Based Interpersonal Behaviors: A Multi-Wave Study. *J Appl Dev Psychol*. 2017;51:12-19. doi:10.1016/j.appdev.2017.02.002
42. Nesi J, Prinstein MJ. Using Social Media for Social Comparison and Feedback-Seeking: Gender and Popularity Moderate Associations with Depressive Symptoms. *J Abnorm Child Psychol*. 2015;43(8):1427-1438. doi:10.1007/s10802-015-0020-0
43. Padín PF, González-Rodríguez R, Verde-Diego C, Vázquez-Pérez R. Social media and eating disorder psychopathology: A systematic review. *Cyberpsychology*. 2021;15(3). doi:10.5817/CP2021-3-6
44. Fioravanti G, Bocci Benucci S, Ceragioli G, Casale S. How the exposure to beauty ideals on social networking sites influences body image: A systematic review of experimental studies. *Adolesc Res Rev*. 2022;7(3):419-458. doi:10.1007/s40894-022-00179-4
45. Kleemans M, Daalmans S, Carbaat I, Anschütz D. Picture perfect: the direct effect of manipulated instagram photos on body image in adolescent girls. *Media Psychol*. 2016;21(1):1-18. doi:10.1080/15213269.2016.1257392
46. Maheux AJ, Roberts SR, Nesi J, Widman L, Choukas-Bradley S. Longitudinal associations between appearance-related social media consciousness and adolescents' depressive symptoms. *J Adolesc*. 2022;94(2):264-269. doi:10.1002/jad.12009
47. Common Sense Media. (2019, May 10). Digital citizenship | Common Sense Education. Common Sense Education. <https://www.commonsense.org/education/digital-citizenship>
48. Magis-Weinberg L, Muñoz Lopez DE, Gys CL, Berger EL, Dahl RE. Short Research Article: Promoting digital citizenship through a school-based intervention in early adolescence in Perú (a pilot quasi-experimental study). *Child Adolesc Ment Health*. 2023;28(1):83-89. doi:10.1111/camh.12625
49. Balt E, Mérelle S, Robinson J, et al. Social media use of adolescents who died by suicide: lessons from a psychological autopsy study. *Child Adolesc Psychiatry Ment Health*. 2023;17(1):48. doi:10.1186/s13034-023-00597-9



FOR RELEASE APRIL 22, 2025

Teens, Social Media and Mental Health

Most teens credit social media with feeling more connected to friends. Still, roughly 1 in 5 say social media sites hurt their mental health, and a growing share think they harm people their age

BY *Michelle Faverio, Monica Anderson and Eugenie Park*

FOR MEDIA OR OTHER INQUIRIES:

Monica Anderson, Director, Internet and
Technology Research

Jeffrey Gottfried, Associate Director, Research

Haley Nolan, Communications Manager

202.419.4372

www.pewresearch.org

RECOMMENDED CITATION

Pew Research Center, April 2025, "Teens, Social
Media and Mental Health"

About Pew Research Center

Pew Research Center is a nonpartisan, nonadvocacy fact tank that informs the public about the issues, attitudes and trends shaping the world. It does not take policy positions. The Center conducts public opinion polling, demographic research, computational social science research and other data-driven research. It studies politics and policy; news habits and media; the internet and technology; religion; race and ethnicity; international affairs; social, demographic and economic trends; science; research methodology and data science; and immigration and migration. Pew Research Center is a subsidiary of The Pew Charitable Trusts, its primary funder.

© Pew Research Center 2025

How we did this

Pew Research Center conducted this study to understand teens' experiences and attitudes around teen mental health and social media. Part of this study also examines parents' perspectives.

The Center conducted an online survey of 1,391 U.S. teens and parents from Sept. 18 to Oct. 10, 2024, through Ipsos. Ipsos recruited the teens via their parents, who were part of its [KnowledgePanel](#). The KnowledgePanel is a probability-based web panel recruited primarily through national, random sampling of residential addresses. Parents were asked to think about one teen in their household (if there were multiple teens ages 13 to 17 in the household, one was randomly chosen). At the conclusion of the parent's section, the parent was asked to have this chosen teen come to the computer and complete the survey in private.

The survey is weighted to be representative of two different populations: 1) parents with teens ages 13 to 17 and 2) teens ages 13 to 17 who live with parents. For each of these populations, the survey is weighted to be representative by age, gender, race and ethnicity, household income and other categories.

Here are [the questions among teens](#) and [among parents](#) used for this report, along with responses, and [the survey methodology](#).

This research was reviewed and approved by an external institutional review board (IRB), Advarra, an independent committee of experts specializing in helping to protect the rights of research participants.

Teens, Social Media and Mental Health

Most teens credit social media with feeling more connected to friends. Still, roughly 1 in 5 say social media sites hurt their mental health, and a growing share think they harm people their age

Rising rates of [poor mental health among youth](#) have been called a national crisis. While this is often linked to factors like the [COVID-19 pandemic or poverty](#), some officials, like former Surgeon General Vivek Murthy, name social media [as a major threat](#) to teenagers.

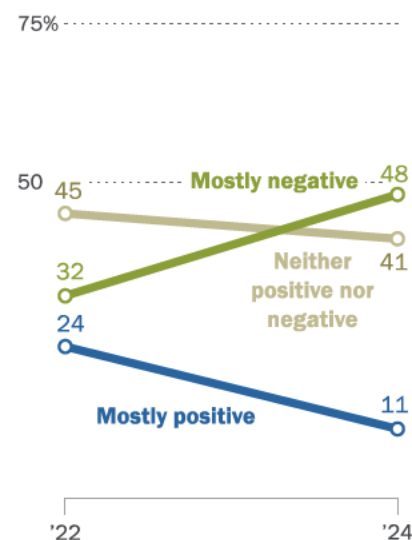
Our latest survey of U.S. teens ages 13 to 17 and their parents finds that parents are generally more worried than their children about the mental health of teenagers today.

And while both groups call out social media's impact on young people's well-being, parents are more likely to make this connection.¹

Still, teens are growing more wary of social media for their peers. Roughly half of teens (48%) say these sites have a mostly negative effect on people their age, up from 32% in 2022. But fewer (14%) think they negatively affect them personally.

48% of teens say social media harm people their age, up from 32% in 2022

% of U.S. teens ages 13 to 17 who say social media have (a) ___ effect on people their age



Note: Those who did not give an answer are not shown.

Source: Survey conducted Sept. 18-Oct. 10, 2024.

"Teens, Social Media and Mental Health"

PEW RESEARCH CENTER

¹ Throughout this report, "teens" refers to those ages 13 to 17 and "parents" refers to those with a child ages 13 to 17.

Other key findings from the survey:

- **More teens report spending too much time on social media:** 45% of teens say they spend too much time on social media in our current survey, up from 36% in 2022.
- **Girls' experiences on social media skew more negative, at times:** Teen girls are more likely than boys to say social media hurt their mental health (25% vs. 14%), confidence (20% vs. 10%) or sleep (50% vs. 40%).
- **A majority of teens see social media as a positive space for friendships and creativity:** 74% of teens say these platforms make them feel more connected to their friends, and 63% say they give them a place to show off their creative side.
- **Teens and parents have different comfort levels talking about teen mental health:** 80% of parents say they're extremely or very comfortable talking to their teen about their teen's mental health. Smaller shares of teens (52%) feel the same way.
- **Social media as a mental health resource:** 34% of teens say they at least sometimes get information about mental health on social media.

Jump to read about views among *parents and teens* on: [Mental health concerns](#) | [Openness to talking about mental health with others](#)

Jump to read about views among *teens* on: [Social media as a mental health resource](#) | [Social media's effect on teens](#) | [Feelings about social media in their own lives](#) | [Screen time](#)

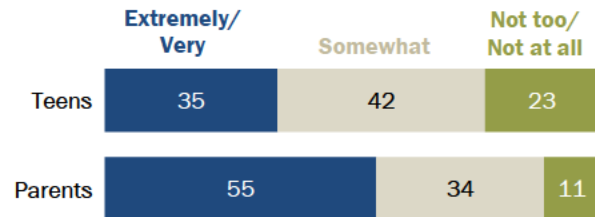
Parents' and teens' concerns about mental health

To better understand how families are grappling with issues related to youth mental health, we asked teens and parents to share their level of concern, thoughts on underlying causes, and openness to discussing mental health.

Parents are more likely than teens to be concerned about teen mental health today. Overall, 55% of parents report being extremely or very concerned about the mental health of teens today. Fewer teens (35%) say the same, according to our survey of 1,391 parents and their teens conducted Sept. 18-Oct. 10, 2024.

Parents are more concerned than teens about teen mental health

% of U.S. parents and teens ages 13 to 17 who say they are ___ concerned about the mental health of teens these days



Note: Those who did not give an answer are not shown.

Source: Survey conducted Sept. 18-Oct. 10, 2024.

"Teens, Social Media and Mental Health"

PEW RESEARCH CENTER

On the other hand, a larger share of teens than parents say they're *not too* or *not at all* worried about the state of teen mental health (23% vs. 11%).

About this report

There are [growing debates](#) about social media's impact on youth mental health. This survey seeks to surface teens' and their parents' perspectives on this topic, not to supply evidence or establish causality.

We used the overarching term "mental health" throughout our survey questions to ask teens and parents about their broad experiences.

Teens' and parents' views, by gender

Teens' concerns about mental health differ by gender. Girls more often than boys say that they are highly concerned about teen mental health (42% vs. 28%).

We also see differences among parents – both based on their gender and the gender of their child.

Mothers are more likely than fathers to say they are extremely or very concerned about the mental state of teens today (61% vs. 47%).

Additionally, parents of a teen girl are more likely than those with a teen boy to express high levels of concern (61% vs. 49%).

Related: [*The Gender Gap in Teen Experiences*](#)

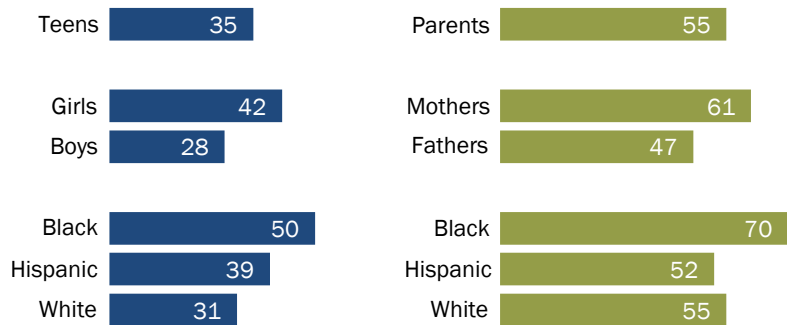
Teens' and parents' views, by race and ethnicity

There are also notable differences by race and ethnicity. Seven-in-ten Black parents say they are extremely or very worried about teen mental health. This is higher than the shares seen among White (55%) and Hispanic (52%) parents.²

Black teens also stand out in their concern about teen mental health. Half of Black teens report being highly concerned, compared with 39% of Hispanic teens and an even smaller share of White teens (31%).

Racial and gender differences in parents' and teens' concerns about teen mental health

% of U.S. parents and teens ages 13 to 17 who say they are **extremely/very concerned** about the mental health of teens these days



Note: White and Black teens and parents include those who report being only one race and are not Hispanic. Hispanic teens and parents are of any race. Those who did not give an answer or gave other responses are not shown.

Source: Survey conducted Sept. 18-Oct. 10, 2024.

"Teens, Social Media and Mental Health"

PEW RESEARCH CENTER

² There were not enough Asian respondents in the sample to be broken out into a separate analysis. As always, their responses are included in the general population figures throughout the report.

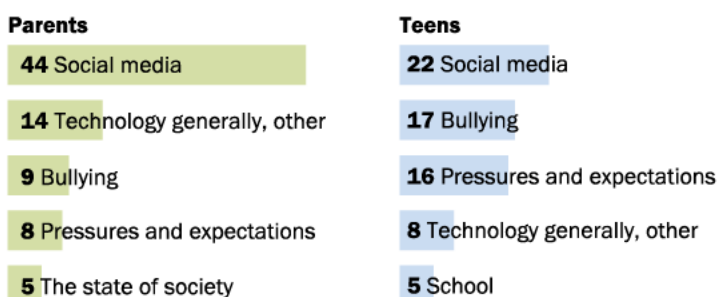
What contributes the most to teens' mental health?

Parents and teens who say they are at least somewhat concerned about teen mental health today were then asked what they think *most negatively* impacts it.

While both groups cited similar themes, parents more often blame social media, while teens cite a range of factors, including social media, bullying and social pressures.

Parents are more likely than teens to cite social media as a threat to teen mental health

Among the 89% of U.S. parents and 77% of teens who say they are at least somewhat concerned about teen mental health these days, % who say ___ is the one thing they think most negatively impacts teen mental health



Note: Teens refers to those ages 13 to 17. Parents refers to those with a child ages 13 to 17. Verbatim responses have been coded into categories. Only responses that were given by at least 5% of respondents are shown. Refer to the Topline for the full list of categories. Source: Survey conducted Sept. 18-Oct. 10, 2024. "Teens, Social Media and Mental Health"

PEW RESEARCH CENTER

Views among parents

Social media is the top reason parents give when asked about what most negatively impacts teens. Among parents who are at least somewhat concerned about teen mental health, 44% say social media have the biggest negative impact on teens today.

“They live in a fake world of social media that limits them as human beings, distancing them from their family.” (Translated from Spanish)
– Mother of teen

“Social media is a big part of teens’ lives nowadays, and they are always trying to live up to the expectations of all the friends on their pages.”
– Father of teen

Some of these parents – though far fewer – mention the negative impacts on teens of **technology more broadly** or name another specific type of technology (14%).

“Technology, which is making them more afraid to try things, makes them less creative and makes them less likely to figure out how to solve their own problems, whether relationally or physically.”
– Mother of teen

And about one-in-ten say online or offline **bullying** (9%) or the **pressures and expectations** that teens experience (8%) is the main contributor.

“Kids bullying, making fun of the less fortunate or the kids that aren't sports-oriented or considered cool.”
– Mother of teen

“[There’s] too much emphasis on the idea that they need to be perfect. In academics, social interactions, appearance, fitness and every conceivable way.”
– Father of teen

Views among teens

Parents often point to social media, but teens cite a broader range of negative influences on youth mental health.

Still, among teens who say they are at least somewhat concerned about the mental health of teens today, **22% cite social media as the main factor.**

“The overuse of social media in our society seems to be the main cause of depression among those in my age group. People seem to let themselves be affected by the opinions of people they don’t know, and it wreaks havoc upon people’s states of mind.”

– Teen boy

“The people they see on social media, it makes them think they have to look and be like them or they won’t be liked.” – Teen girl

Another 8% of these teens point to **technology broadly** or another type of technology.

About one-in-five teens who are at least somewhat concerned cited **bullying** – in person or online (17%). And 16% say the **pressures and expectations** placed on teens today is what most negatively impacts teen mental health.

“Bullying from other students and the ones that want to fit in and be accepted.”

– Teen boy

“Everyone expects teens to have it all figured out by the time we get out of high school. Sometimes we don’t know what we want to do. We are figuring life out too.”

– Teen girl

Comfort levels with discussing mental health

The [National Institute of Mental Health](#) highlights the importance of open communication to help teens feel supported. But are parents and teens comfortable having these conversations?

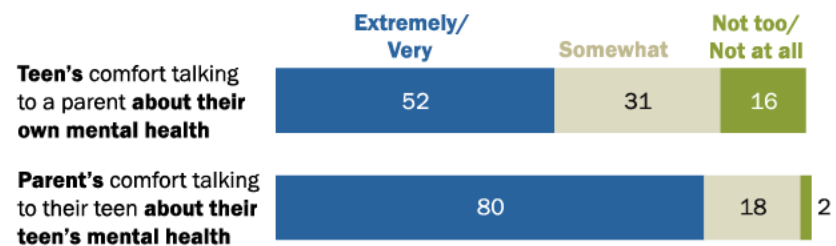
The vast majority of parents are comfortable talking with their teen about their child's mental health; fewer teens are comfortable doing this.

Eight-in-ten parents say they would be extremely or very comfortable doing so, compared with 52% of teens.

Most mothers and fathers say they'd be extremely or very comfortable having these conversations with their teens. However, the share is higher among moms than dads (84% vs. 75%).

80% of parents say they would be highly comfortable talking to their teen about their teen's mental health; fewer teens would be comfortable with this

% of U.S. parents and teens ages 13 to 17 who say they would be ___ comfortable talking with one another about the teen's mental health



Note: Those who did not give an answer are not shown.

Source: Survey conducted Sept. 18-Oct. 10, 2024.

"Teens, Social Media and Mental Health"

PEW RESEARCH CENTER

Just 2% of parents say they would be not too or not at all comfortable, while this share rises to 16% among teens.

Besides parents, we also asked teens about their comfort levels in discussing their mental health with four other types of people: friends, therapists, family members and teachers. Our survey finds their openness varies widely by who they're talking to.

A parent: Roughly half of the teens say they would be extremely or very comfortable talking with a parent about their own mental health.³

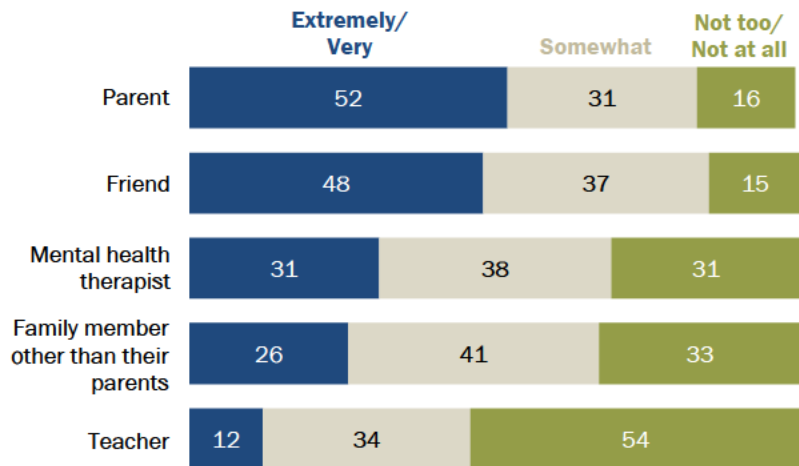
A friend: 48% say they'd be highly comfortable talking about their mental health with a friend. This makes parents and friends the top choices for teens when having these discussions.

A therapist or family member: 31% say they would be highly comfortable talking about their mental health with a therapist. And a slightly smaller share (26%) say this about talking with a family member other than their parents.

A teacher: Relatively few teens (12%) say they would be extremely or very comfortable discussing their mental health with a teacher. In fact, 54% say they would *not* be comfortable with this.

More teens are comfortable talking about their mental health with a parent or friend than a therapist or teacher

% of U.S. teens ages 13 to 17 who say they would be ___ comfortable talking with each of the following people about their mental health



Note: Those who did not give an answer are not shown.

Source: Survey conducted Sept. 18-Oct. 10, 2024.

"Teens, Social Media and Mental Health"

PEW RESEARCH CENTER

³ Previous Center surveys show that parents are seen by teens as being more effective in addressing cyberbullying, compared with other groups.

Teens' views, by gender

Teen girls are more comfortable than boys talking about their mental health with friends. While 58% of teen girls say they are highly comfortable doing this, that share drops to 38% for boys.

Girls are also more likely to say they would have this comfort level with a mental health therapist (34% vs. 27%).

Similar shares of boys and girls say they'd be extremely or very comfortable talking to parents, other family members or teachers about their own mental health.

Teens' views, by race and ethnicity

There are also racial and ethnic differences in teens' comfort levels speaking with a therapist or a teacher. Roughly four-in-ten Black teens (41%) say they'd be extremely or very comfortable doing so, compared with smaller shares of Hispanic (31%) and White (28%) teens.

Black (17%) and Hispanic (15%) teens are more likely than White teens (10%) to say they would be highly comfortable talking to a teacher about their mental health.

The share of teens who say they'd be highly comfortable talking about this with friends, parents and other family members varies little by race and ethnicity.

Social media as a mental health resource

Some teens are also turning to social media to find information about mental health. Platforms like [TikTok have become spaces for influencers](#) and therapists alike to share their experiences and advice about mental health.

In our survey, **34% of teens say they at least sometimes get information about mental health on social media.** This includes 9% who say they do this extremely or fairly often.

We also asked these teens how important social media platforms are as a resource for mental health information. Among those who do this at least sometimes, **63% say it's an important way they get information about mental health.**

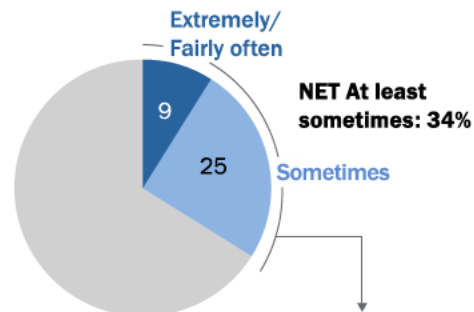
Another 37% of these teens say social media are *not* an important way they get mental health information.

Teens' experiences, by gender

Teen girls are more likely than boys to get this information on social media. Four-in-ten girls say they at least sometimes get mental health information on social media, compared with 28% of boys.

34% of teens get mental health info on social media; majority of this group says these sites are an important source

% of U.S. teens ages 13 to 17 who say they get information about mental health on social media ...



Among those who say they do this at least sometimes, % who say social media are ___ to get this information



Source: Survey conducted Sept. 18-Oct. 10, 2024.
"Teens, Social Media and Mental Health"

PEW RESEARCH CENTER

However, among those who at least sometimes get mental health information on social media, statistically similar shares of girls (64%) and boys (60%) say it's an important way they get this information.

Teens' experiences, by race and ethnicity

Larger shares of Black teens report using social media to get information about mental health. About half of Black teens (49%) say they do this at least sometimes, compared with smaller shares of Hispanic (35%) and White (30%) teens.

Teens' views of – and experiences on – social media

One area where teens share contrasting views about social media is when discussing its effect on their peers versus their own experiences.

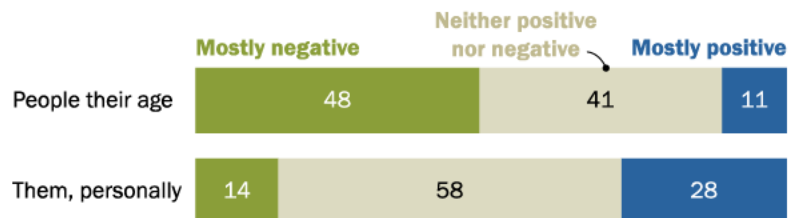
Similar to [the last time we asked this question](#), **more teens think social media have a negative effect on people their age than on them personally.** About half of teens (48%) say social media platforms have a mostly negative effect on people their age. Meanwhile, 14% see a mostly negative impact for *themselves*, up slightly from 9% in 2022.

Teens are more than twice as likely to say social media have a positive impact on themselves than on their peers (28% vs. 11%).

Still, the most common response falls into the neutral category. About six-in-ten teens (58%) say the effect on them is neither positive nor negative.

Teens are more likely to think social media are bad for their peers than for themselves

% of U.S. teens ages 13 to 17 who say social media have (a) ___ effect on ...



Note: Those who did not give an answer are not shown.

Source: Survey conducted Sept. 18-Oct. 10, 2024.

"Teens, Social Media and Mental Health"

PEW RESEARCH CENTER

Views of peer impact over time

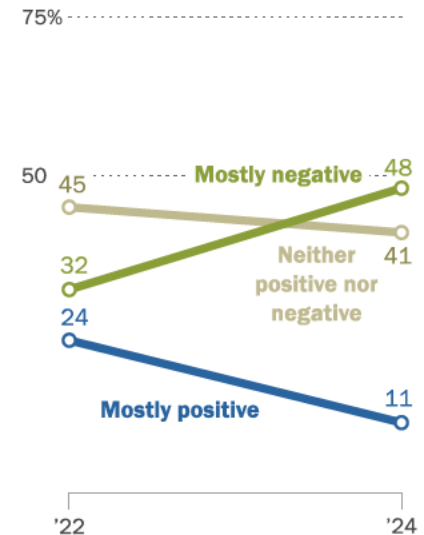
Teens' views of the impact of social media on their peers has grown increasingly negative. The share who say these sites have a mostly negative effect on people their age is up 16 percentage points since 2022.

At the same time, the share who believe these platforms have a mostly *positive* effect on people their age decreased from 24% in 2022 to 11% in our current survey.

The percentage who describe social media's effect on their peers as neither positive nor negative has remained statistically unchanged over this time span.

48% of teens say social media harm people their age, up from 32% in 2022

% of U.S. teens ages 13 to 17 who say social media have (a) ___ effect on people their age



Note: Those who did not give an answer are not shown.

Source: Survey conducted Sept. 18-Oct. 10, 2024.

"Teens, Social Media and Mental Health"

PEW RESEARCH CENTER

How teens see social media's impact on mental health, friendships, sleep

Teens' views of the benefits and harms of social media vary by which aspect of their lives you ask about. Still, many believe these platforms don't have much influence over them.

In our survey, teens are far more likely to say social media hurt rather than help their [sleeping habits](#) and [productivity](#), which are both crucial for well-being, according to experts.

Four-in-ten or more teens say social media platforms hurt the amount of sleep they get (45%), as well as their productivity (40%).

Small shares – about one-in-ten or fewer – say social media platforms *help* with these things. And roughly one-third say these platforms neither help nor hurt.

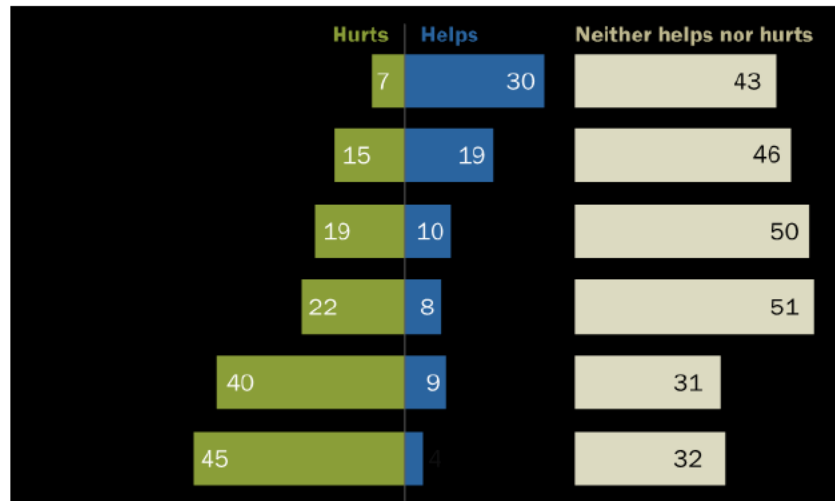
About one-in-five teens say social media hurt their mental health (19%) or grades (22%). Roughly one-in-ten each say these platforms help. But the largest shares say these platforms have a neutral impact on their mental health (50%) and grades (51%).

Similar shares of teens say social media help (19%) or hurt (15%) their confidence. Still, nearly half (46%) say these platforms neither hurt nor help.

Friendships are the only aspect of teen life that we asked about in which more teens say social media help rather than harm these relationships (30% vs. 7%). Again, a sizable share of teens (43%) describe social media's impact in neutral terms.

Teens are more likely to say social media sites hurt than help their sleep, productivity and mental health, but see a more positive impact on their friendships

% of U.S. teens ages 13 to 17 who say using social media ___ each of the following a lot/a little



Note: Those who did not give an answer or gave other responses are not shown.

Source: Survey conducted Sept. 18-Oct. 10, 2024.

"Teens, Social Media and Mental Health"

PEW RESEARCH CENTER

Teens' experiences, by gender

Similar to our previous surveys, teen girls are generally more likely than boys to report having a [more negative experience](#) on social media.

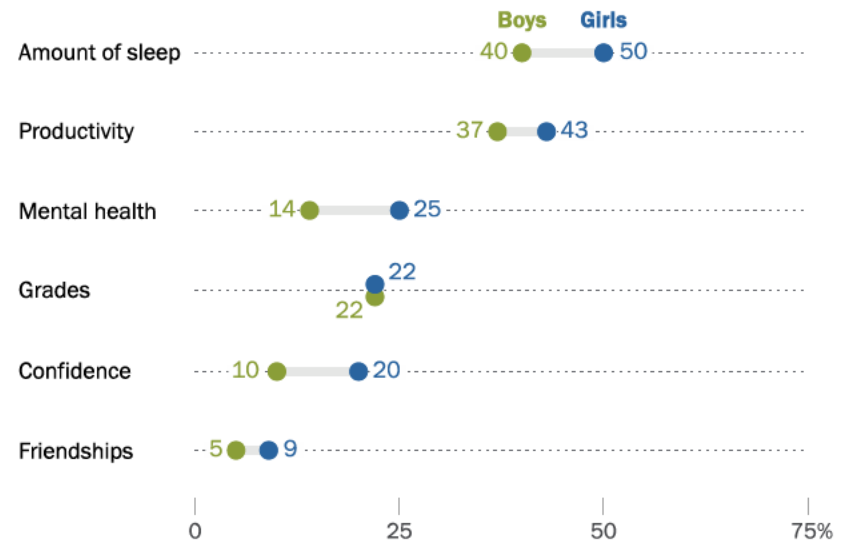
Teen girls stand out from boys in saying social media are harmful to their mental health. While 25% of girls say social media have hurt their mental health, that share drops to 14% among boys. Still, regardless of gender, the largest share says social media sites neither help nor hurt this.

At the same time, girls are more likely than boys to say the sites hurt the amount of sleep they get (50% vs. 40%), their confidence (20% vs. 10%) and friendships (9% vs. 5%).

Gender differences on social media's impact on teens' productivity or grades are not statistically significant.

Teen girls are more likely than boys to say social media hurt their mental health, sleep, confidence

% of U.S. teens ages 13 to 17 who say using social media has hurt their ___ a lot/a little



Note: Those who did not give an answer or gave other responses are not shown.

Source: Survey conducted Sept. 18-Oct. 10, 2024.

"Teens, Social Media and Mental Health"

PEW RESEARCH CENTER

There are no meaningful gender differences among teens who say social media *help* any of the six aspects we asked about.

Social media: Connections, creativity and drama

A majority of teens credit social media with forming connections and expressing their creativity.

Roughly three-quarters of teens (74%) say what they see on social media makes them feel more connected to what's going on in their friends' lives. And 63% say social media platforms are a place they can show their creative side.

And about half – 52% each – say what they see on these sites makes them feel more accepted or as if they have people who will support them through tough times.

Even as teens have positive experiences on social media, they also encounter a less desirable side. About

four-in-ten teens (39%) say social media make them feel overwhelmed by drama.

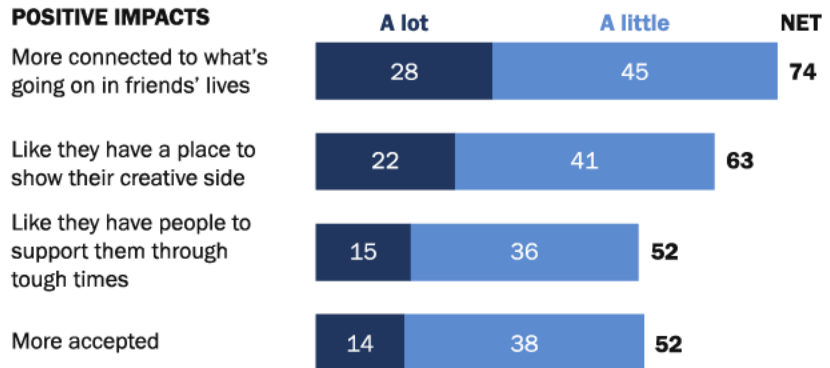
Smaller shares say these platforms make them feel

pressure to post popular content (31%), excluded by friends (31%) or worse about their own life (27%).

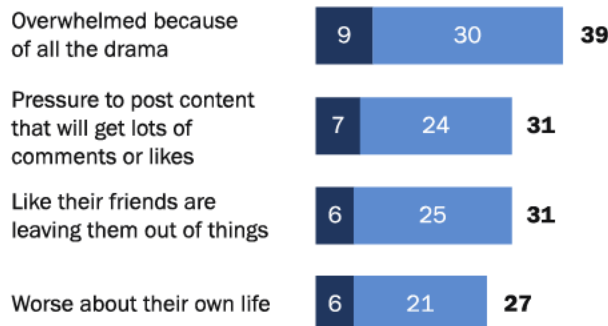
Most teens say social media keep them connected to friends, but some get overwhelmed by the drama

% of U.S. teens ages 13 to 17 who say that, in general, what they see on social media makes them feel a lot/a little ...

POSITIVE IMPACTS



NEGATIVE IMPACTS



Note: Figures may not add up to the NET value due to rounding. Those who did not give an answer or gave other responses are not shown.

Source: Survey conducted Sept. 18-Oct. 10, 2024.

"Teens, Social Media and Mental Health"

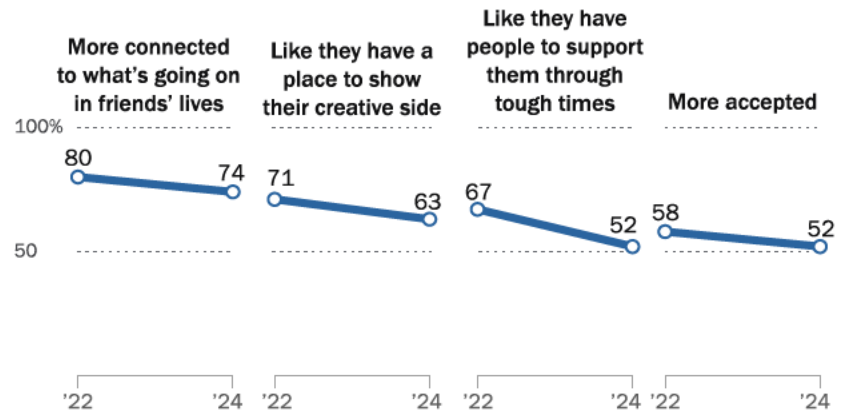
PEW RESEARCH CENTER

Fewer teens now credit social media as a support system. The share who say social media platforms make them feel like they have people who can support them through tough times has declined to 52% in 2024 from 67% in 2022.

Fewer teens in our current survey than in 2022 believe social media let them showcase their creativity, make them feel more connected with friends, or make them feel accepted. However, about half or more still acknowledge these platforms' positive effects.

Since 2022, drop in teens saying social media make them feel supported; but about half still say this

*% of U.S. teens ages 13 to 17 who say that, in general, what they see on social media makes them feel **a lot/a little** ...*



Note: Those who did not give an answer or gave other responses are not shown.

Source: Survey conducted Sept. 18-Oct. 10, 2024.

"Teens, Social Media and Mental Health"

PEW RESEARCH CENTER

The shares of teens who cite having any of the four negative experiences with social media that we asked about have seen little to no change since 2022.

Teens' experiences, by gender

As was true with our previous survey, **larger shares of girls than boys report having a more negative experience on social media.** For example, 34% of teen girls say social media platforms make them feel worse about their own lives, compared with 20% of boys. This is [consistent with our findings](#) from 2022.

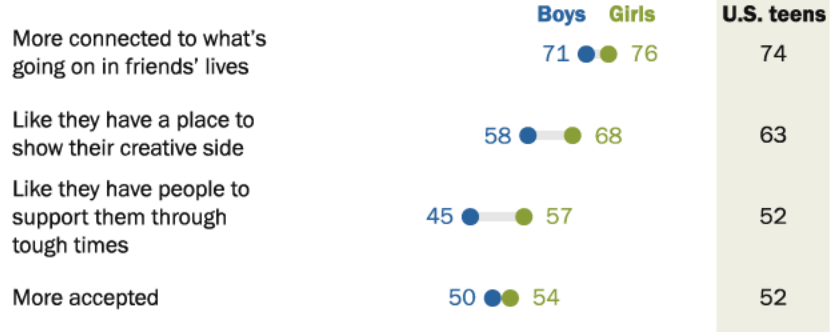
Girls are also more likely than boys to say social media make them feel overwhelmed because of drama (45% vs. 34%), pressure to post popular content (36% vs. 26%), or feel excluded by friends (36% vs. 26%).

Still, girls more often than boys report experiencing some of the positive sides of social media. Larger shares of teen girls than boys say these sites make them feel like they have people to support them (57% vs. 45%) and a place to show their creative side (68% vs. 58%).

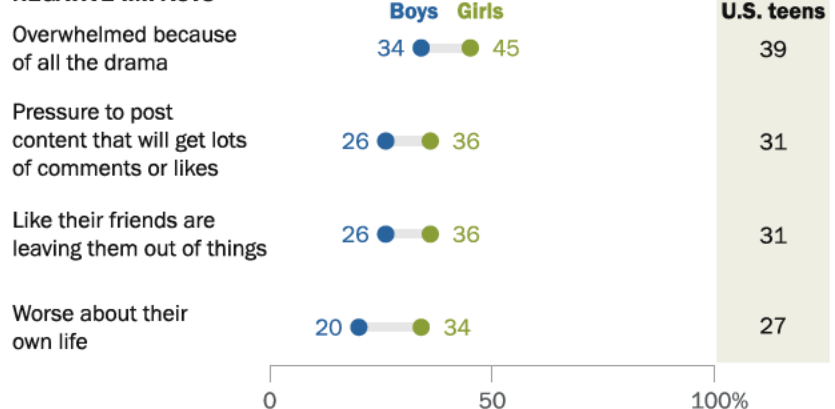
Teen girls more likely than boys to report experiencing both some of the good and bad sides of social media

% of U.S. teens ages 13 to 17 who say that, in general, what they see on social media makes them feel *a lot/a little ...*

POSITIVE IMPACTS



NEGATIVE IMPACTS



Note: Those who did not give an answer or gave other responses are not shown.

Source: Survey conducted Sept. 18-Oct. 10, 2024.

"Teens, Social Media and Mental Health"

PEW RESEARCH CENTER

Teens' experiences, by race and ethnicity

There are only modest racial and ethnic differences in whether teens have these kinds of experiences on social media. However, there are differences in the degree to which they feel this way.

For instance, **a larger share of Black teens than White and Hispanic teens say they feel a lot of support and acceptance from social media.** One-quarter of Black teens say social media platforms make them feel much more accepted. Smaller shares of White (10%) or Hispanic (13%) teens say this.

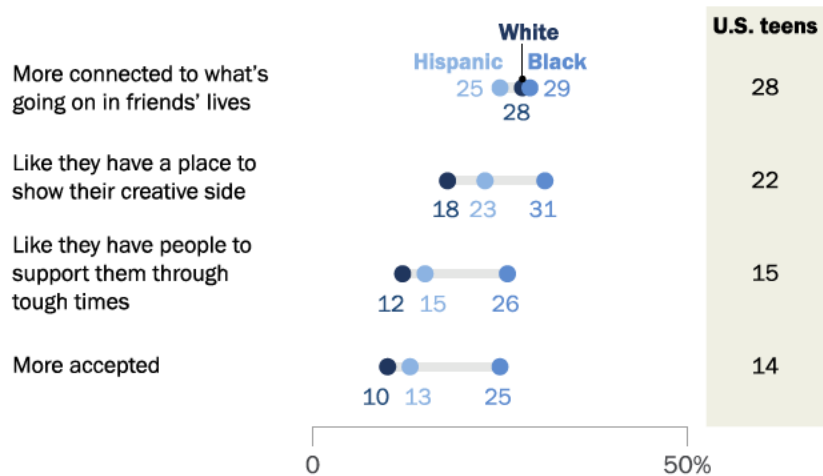
Black teens (26%) are also more likely than White (12%) or Hispanic (15%) teens to say that what they see on social media makes them feel like they have a lot of support through tough times.

Additionally, 31% of Black teens say that what they see on the sites makes them feel a lot like they have a place to be creative, compared with 18% of White teens who say the same. Hispanic teens do not meaningfully differ from either group.

There are little to no racial and ethnic differences among teens who say social media make them feel overwhelmed by drama, pressures when posting, left out by friends, or worse about their own life.

Black teens are more likely than White and Hispanic teens to report feeling a lot of support and acceptance from social media

% of U.S. teens ages 13 to 17 who say that, in general, what they see on social media makes them feel a lot ...



Note: White and Black teens include those who report being only one race and are not Hispanic. Hispanic teens are of any race. Those who did not give an answer or gave other responses are not shown.

Source: Survey conducted Sept. 18-Oct. 10, 2024
 "Teens, Social Media and Mental Health"

PEW RESEARCH CENTER

Teens' views on screen time and efforts to cut back

Parents [have many concerns](#) about their children's use of social media, and screen time is at the top of their minds. Some legislators share these sentiments, [proposing regulations to set time](#) limits on app usage.

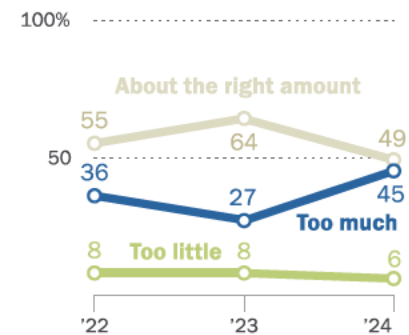
Teens themselves are more likely today than two years ago to describe their social media use as excessive. More than four-in-ten teens (45%) say they spend too much time on social media. This is up from [27% in 2023](#) and [36% in 2022](#).

The share of those who say they spend about the right amount of time on it has dropped to 49% in 2024 from 64% in 2023 and 55% in 2022.

The percentage of teens who say they spend too little time on social media has remained relatively constant over the past two years.

Growing shares of teens say they spend too much time on social media

% of U.S. teens ages 13 to 17 who say that, overall, they spend ___ (of) time on social media



Note: Those who did not give an answer are not shown.

Source: Survey conducted Sept. 18-Oct. 10, 2024.

"Teens, Social Media and Mental Health"

PEW RESEARCH CENTER

Some teens are cutting back on their social media use. We found that 44% of teens say they have cut back on using social media, and an identical share say the same for their smartphone use.

Both of these shares have increased since [we asked this question in 2023](#). Then, 39% of teens said they cut back on social media, and 36% said the same about their phone use.

Still, more than half of teens (55% each) say they have *not* cut back on using smartphones and social media.

44% of teens say they have cut back on phone and social media use; girls more likely than boys to do so

% of U.S. teens ages 13 to 17 who say that they ___ cut back on their use of the following

	SMARTPHONE		SOCIAL MEDIA	
	Have	Haven't	Have	Haven't
Teens	44	55	44	55
Boys	40	59	40	60
Girls	49	50	48	51

Note: Those who did not give an answer are not shown.

Source: Survey conducted Sept. 18-Oct. 10, 2024.

"Teens, Social Media and Mental Health"

PEW RESEARCH CENTER

Teens' experiences, by gender

Teen girls are more likely to say they've tried to reduce their screen time. While about half of girls say they have tried to cut back on social media and smartphone use, 40% of boys say the same for each.

Teens' experiences, by their screen time

Teens who report spending too much time on social media are more likely to report cutting back on it. Roughly half of this group (49%) say they have attempted to do this. However, this number drops to 41% when looking at those who are satisfied with the amount of time they spend on social media.

Acknowledgments

This report is a collaborative effort based on the input and analysis of the following individuals. Find related reports online at [pewresearch.org/internet](https://www.pewresearch.org/internet).

Primary researchers

Michelle Faverio, *Research Associate*

Monica Anderson, *Director, Internet and Technology Research*

Eugenie Park, *Research Assistant*

Research team

Jeffrey Gottfried, *Associate Director, Research*

Olivia Sidoti, *Research Assistant*

Colleen McClain, *Senior Researcher*

Editorial and graphic design

Kaitlyn Radde, *Associate Information Graphics Designer*

Rebecca Leppert, *Copy Editor*

Communications and web publishing

Haley Nolan, *Communications Manager*

DeVonte Smith, *Communications Associate*

Sara Atske, *Digital Producer*

In addition, the project benefited greatly from the guidance of Pew Research Center's methodology team: Courtney Kennedy, Scott Keeter, Ashley Amaya, Andrew Mercer, Dorene Asare-Marfo, Anna Brown, Arnold Lau and Dana Popky. This project also benefited from feedback by the following Pew Research Center staff: Naomi Forman-Katz, Juliana Menasce Horowitz, Gregory A. Smith and Eileen Yam.

The Center gained invaluable advice from the guidance of Amy Green, Ph.D., Head of Research, Hopelab, as well as from those on our advisory board: Fred Dillon, Director of Partnerships and Strategy, University of California, Berkeley School of Public Health; Jackie Menjivar, Manager of Peer and Youth Advocacy, Mental Health America; Jacqueline Nesi, Ph.D., Assistant Professor, Department of Psychiatry and Human Behavior, Brown University; and S. Craig Watkins, Ph.D., Ernest A. Sharpe Centennial Professor, University of Texas at Austin. The feedback shared for this

project is solely that of the individuals and does not express the views, policies or positions of their respective employers.

Methodology

The analysis in this report is based on a self-administered web survey conducted from Sept. 18 to Oct. 10, 2024, among a sample of 1,391 dyads, with each dyad (or pair) comprised of one U.S. teen ages 13 to 17 and one parent per teen. The margin of sampling error for the full sample of 1,391 teens is plus or minus 3.3 percentage points. The survey was conducted by Ipsos Public Affairs in English and Spanish using KnowledgePanel, its nationally representative online research panel.

The research plan for this project was submitted to an external institutional review board (IRB), Advarra, which is an independent committee of experts that specializes in helping to protect the rights of research participants. The IRB thoroughly vetted this research before data collection began. Due to the risks associated with surveying minors, this research underwent a full board review and received approval (Approval ID Pro00080537).

KnowledgePanel members are recruited through probability sampling methods and include both those with internet access and those who did not have internet access at the time of their recruitment. KnowledgePanel provides internet access for those who do not have it and, if needed, a device to access the internet when they join the panel. KnowledgePanel's recruitment process was originally based exclusively on a national random-digit-dialing (RDD) sampling methodology. In 2009, Ipsos migrated to an address-based sampling (ABS) recruitment methodology via the U.S. Postal Service's Delivery Sequence File (DSF). The Delivery Sequence File has been estimated to cover as much as 98% of the population, although some studies suggest that the coverage could be in the low 90% range.⁴

Panelists were eligible for participation in this survey if they indicated on an earlier profile survey that they were the parent of a teen ages 13 to 17. A random sample of 3,233 eligible panel members were invited to participate in the study. Responding parents were screened and considered qualified for the study if they reconfirmed that they were the parent of at least one child age 13 to 17 and granted permission for their teen who was chosen to participate in the study. In households with more than one eligible teen, parents were asked to think about one randomly selected teen and that teen was instructed to complete the teen portion of the survey. A survey was considered complete if both the parent and selected teen completed their portions of the questionnaire, or if the parent did not qualify during the initial screening.

Of the sampled panelists, 1,665 (excluding break-offs) responded to the invitation and 1,391 qualified, completed the parent portion of the survey, and had their selected teen complete the teen portion of the survey, yielding a final stage completion rate of 51.5% and a qualification rate

⁴ AAPOR Task force on Address-based Sampling. 2016. "[AAPOR Report: Address-based Sampling](#)."

of 84%.⁵ The cumulative response rate accounting for nonresponse to the recruitment surveys and attribution is 2.7%. The break-off rate among those who logged on to the survey (regardless of whether they completed any items or qualified for the study) is 21.4%.

Upon completion, qualified respondents received a cash-equivalent incentive worth \$10 for completing the survey. To encourage response from non-Hispanic Black panelists, the incentive was \$40.

All panelists received email invitations and any nonresponders received reminders, shown in the table. The field period was closed on Oct. 10, 2024.

Weighting

The analysis in this report was performed using separate weights for parents and teens. The parent weight was created in a multistep process that begins with a base design weight for the parent, which is computed to reflect their probability of selection for recruitment into KnowledgePanel. These selection probabilities were then adjusted to account for the probability of selection for this survey which included oversamples of Black and Hispanic parents. Next, an iterative technique was used to align the parent design weights to population benchmarks for parents of teens ages 13 to 17 on the dimensions identified in the accompanying table, to account for any differential nonresponse that may have occurred.

Invitation and reminder dates

Invitation	Sept. 18, 2024
First reminder	Sept. 20, 2024
Second reminder	Sept. 24, 2024
Third reminder (<i>only sent to Hispanic nonresponders and non-Hispanic Black nonresponders</i>)	Oct. 1, 2024
Fourth reminder (<i>only sent to non-Hispanic Black nonresponders</i>)	Oct. 4, 2024
Fifth reminder (<i>only sent to non-Hispanic Black nonresponders</i>)	Oct. 7, 2024

Weighting dimensions

Variable	Benchmark source
Age x Gender	2024 March Supplement of the Current Population Survey (CPS)
Race/Ethnicity	
Census Region	
Metropolitan Status	
Education (parents only)	
Household Income	2022 American Community Survey (ACS)
Household Income x Race/Ethnicity	
Total Household Size	
Language proficiency	

Note: Estimates from the ACS are based on noninstitutionalized adults.

PEW RESEARCH CENTER

⁵ The 1,391 qualified interviews exclude two cases that were dropped for having skipped one-third or more of the survey questions.

To create the teen weight, an adjustment factor was applied to the final parent weight to reflect the selection of one teen per household. Finally, the teen weights were further raked to match the demographic distribution for teens ages 13 to 17 who live with parents. The teen weights were adjusted on the same teen dimensions as parent dimensions with the exception of teen education, which was not used in the teen weighting.

Sampling errors and tests of statistical significance take into account the effect of weighting. Interviews were conducted in both English and Spanish.

In addition to sampling error, one should bear in mind that question wording and practical difficulties in conducting surveys can introduce error or bias into the findings of opinion polls.

The following table shows the unweighted sample sizes and the error attributable to sampling that would be expected at the 95% level of confidence for different groups in the survey:

Group	Unweighted sample size	Plus or minus ...
Teens (ages 13 to 17)	1,391	3.3 percentage points
Boys	698	4.6 percentage points
Girls	669	4.7 percentage points
White, non-Hispanic	530	4.9 percentage points
Black, non-Hispanic	247	8.0 percentage points
Hispanic	450	5.9 percentage points

Note: This survey includes oversamples of non-Hispanic Black and Hispanic respondents. Unweighted sample sizes do not account for the sample design or weighting and do not describe a group's contribution to weighted estimates. Refer to the Weighting section for details.

PEW RESEARCH CENTER

Group	Unweighted sample size	Plus or minus ...
Parents of teens (ages 13 to 17)	1,391	3.2 percentage points
Men	538	5.0 percentage points
Women	853	4.2 percentage points
White, non-Hispanic	586	4.5 percentage points
Black, non-Hispanic	278	7.8 percentage points
Hispanic	423	5.8 percentage points

Note: This survey includes oversamples of non-Hispanic Black and Hispanic respondents. Unweighted sample sizes do not account for the sample design or weighting and do not describe a group's contribution to weighted estimates. Refer to the Weighting section for details.

PEW RESEARCH CENTER

Sample sizes and sampling errors for subgroups are available upon request.

Dispositions and response rates

The tables below display dispositions used in the calculation of completion, qualification and cumulative response rates.⁶

Dispositions	
Total panelists assigned	3,233
Total study completes (including nonqualified)	1,665
Number of qualified completes	1,391
Number of study break-offs	453
Study Completion Rate (COMPR)	51.5%
Study Qualification Rate (QUALR)	84%
Study Break-off Rate (BOR)	21.4%

⁶ For more information on this method of calculating response rates, refer to Callegaro, Mario, and Charles DiSogra. 2008. ["Computing response metrics for online panels."](#) Public Opinion Quarterly.

Cumulative response rate calculations	
Study-Specific Average Panel Recruitment Rate (RECR)	8.7%
Study-Specific Average Household Profile Rate (PROR)	59.5%
Study-Specific Average Household Retention Rate (RETR)	39.6%
Cumulative Response Rate	2.7%

Advisory board

In addition to a team of subject area and methodological experts at the Pew Research Center, the project was also guided by an advisory board of four members. This board included experts in a variety of areas related to youth, including technology use and mental health.

- Fred Dillon, Director of Partnerships and Strategy, University of California, Berkeley School of Public Health
- Jackie Menjivar, Manager of Peer and Youth Advocacy, Mental Health America
- Jacqueline Nesi, Ph.D., Assistant Professor, Department of Psychiatry and Human Behavior, Brown University
- S. Craig Watkins, Ph.D., Ernest A. Sharpe Centennial Professor, University of Texas at Austin

Advisors provided feedback at various key points during the report, including the questionnaire and a draft of the report. Pew Research Center remains solely responsible for all aspects of the research, including any errors associated with its products and findings. The feedback shared for this project is solely that of the advisors and does not express the views, policies or positions of their respective employers.

© Pew Research Center 2025

Topline questionnaire: Parents survey

2024 PEW RESEARCH CENTER'S TEENS SURVEY
SEPTEMBER 18 - OCTOBER 10, 2024
PARENTS OF TEENS AGES 13-17
TOTAL N=1,391

THE QUESTIONS PRESENTED BELOW ARE PART OF A LARGER SURVEY CONDUCTED ON THE IPSOS KNOWLEDGE PANEL. OTHER QUESTIONS ON THIS SURVEY HAVE BEEN PREVIOUSLY RELEASED OR ARE BEING HELD FOR FUTURE RELEASE.

NOTE: ALL NUMBERS ARE PERCENTAGES UNLESS OTHERWISE NOTED. THE PERCENTAGES LESS THAN 0.5% ARE REPLACED BY AN ASTERISK (*). ROWS/COLUMNS MAY NOT TOTAL 100% DUE TO ROUNDING.

PN = Programming note

	Sample size	Margin of error at 95% confidence level
U.S. parents of teens ages 13-17	1,391	+/- 3.2 percentage points

ASK ALL:

PTMHCONC

How concerned are you about the mental health of teens these days?

[PN: ROTATE RESPONSES 1-5 OR 5-1 FOR HALF]

Sep 18-Oct 10, 2024

19	Extremely concerned
36	Very concerned
34	Somewhat concerned
7	Not too concerned
3	Not at all concerned
*	No answer

ASK THOSE WHO SAID AT LEAST SOMEWHAT CONCERNED (PTMHCONC=1-3) [N=1,254]:

PTMHREAS

In a couple of words, what is the ONE THING you think most negatively impacts the mental health of teens these days? [PN: SHORT OPEN-END]

Sep 26-Oct 23, 2023

44	Social media
14	Technology generally, other
9	Bullying
8	Pressures and expectations
5	The state of society
3	Mental health
3	Family life
2	Violence
1	Alcohol, smoking, drugs
8	Other
3	No answer

ASK ALL:

PTTALKMH

How comfortable would you be talking to your teen about their mental health?
[**PN: ROTATE RESPONSES 1-5 OR 5-1 TO MATCH PTMHCONC**]

Sep 18-Oct 10, 2024

40	Extremely comfortable
40	Very comfortable
18	Somewhat comfortable
2	Not too comfortable
*	Not at all comfortable
*	No answer

Topline questionnaire: Teens survey

2024 PEW RESEARCH CENTER'S TEENS SURVEY
SEPTEMBER 18 - OCTOBER 10, 2024
TEENS AGES 13-17
TOTAL N=1,391

THE QUESTIONS PRESENTED BELOW ARE PART OF A LARGER SURVEY CONDUCTED ON THE IPSOS KNOWLEDGE PANEL. OTHER QUESTIONS ON THIS SURVEY HAVE BEEN PREVIOUSLY RELEASED OR ARE BEING HELD FOR FUTURE RELEASE.

NOTE: ALL NUMBERS ARE PERCENTAGES UNLESS OTHERWISE NOTED. THE PERCENTAGES LESS THAN 0.5% ARE REPLACED BY AN ASTERISK (*). ROWS/COLUMNS MAY NOT TOTAL 100% DUE TO ROUNDING.

PN = Programming note

	Sample size	Margin of error at 95% confidence level
U.S. teens ages 13-17	1,391	+/- 3.3 percentage points

ASK ALL:
TTALKMH

If you wanted to, how comfortable would you be talking about your mental health with each of the following? [PN: RANDOMIZE ITEMS BUT ITEM E CAN NEVER COME BEFORE ITEM B; ROTATE RESPONSE OPTIONS 1-5 OR 5-1 TO MATCH GOALS_V2]

		<u>Extremely comfortable</u>	<u>Very comfortable</u>	<u>Somewhat comfortable</u>	<u>Not too comfortable</u>	<u>Not at all comfortable</u>	<u>No answer</u>
a.	A friend						
	Sep 18-Oct 10, 2024	14	34	37	12	3	*
b.	A parent						
	Sep 18-Oct 10, 2024	20	32	31	12	4	*
c.	A mental health therapist						
	Sep 18-Oct 10, 2024	10	20	38	22	9	*
d.	A teacher						
	Sep 18-Oct 10, 2024	3	9	34	35	19	*
e.	A family member other than your parents						
	Sep 18-Oct 10, 2024	6	20	41	23	10	*

ASK ALL:

TMHCONC

How concerned are you about the mental health of teens these days?

[PN: ROTATE RESPONSE OPTIONS 1-5 OR 5-1 TO MATCH GOALS_V2]Sep 18-Oct 10, 2024

9	Extremely concerned
26	Very concerned
42	Somewhat concerned
18	Not too concerned
5	Not at all concerned
*	No answer

ASK THOSE WHO SAID AT LEAST SOMEWHAT CONCERNED (TMHCONC=1-3) [N=1,059]:

TMHREAS

In a couple of words, what is the ONE THING you think most negatively impacts the mental health of teens these days? **[PN: SHORT OPEN-END]**Sep 18-Oct 10, 2024

22	Social media
17	Bullying
16	Pressures and expectations
8	Technology generally, other
5	School
4	The state of society
3	Family life
2	Alcohol, smoking, drugs
2	Violence
2	Mental health
12	Other
7	No answer

ASK ALL:

SMTIME

Overall, would you say the amount of time you spend on social media is...

[PN: DISPLAY RESPONSE OPTIONS 1-2 FOR HALF OF SAMPLE AND 2-1 FOR HALF OF SAMPLE, WITH 3 ALWAYS LAST]Sep 18-Oct 10, 2024

45	Too much
6	Too little
49	About right
*	No answer

Sep 26-Oct 23, 2023

27
8
64
1

Apr 14-May 4, 2022

36
8
55
*

ASK ALL:

TCUTBACK

Have you ever chosen to cut back on the amount of time you spend on the following? [**PN: RANDOMIZE ITEMS**]

	<u>Yes, I have done this</u>	<u>No, I have not done this</u>	<u>No answer</u>
a. Your smartphone			
Sep 18-Oct 10, 2024	44	55	1
Sep 26-Oct 23, 2023	36	63	1
b. Social media			
Sep 18-Oct 10, 2024	44	55	1
Sep 26-Oct 23, 2023	39	60	1

NO ITEM c**ASK ALL:**

SOC1

Overall, what effect would you say social media has had on people your age?

<u>Sep 18-Oct 10, 2024</u>		<u>Apr 14-May 4, 2022</u>
11	Mostly positive	24
48	Mostly negative	32
41	Neither positive nor negative	45
*	No answer	0

ASK ALL:

SOC1b

Overall, what effect would you say social media has had on YOU, PERSONALLY?

<u>Sep 18-Oct 10, 2024</u>		<u>Apr 14-May 4, 2022</u>
28	Mostly positive	32
14	Mostly negative	9
58	Neither positive nor negative	59
*	No answer	*

[PN: RANDOMIZE ORDER OF SOC2POS AND SOC2NEG]

ASK ALL:

SOC2POS

In general, does what you see on social media make you feel...

[PN: RANDOMIZE ITEMS]

NO ITEM a		<u>Yes, a lot</u>	<u>Yes, a little</u>	<u>No</u>	<u>No answer</u>
b.	Like you have a place where you can show your creative side				
	Sep 18-Oct 10, 2024	22	41	36	1
	Apr 14-May 4, 2022	29	42	29	*
c.	More connected to what's going on in your friends' lives				
	Sep 18-Oct 10, 2024	28	45	26	1
	Apr 14-May 4, 2022	33	47	20	*
d.	Like you have people who can support you through tough times				
	Sep 18-Oct 10, 2024	15	36	48	1
	Apr 14-May 4, 2022	22	45	33	*
e.	More accepted				
	Sep 18-Oct 10, 2024	14	38	47	1
	Apr 14-May 4, 2022	15	42	42	*

ASK ALL:
SOC2NEG

In general, does what you see on social media make you feel...
[PN: RANDOMIZE ITEMS]

	<u>Yes, a lot</u>	<u>Yes, a little</u>	<u>No</u>	<u>No answer</u>
a. Worse about your life				
Sep 18-Oct 10, 2024	6	21	72	1
Apr 14-May 4, 2022	5	19	77	*
b. Overwhelmed because of all the drama				
Sep 18-Oct 10, 2024	9	30	60	1
Apr 14-May 4, 2022	8	31	61	*
c. Pressure to post content that will get lots of comments or likes				
Sep 18-Oct 10, 2024	7	24	68	1
Apr 14-May 4, 2022	7	23	71	*

NO ITEM d

e. Like your friends are leaving you out of things				
Sep 18-Oct 10, 2024	6	25	68	1
Apr 14-May 4, 2022	6	25	69	*

ASK IF SOCIAL MEDIA USER (TSNSUSE=1) [N=1,116]:

SMEFFECT

Do you think using social media has helped or hurt...

[PN: RANDOMIZE ITEMS; ROTATE RESPONSES 1-5 OR 5-1 FOR HALF]

	<u>Helped a lot</u>	<u>Helped a little</u>	<u>Neither helped nor hurt</u>	<u>Hurt a little</u>	<u>Hurt a lot</u>	<u>No answer</u>
a. Your friendships						
Sep 18-Oct 10, 2024	11	26	53	7	1	1
b. Your grades						
Sep 18-Oct 10, 2024	3	7	63	22	4	*
c. Your mental health						
Sep 18-Oct 10, 2024	3	9	63	21	3	1
d. How much sleep you get						
Sep 18-Oct 10, 2024	2	3	39	43	13	1
e. How productive you are						
Sep 18-Oct 10, 2024	2	9	39	39	11	*
f. Your confidence						
Sep 18-Oct 10, 2024	3	20	58	15	4	*

BASED ON ALL TEENS:
SMEFFECT

		<u>Helped a lot</u>	<u>Helped a little</u>	<u>Neither helped nor hurt</u>	<u>Hurt a little</u>	<u>Hurt a lot</u>	<u>Does not use social media</u>	<u>No answer to TSNSUSE</u>	<u>No answer to SMEFFECT</u>
a.	Your friendships Sep 18-Oct 10, 2024	9	21	43	6	1	19	*	*
b.	Your grades Sep 18-Oct 10, 2024	2	6	51	18	4	19	*	*
c.	Your mental health Sep 18-Oct 10, 2024	3	8	50	17	2	19	*	*
d.	How much sleep you get Sep 18-Oct 10, 2024	2	2	32	34	10	19	*	1
e.	How productive you are Sep 18-Oct 10, 2024	2	7	31	31	9	19	*	*
f.	Your confidence Sep 18-Oct 10, 2024	3	16	46	12	3	19	*	*

[PN: DISPLAY SMMHRES AND SMMHRES2 ON THE SAME SCREEN]

ASK IF SOCIAL MEDIA USER (TSNSUSE=1) [N=1,116]:

SMMHRES How often do you get information about mental health on social media?
[PN: ROTATE RESPONSES 1-5 OR 5-1 TO MATCH GOALS_V2]

Sep 18-Oct 10, 2024

3	Extremely often
9	Fairly often
31	Sometimes
33	Rarely
24	Never
*	No answer

BASED ON ALL TEENS:

SMMHRES

Sep 18-Oct 10, 2024

2	Extremely often
7	Fairly often
25	Sometimes
27	Rarely
19	Never
19	Does not use social media
*	No answer to TSNSUSE
*	No answer to SMMHRES

ASK IF SOCIAL MEDIA USER (TSNSUSE=1) [N=1,116]:

SMMHRES2 How important is social media to you as a way to get information about mental health?

Sep 18-Oct 10, 2024

6	The most important way
37	An important way, but not the most important
57	Not an important way
*	No answer

BASED ON TEENS WHO SAID THEY GET INFORMATION ABOUT MENTAL HEALTH ON SOCIAL MEDIA AT LEAST SOMETIMES (SMMHRES=1-3) [N=484]:

SMMHRES2

Sep 18-Oct 10, 2024

10	The most important way
53	An important way, but not the most important
37	Not an important way
*	No answer



**Senate Judiciary Committee
Subcommittee on Privacy, Technology and the Law**

**Statement of Cayce Savage
September 6, 2025**

To: Chair Blackburn, Ranking Member Klobuchar and Members of the Subcommittee.

I am a user experience researcher. It is my job to listen to and advocate for users. I have a graduate degree in experimental psychology and twelve years of experience working as a researcher, eight of which have been in my capacity as a user experience researcher. I do this work because, fundamentally, I care about people.

I worked at Meta from 2019 to 2023. In those four years, and most especially as I led research on youth safety in Virtual Reality, it became clear to me that Meta is uninterested in listening to their users or in prioritizing their safety.

While I write here about virtual reality, it is important to understand that the way Meta has approached safety for VR is emblematic of its negligent approach to safety for all of its products. The research on what we must do to ensure new technology is safe for children is very clear. Yet, across social media, messaging apps, and now wearable technology Meta has failed to prioritize child safety until they are scrutinized by outside regulators. Then, they scramble to develop features they know are insufficient and largely unused, and advertise this as proof of their responsibility.

For example, research, both within and outside of Meta, has well established that parent awareness and education of what occurs within social media is critical to ensuring the safety of young users. Despite this, parent education has only become a priority for Instagram within the past few years, following Frances Haugen's disclosure in 2021.

This knowledge from the social media space should have been used to identify child safety priorities early in Meta's VR development process. Meta should have conducted research on parent awareness of their children's VR experiences. Yet again, child safety as an area of inquiry and investment failed to be a priority for Meta until regulatory pressure began. If any digital experience were to merit particular investment in safety, it would be the hardware children are wearing on their bodies which poses heightened and unique psychological, social, and even physical danger. And yet, Meta pushed to move fast and drive engagement, instead of ensuring the experience was safe.

Written Statement of Cayce Savage (Continued)

Child safety is a necessary priority for Meta's VR devices. Meta cannot claim ignorance of this. Research both within and outside of Meta clearly shows us that children drive the adoption of new technology within the home; this is even more so the case for technology, like VR, which is associated with being social and with playing games. Meta's focus on the social and gaming aspects of VR is so blatant that the VR app Meta invested millions in developing as a "big bet" - Horizon Worlds - is primarily a social app in which users can *also* choose to play games. During the 2024 holiday season, Meta focused its VR marketing efforts on promoting its Batman: Arkham VR game, which it sold as a bundle with its headsets. Meta is advertising its VR headsets as something it knows will be attractive to children.

Meta is aware that its VR platform is full of children- it is common knowledge inside the company. Meta purposefully turns a blind eye to this knowledge, despite it being obvious to anyone using their products. Users regularly write Meta feedback like this, **"I love Horizon Worlds! I hate that it's an adult only space that's been inundated by unsupervised kids though. More needs to be done to keep children out of this app."**

The reality is that if Meta were to acknowledge the presence of underage users, they would be required to kick those users off of their platform in order to remain COPPA compliant. This isn't happening because it would decrease the number of active users Meta is reporting to shareholders, as well as its engagement metrics. It is more profitable to pretend to have no way of better identifying the real ages of their users. At Meta, engagement is the priority above everything else.

Because VR is immersive and embodied, negative experiences cause greater psychological harm than similar experiences on an iPad or Xbox. To use VR, you must place a piece of hardware on your head which obscures your vision and hearing. From this point forward, all you can see and hear is the virtual world. I personally find that the process of putting on the headset feels especially vulnerable, because I always realize I can no longer see or hear what's happening around me in the real world.

On the platform you have a virtual body. Academic research establishes that embodying a virtual avatar in an immersive context like this heightens the degree to which you identify with your virtual self. If someone corners you and gropes you in the virtual world, it will feel much more personal and emotionally disturbing than if this were to happen to you in a game on your phone. All you can see or hear is what's happening in VR, and it's a 360° experience. It's the difference between watching a scary movie and being inside a haunted house.

Unlike most adults, who are cognitively able to understand the difference between reality and fantasy, children in early development experience *everything* as real. For a child using VR, then,

Written Statement of Cayce Savage (Continued)

the degree of immersion is heightened, making the effect of negative experiences even more severe and disturbing.

Experientially, VR is more like being in Disney World than like playing a game on an iPad. In VR, your child is going to a three dimensional world which, for those few hours, will feel real. In the majority of cases, your child is going into this world without you, because VR is expensive and most families only purchase one headset. Unlike Disney World, though, your child is entering this virtual world in the body of an adult because Meta refused to develop age-specific avatars.

Most of the other people in this virtual world are other children without adults - and a lot of adults who didn't come with kids. It is normal to talk to strangers here, despite household rules about stranger danger. My research showed that it only takes a few interactions before children consider someone they met online as a friend.

Unlike Disney World, this is a place where there are no guards, no nice people in costumes, no security cameras.

There are some age-restricted experiences, but these restrictions will likely be ineffective because the likelihood of your child using an adult-aged account is high (as VR users everywhere will observe). Across Meta's products, data shows that users (and especially young users) consistently misrepresent their age as being over 18. My own research on VR parental supervision showed that, due to the lack of parental education, parents often don't see a need for their children to use an accurately aged account. Research also clearly shows that children prefer to use adult aged accounts across products, as part of development is the desire to seek increasingly mature experiences.

In the virtual world, then, your child likely represents themselves as over 18. Who is going to know otherwise? Just like every other avatar in Meta's virtual world, they look like an adult.

Everything that happens in this world will be real. The relationships, the things that are said and done, the emotions, all of it will be real. Other users - almost always, people your child doesn't know in real life - can physically corner or surround them. Their hearing is spatial, so users can come up behind them and whisper in their ear. And remember, VR is tracking a user's real life movements. So, assault in VR requires the movements to happen in real life.

Your child, especially if they are young, may not remember later whether what happened occurred in the real world or in the virtual one. And you will have no way of knowing what they experienced. Even if your child casts their headset to the TV, it isn't real for you. It's a flat image

Written Statement of Cayce Savage (Continued)

on a TV that you can walk away from. But your child is experiencing it as if it is real. And you aren't there.

When your child returns from this place, you might ask, "How was your time in the Metaverse?" and most of your children will say that it was fun. An eight year old doesn't know what grooming is. A twelve year old who's being sexually propositioned may not want to tell you because she doesn't think it's a big deal and she wants to keep using the headset.

The research on virtual reality and the way it affects our children is still in its infancy. We are still understanding the effects of embodying a virtual avatar that moves when you move. We are still understanding the effects of sexual assault in a virtual space where your visual and auditory experience is immersive. There are so many things for us still to learn. We do know that some users experience "phantom sense," a phenomenon in which they physically feel what's happening to their virtual avatar on their body in the real world. What happens in virtual reality is very real indeed.

Most importantly, Meta is aware that these children are being harmed in VR. In my time on the team, I quickly became aware that it was not uncommon for children in VR to experience bullying, sexual assault, to be solicited for nude photographs and sexual acts by pedophiles, to be regularly exposed to mature content like gambling and violence, and to participate in adult experiences like strip clubs and watching pornography with strangers.

I wish I could tell you what percentage of children using VR experience these harms, but Meta would not allow me to conduct this research.

I personally saw these things happening in VR, consistently heard reports from teens and parents in research, and read countless accounts from concerned parents online. It is easy to learn that children are not safe using Meta's VR products, just by reading public app reviews. One in particular haunts me – It reads, **"Thanks Meta for making this the pedophile kingdom. They have made it so easy for us to meet and exchange information with children here."**

Meta first acquired Oculus, its VR technology, in 2014. I was the first, and for a time, the only researcher dedicated to understanding whether its VR software experiences were safe for children - and I wasn't hired until 2022. So, for eight years, as tens of millions of headsets were sold, Meta did not think about the safety of the children it relied on to achieve global market dominance. Meta, a company valued at almost two trillion dollars, is putting minimum effort into ensuring its products are safe.

Written Statement of Cayce Savage (Continued)

When Meta did invest in parental supervision features for VR - the very basics of child safety - it did so only in response to external regulatory pressure. After eight years of total inaction, Meta leadership demanded these safety features be developed in less than a year, a timeframe which didn't allow for appropriate due diligence. Research across the digital world is very clear that parental awareness and use of supervision features is a significant challenge which *must* be addressed through parental education, *particularly* for new technology like VR. Yet, development of these features was so rushed that work to this end was not prioritized. Despite knowing this, Meta shamelessly announced that it believed its VR supervision features were a meaningful step towards child safety. Unfortunately, this lack of appropriate resourcing and due diligence is common when Meta builds safety features.

Throughout my time on Meta's VR Youth team, child safety issues regularly went unresearched and unaddressed, despite the frequency and severity of the harm. I was given a legal counterpart to scrutinize everything that I did, to tell me what research I could and couldn't do, and to ensure my research reports would not create "risk" for Meta should they be publicly disclosed. I was told not to investigate the kinds of harm children were experiencing in VR, and made to feel I was risking my job if I pressed the matter. This scrutiny became increasingly severe during my time on the team, such that I do not believe I would have been able to publish my reports from the first half of 2022 even in 2023.

Instead of amplifying the voices of our users, my work began being used to silence them so that Meta could claim deniability. I know a number of my colleagues were put in similar positions.

Meta cannot be trusted to tell the truth about the safety or use of its products. For example, in 2023 Meta said it didn't have a record of the large number of underaged children using its VR headsets. This was because it had purposefully avoided gathering that data, despite a number of Meta's leadership sharing that their children use VR, indicating that even Meta's staff were unaware of the minimum age of use, or chose to ignore it. Despite this, research proposed to address this issue was disallowed.

I deliberated for a long time about whether to come forward. Meta responded to Frances Haugen's disclosure in 2021 by cracking down on research internally. Researchers across the company were subjected to sudden censorship, and told it was for our own protection so we wouldn't be part of any future "leaks." Candidly, I am worried that speaking to you today will put my former colleagues, as well as the field of user research within Meta at risk. To my former colleagues who continue to advocate internally for child safety, I would like to express the greatest gratitude and admiration.

Written Statement of Cayce Savage (Continued)

Previous whistleblowers have come before this body to publicly testify to the suffering adults and children experience using Meta's products. Meta has promised it would change. I am here to tell you that Meta has changed, and that these changes have been for the worse. Meta has spent the time and money it could've spent making its products safer shielding itself instead, all the while developing emerging technologies which pose even greater risk to children than Instagram.

Meta consistently demonstrates that it cares more about the bottom line than the emotional or physical safety of the children who use its products every day.

How can Meta care for the safety of children, when it doesn't acknowledge that they exist?

Senate Judiciary Committee Hearing
“Hidden Harms: Examining Whistleblower Allegations
that Meta Buried Child Safety Research”

Questions for the Record for Cayce Savage

QUESTIONS FROM SENATOR BLACKBURN

1. Was Meta truthful in its responses to the Washington Post story about Meta’s child safety practices in its virtual reality (VR) devices?

No, Meta was not truthful.

“In a statement to The Post, Meta spokeswoman Dani Lever said that the allegation that Meta curtailed research is based on a few examples “stitched together to fit a predetermined and false narrative...””

This is not a predetermined, nor a false narrative.

“...and that the company has had no blanket prohibition on research about people under 13. Meta has produced research on youth safety in virtual reality and the company consulted children and their parents as it created the tween accounts, she said.”

We are not claiming that Meta has a “blanket prohibition” on research about individuals under 13. The issue is not whether research was done at all, but how difficult Meta made it to do research with *anyone* under the age of 18, despite there being a grievous need for it. In particular, required legal reviews significantly lengthened research timelines, which is often unacceptable for researchers, given that product teams and leadership demand they usually conduct and report research as quickly as possible. This process became even more arduous for researchers needing to conduct research with people under 13. Despite my title being the lead - and only - youth-focused VR UXR, I had to request special permission to conduct research with people under 13 to support Project Salsa - the purpose of which was to lower the minimum age of VR headset use from 13 to 10, meaning research with 10-12 year olds was *necessary*. Despite this, and despite the fact that leadership was pushing the Project Salsa team to move as quickly as possible, it took several months for my legal counterpart to even identify a path by which I would be allowed to conduct research with people under 13, despite this being something we had been discussing since the beginning of my time on the team many months prior. legal never permitted me to conduct research with individuals under 13.

“Lever added that Meta’s virtual reality devices have long had safety features including the ability to block problematic users, and over time the company has used research to develop additional protections for young people, including parental supervision measures and default settings that allow teens to communicate only with people they know.”

We are specifically discussing the presence of safety features *for children*, which Meta has only had for its VR devices since mid-2022, eight years after its acquisition of Oculus and six years after it released its VR headset to the market, despite copious existing research which indicated that children would likely be heavily early adopters.

With regards to the parental supervision measures and default settings - While these are good things to have, our documentation and declarations show that these are insufficient so long as Meta fails to (1) educate parents about the risks their children face in VR and (2) improve the quality of their age data to ensure teen users are actually using teen accounts - only then will features like parental supervision and social default settings be triggered.

““We stand by our research team’s excellent work and are dismayed by these mischaracterizations of the team’s efforts,” Lever said.”

We are the research team in question and we are not mischaracterizing.

“Meta did not directly dispute or confirm the events in Germany described by the researchers but said such a deletion would have been meant to ensure compliance with a U.S. federal law governing the handling of children’s personal data and with the General Data Protection Regulation, a landmark European privacy law that broadly prohibits companies from collecting personal information from anyone without consent. “Global privacy regulations make clear that if information from minors under 13 years of age is collected without verifiable parental or guardian consent, it has to be deleted,” Lever’s statement said.”

GDPR and COPPA (As I assume Ms. Lever meant by “a U.S. federal law”) only apply when collecting data directly from a child under 13 (i.e. interviewing them directly) or when dealing with personally identifiable information (i.e. their address). Neither of these circumstances were present in this case.

With respect to “If information from minors under 13 years of age is collected without verifiable parental or guardian consent,” we were interviewing the child in question’s *mother*, who gave explicit consent both before the interview and during, by urging her elder son to continue speaking about the younger son’s usage.

Meta told The Post that the headsets were meant only for people 13 and older and emphasized that the product packaging made that clear.

Here is everything Meta’s VR box says about child usage (on the bottom of the box in small font): “Parents: Not all children are ready for Meta Quest. See child safety guidance at QR code or meta.com/quest/parent-info. Meta accounts for 10+ (varies by region).” and, in another paragraph, “Not recommended for younger or smaller-sized children or if headset cannot be adjusted to fit properly.”

Nowhere on Meta’s box does it explicitly state the *minimum age of use for the headset itself*. I’ll also note that Ms. Lever appears confused regarding Meta’s minimum age of use - It’s 10, not 13.

“Meta said that lawyers have long partnered with research teams at the company and that there is nothing controversial about Meta lawyers advising researchers on attorney-client privilege or explaining that some work might require legal advice.”

That would be true if that was what Meta’s lawyers were doing. As clearly presented with first-hand knowledge and documentation submitted to Congress, Meta’s lawyers were actively interfering with research, including preventing some work from being done and editing some work after the fact to obscure findings.

“Changes instituted after Haugen’s disclosures were intended to make sure that research is high-quality and accurate, the company said.”

In context, this reads like Meta believes its lawyers are qualified to assess the quality of and manage the research process. They are not.

This is also *not what Meta’s lawyers were doing*. If that were the case, they wouldn’t have been prohibiting certain topics from being researched, but rather providing guidance as to the best approach.

“Meta told The Post that the company does not view app reviews as a reliable source of information about users’ ages and that it has better ways to determine how old users are.”

We did not assert that app reviews were being used to assess the ages of users. I used app reviews to gather qualitative evidence that children were being harmed using Meta’s VR devices and to identify what kinds of harms those children were experiencing. These were a public source accessible to me after Meta’s legal team had prevented me from conducting original research into this topic.

With respect to “It has better ways to determine how old users are”...not really. That’s why I had proposed Project Horton to research age assurance. Until Meta released its age verification solution, which only applies after the fact to require users to provide evidence of their age *if* Meta suspects they are underaged, it had relied *entirely* on stated age, which research across Meta’s products shows is highly unreliable. At this current juncture, using app reviews as an age signal might be a good idea until Meta develops a more robust age assurance ecosystem.

“The company disputed that a lawyer would be in a position to approve or a (sic) reject a study and said that lawyers never edit research results. Lawyers offer advice and suggestions, the company said, but research leaders ultimately determine which studies to pursue and the scope of their projects.”

Unfortunately, Meta’s assertions are wholly untrue. I and many of my colleagues repeatedly experienced Meta Legal explicitly approving/rejecting studies, editing research results, and determining the scope of our studies.

“Asked about the rush, Lever said the effort to create tween accounts came “on top of all the protections we had already in place” for teens.”

“All the protections” already in place at Meta were under adopted, ineffective and insufficient - and Meta knows this.

“Meta told The Post that it chose a 10-year-old cutoff so it could make sure it was offering age-appropriate content.”

Before Meta leadership made the decision to lower the minimum age to 10, *no* research was conducted on the age appropriateness of VR content, only on the headset hardware, despite myself and other researchers flagging this as a serious safety gap. When I and other researchers raised concerns that Meta’s VR app ratings were insufficient to help parents make meaningful decisions about age appropriateness, Meta flatly told us that it did not want to invest in this area.

“The company said it later implemented an initiative that asked headset users to confirm their birth dates. Those who said they were under 10 were removed.”

This Meta assertion is misleading and the company knows it. Any of Meta’s so-called protections that rely on self-disclosure are insufficient. The issues contributing to underage usage are (1) a lack of parent education and (2) a lack of reliability in stated age data. Asking users to verify their age under these circumstances means the majority of under age users are still going undetected, as parents may provide their own information to “verify” the account. Moreover children have shown that they are more than capable of finding clever work arounds (using someone else’s ID, using AI images for the face scanner, etc).

“Lever told The Post that leaders of the Reality Labs research team decided not to move forward with Project Horton because the company was already developing parental control tools and the initiative that asked headset users to confirm their ages by entering their birth date.”

Project Horton was formally reviewed and approved *after the parental supervision tools in question had already been released to the public*. There was no new information about the parental *supervision* (not “control”) tools which would have affected anyone’s opinion regarding the necessity of this project.

Asking users to confirm their ages by entering their birth date is a low confidence method for gathering age data. It is very easy and common for users to simply give false information - Especially when users and their parents aren’t aware of the risks which make providing an accurate birthday important. Reliance on “stated age” (as this was called internally) is the reason I had proposed Project Horton in the first place.

“An internal FAQ explaining the changes said the company’s “culture of openness” must now be balanced against “the risks that naturally stem from conducting and sharing research on sensitive topics and populations.” Meta told The Post that the changes were meant to ensure that research projects are accurate and findings are incorporated into the company’s product decisions.”

Meta's statements here are false. Meta research leadership and my legal counterpart both told me that this shift in culture and process was to "protect" myself and other researchers in the event our work was to be "leaked" to the public. I was also explicitly *told* by Legal that this shift was to "mitigate risk" to Meta.

"Meta told The Post that it requires users to verify their age with an ID or credit card if it suspects they are lying and that it created a tool to help third-party VR developers understand their users' ages."

Yes, *if it suspects they are lying*. This means the user will have already been using the product for some time, and that this will only happen for *some* of the underaged users on Meta's platform. A company prioritizing user safety should aim to identify underaged users *proactively* and *en masse*.

"In his affidavit submitted to Congress, the researcher wrote that he thought he was being told to avoid gathering data that could "implicate the company in future engagements with regulators." Meta said that characterization was inaccurate and that the lawyer was trying to help the researcher achieve the approved objective of his study, which did not involve collecting information about users under 13."

To be clear, a user above the age of 13 mentioning that someone - not in the room - under 13 is using a VR headset is appropriate and standard research practice, and is neither in violation of COPPA nor GDPR. If Meta were leveraging research in good faith, it would *want* to collect these insights, as they would indicate that there was an issue of underage usage which should be addressed.

a. A Meta spokesperson stated that Meta added more protections for young people on its VR devices. Are you aware of any protections that Meta added?

Meta's continued pattern of vaguely referring to "protections" and the like indicates that they are not approaching this conversation in good faith. Any features Meta has already added to its product are now public facing, meaning there is no reason for Meta to avoid citing precisely *which* "protections" it has added. If Meta's goal is truly to deliver safer experiences, surely it would wish to educate the public how to use its products more safely at every opportunity.

Meta has released additional features since my time on the team. We are not asserting that Meta has not released *any* "protections," but that the "protections" it has released are retroactive and insufficient - and Meta is aware of and disingenuous about the efficacy of these "protections." For example, the website behind the QR code on the VR headset box delivers concise and actionable supervisory and safety guidance for parents, *but* this information is needed in more discoverable places (for example, in a flyer *in the box itself*), as it is well established that putting information behind a QR code decreases the likelihood of people accessing it. Meta is aware of this through my own assertions, the assertions of my colleagues, and because this is general best practice within the UX field.

The core safety risks to young users which our disclosure has raised still have not yet been meaningfully addressed. If Meta's defense is that it has added new protections, why have those protections not meaningfully addressed the largest risks to the safety of young users? This too reflects Meta's bad faith approach to this conversation. At the time I left the company children were rampant in VR, and I regularly observed and heard accounts of children being propositioned for sex acts, groomed, harrassed, getting doxxed and more. The vague mentions of "protections" could refer to something as simple as moving the parental education page in front of the Meta account log in requirement (as they have recently done), a change which is certainly a good one, but which does not meaningfully address the fundamental issue that *user awareness remains low about the minimum age of use of their headsets and the risks of harm on platform*. For example, Meta has still not chosen to clearly and concisely state the minimum age of headset use on the box itself. Their own spokesperson did not even seem to know the minimum age of headset use when responding to this whistleblower disclosure.

Finally, Meta has a history of adding features and using their presence as proof that Meta is behaving responsibly, when these features do not necessarily make the experience safer. For example, Meta bragged about its parental supervision features for teen, then tween VR users, when existing research of which Meta was aware clearly showed that parental supervision features alone are not sufficient because they often go underutilized, and need to be paired with meaningful conversation (and co-usage for younger users). Meta's own internal data reflected this, showing low adoption rate of their VR parental supervision features.

Meta's spokespeople perhaps forget that some whistleblowers that are party to this disclosure are *still at the company*, and so the information we have about what "protections" Meta has added is current. I would like to see a list of the "protections" Meta's spokesperson speaks of, as well as a detailed explanation of why the company believes these efforts are effective, given the grievous nature and frequency of harm to which they are responding.

- b. Meta disputed your assertion that lawyers were able to approve or reject research projects, and they said that lawyers never edit results.**
 - i. Is this statement consistent with your experience at Meta?**
 - ii. Would a company lawyer being involved in child safety research interfere with such research?**

[b.i.] This statement is wholly inconsistent with my personal experience at Meta, as well as the experience of many of my colleagues, with whom I regularly discussed this issue. During my time in Meta's Reality Labs, legal interference was so frequent and disruptive that my UXR team spent numerous meetings discussing this issue. I was also told by researchers supporting a variety of Meta's products, including Instagram, Horizon, and Reality Labs more broadly (mixed reality, wearables, etc) that Legal interfered with their research, and witnessed this occurring on more than one occasion.

I will also note that Legal's leadership was well aware that Legal was acting in this capacity, as I experienced Legal directors engaging in this behavior themselves. UXR leadership was also aware that Legal was behaving in this capacity and told our research team on numerous occasions to defer to Legal when making decisions about research.

Legal interference I (and my colleagues) experienced included:

- Rejecting proposed areas of inquiry, stating that they were too “sensitive” or “risky” (This included investigating what kinds of harms children were experiencing in VR.)
- Editing specific research questions (meaning, within a specific area of inquiry, the more specific things we could investigate)
- Editing discussion guides and survey questions
- Editing research reports to remove or abstract information
- Controlling with whom research reports could be shared

To make this very clear, *Legal was given the power to behave in these ways by both legal and research leadership*, and there are *no other bodies that engage with research in this way, nor have this power at Meta*.

[b.ii.] Yes, “youth” in VR was my explicit area of study, and I was given a legal counterpart to review *everything* I wrote down which I intended to share with anyone other than my manager, and with whom I was instructed by my manager to discuss any plans for future research. Legal’s interference prevented me from investigating (1) the prevalence and causes of underage users in VR, (2) the harms these users experienced and potentially caused, (3) what could be done to address points 1 and 2.

c. Andy Stone, Meta Spokesperson, stated that Meta approved almost 180 studies on safety and well-being on its virtual reality platforms since 2022. How would you respond to this assertion?

This is an absurd statement which belies, at best, a fundamental lack of research literacy. That Meta would allow someone displaying such a lack of knowledge to speak on their behalf is itself concerning.

Firstly, the number of studies *approved* is not the same as the number of studies *conducted*. As we saw from the age assurance project (Project Horton) example, a study could be approved and still not be conducted.

Secondly, we have not claimed Meta’s Reality Labs has done no safety and well-being research. That was my colleague Dr. Sattizahn’s specific area of study for which he conducted numerous research studies. My specific concern is about the lack of due diligence with respect to the safety and well-being of *children* using Meta’s VR headsets, given their heavy presence in Meta’s virtual spaces. Children have meaningfully different safety and well-being needs from those of adults with respect to the usage of digital media, so dedicated research is necessary.

Thirdly, even the number of studies conducted is not a sensible metric by which to gauge Meta’s dedication to user safety. It matters what the studies’ areas of inquiry area are, with whom the research is conducted and at what scale, the truthfulness and directness with which researchers are able to report findings, whether other staff are made aware of the research findings, whether the research findings are actioned upon, and whether the actions taken are meaningful. As our evidence, disclosures, and testimony show, Meta Legal and leadership actively undermine these

steps. Given the grievous nature of the concerns under discussion, it would benefit the public if Mr. Stone could stay on topic in future communications.

2. What is the relationship between Meta's Reality Labs and Instagram?

Meta shares a variety of resources across its wide diversity of products, including Reality Labs and Instagram. The bulk of Meta's resources are dedicated to whatever area it considers to be its strategic area of focus at the time. Prior to 2021, Instagram was Meta's area of focus, such that the majority of its funding, talent, and headcount resources were concentrated there. When I joined Reality Labs in January of 2022, it was widely acknowledged internally that Meta's focus had shifted from Instagram to Reality Labs, such that the funding, talent, and headcount were being increasingly concentrated there instead. The implications of this were that people were transferring internally from Instagram to Reality Labs at an increasing rate, bringing with them established processes, knowledge, etc.

Internal transfers from Instagram to Reality Labs were very common, and there was no contextual training to make this transition. This actively caused issues, as VR is a general computing hardware device often used for gaming, and Instagram is a social media app. Folks coming over from Instagram often struggled to make the conceptual shift; I had to repeatedly explain to fellow Reality Labs employees, including leadership in C-suite, that VR was different from a two dimensional software experience and that this had strong implications for user safety and well-being (i.e. The immersive and embodied nature of VR means that harm has greater impact than equivalent experiences on any two dimensional app, and so establishing robust protections is even more critical in VR.).

Individuals coming over from Instagram to Reality Labs brought with them established processes, such as the rapid six month development cycle used for app development. This rapidity contributed to and, in some cases caused, user safety issues. For example, leadership demanded the VR Parental Supervision product team develop net-new parental tools for VR in less than a year, when this is something which needed significant research and careful thought.

Many employees work across products (i.e. Product Compliance and Policy), including VR/Reality Labs and Instagram, and make decisions which affect both of these areas. Some of these teams are even user-facing - For example, the Avatars team creates avatars which are used across both Instagram and VR, as well as a number of Meta's other products.

Some employees dedicated to Reality Labs' products also supported Instagram. For example, during my time in Reality Labs, I shared my VR research with Instagram teams to guide their decision making, and vice versa. I also partnered with Instagram researchers to conduct net-new research relevant to both of our products. Such knowledge sharing and collaboration is common and encouraged across Meta's products - Or rather, it was when I worked there.

Most of Meta's products are connected on the backend. For example, when I worked with the VR Integrity team to identify those users behaving maliciously towards children, the team noted that they were significantly hindered in their ability to do this. The problem was, the information VR users gave when setting up their VR headsets and accounts didn't correspond to information

they used when setting up their other Meta accounts (Facebook, Instagram, etc), so the team's access to existing information about the person (such as age) was more limited than usual. This is an example of just how normal it is for Meta's teams to collaborate and share information across products, including about its users.

Finally, Meta is actively pursuing avenues by which to create shared experiences across VR and Instagram in order to boost engagement. For example, Meta has been showing short video clips of VR on Instagram, and has been pursuing the creation of an "Instagram feed" within the VR homescreen. Not only are these products connected in a myriad ways on the backend, but Meta is actively seeking ways to connect them for the user as well.

3. What implications are there for user safety when Instagram or other social media content is integrated into VR?

Firstly, this is a privacy issue, given the high prevalence of VR headset and account sharing. Only one user's Instagram is going to be shown within the VR homescreen, and introducing an Instagram feed into VR means anyone in the household using the headset can easily access this person's private account.

Secondly, as I mention in my documentation and declaration, VR introduces new and more severe kinds of risks. Reading a bullying message in Instagram in real life may feel painful, but reading it in VR may feel even more severe - Research into the effects of this kind of experience don't yet exist within or outside of Meta.

Thirdly, overuse is a serious concern for VR, as the headset covers your eyes, making it difficult to perceive time passing in the real world. We already know Instagram can be addictive for both adults and children, but introducing Instagram (or any social media) into VR could potentially exacerbate this effect. Again, the research on this risk has not been done.

4. Meta has said publicly that its VR headsets are intended for children aged 10 and older. But based on the internal documents you shared, as many as 80 to 90 percent of users in some virtual rooms were under ten years old.

a. How are underage users able to access Meta VR?

Underage users are able to access Meta VR in two ways:

- Sharing a headset/account with an older user
- Using inaccurately aged accounts (i.e. their parent's account or an account the child intentionally made to have an older age)

Headset sharing is common, as VR headsets are expensive and most households do not own a headset for every household member. Account sharing is common, especially for younger users, for a variety of reasons, including convenience and the perception that this enables supervision.

Research indicated that parents are most involved in their child's usage of Meta's VR headsets during account creation, and that parents may create an account on behalf of their child, or instruct their child to create an account using the parent's information, to protect the child (by not

giving Meta the child's information) and to facilitate supervision. It is also very well established in research across digital media/experiences that children, especially tweens and teens, seek increasingly mature experiences, and so are likely to create adult-aged accounts for a variety of reasons (i.e. to have access to M- rated games).

b. Why is this problem still ongoing?

Firstly, because Meta has not sufficiently invested in parental education. Parents are largely unaware of Meta's stated minimum age of use for their VR headsets (it's not even on the box) and are largely unaware of the risks their children face when using VR. For these reasons, many parents do not understand why adhering to the minimum age of use or using accurately aged accounts for tweens or teens matters, and so they continue to allow underaged usage and inaccurately aged accounts. I want to emphasize that this education is not difficult to do - Simply doing things like putting a flyer in the VR box and putting the minimum stated age on a discoverable part of the box itself would go a long way.

Secondly, because Meta released this technology without setting the precedent for appropriately aged usage in the first place. Even the best approach to education about minimum age and risk is going to be less impactful now that the headset is in so many households and underaged usage is normalized.

Thirdly, because Meta refuses to invest in meaningful age assurance. As I discuss in my declaration, age assurance is comprised of stated age, predicted age, and age verification. To meaningfully improve their age assurance ecosystem, Meta needs to:

- Educate users and parents about why providing an accurate stated age matters (The reason is the risk children face)
- Investigate age prediction technologies, such as pupil distance, height determination, etc. This will require Meta to work closely with industry experts and parents to ensure this approach feels appropriate (This was the work proposed in my "age assurance" study, called Project Horton, which was shut down by Meta.), given that VR is a newer form of technology which enables novel forms of age prediction. It is of paramount importance that any new age prediction approaches feel appropriate, given concerns about user privacy.

Meta continues to assert that they now require age verification if they suspect an account is being used by a minor, but Meta knows that, without these other two steps, verification can be easily foiled and is unlikely to catch the majority of underaged users or users who should be using a tween or teen account.

These are the tactical reasons underaged usage continues, but all of these are things Meta could readily address - If it wanted to. The reason the issue persists is because Meta does not want to deal with the business downside. Meta is required to remove accounts when it becomes aware they are being used by underaged individuals. Doing so would decrease their usage metrics, which Meta relies on to demonstrate shareholder value. Meta chooses not to meaningfully address underaged usage in favor of maintaining inflated metrics for their shareholders.

5. What can Meta do to make VR safer? Why isn't Meta implementing these measures?

What Meta can do to make VR safer:

1. Meta should listen to its users and prioritize their safety.
2. Meta should begin investigating safety risks and mitigations *proactively*. Today, Meta tends not to conduct good-faith research on the safety of its products - including VR - until after it's already in a rush to get the product out to market. For example, Meta could have begun developing parental supervision features for VR when it first acquired Oculus, but instead waited eight years until it was already the subject of regulatory oversight to invest in this much needed feature set. Having multiple years to research these features would have ensured that Meta could produce an industry-leading experience, but they chose to develop something in a rushed manner and release a sub-par experience.
3. Meta should establish a practice of proactively referencing existing research and speaking with relevant experts - Many of whom they already employ. I witnessed Meta regularly ignore its *own employees* for whom they paid for their expertise, when it was perceived that engaging with the concerns the employee raised would generate "risk" or slow the team down. I also witnessed Meta ignore experts outside of the company. For example, Meta's VR policy team regularly engaged with industry experts to get their thoughts on Meta's approach to various aspects of its product. The concerns of these experts were regularly ignored.
4. Meta should enable its researchers to do their job (without interference from legal) in order to identify the risks users face and the paths towards addressing those risks.
5. Meta should *meaningfully* invest in accurately identifying the ages of its VR users. Any other safety features related to a user's age are meaningless without this.
6. Meta should *meaningfully* invest in parental education, especially regarding the minimum age of use, the risks that children face, and how best to keep young users safe (i.e. time limits, co-usage, etc).

Why Meta is not implementing these measures:

The things I've listed above would arguably be *more efficient* than any frantic, after-the-fact scrambling on Meta's part. Having a safer experience is better for the health of both the product and the company, as it increases usage, time used, company trust, sentiment, etc. Even Walt Disney insisted that investing in user safety as a pillar of development is just good business sense. The only conclusion I'm able to come to here is simply that Meta's desire to "move fast" and get products out in front of the public as quickly as possible is more of a priority than user safety. I might say that perhaps Meta doesn't understand the business value of trust and safety, but they employ *hundreds* of researchers who have repeatedly told them otherwise. Unfortunately, prioritizing speed over safety is a conscious choice.

6. Did the Meta legal team understand the safety implications when it instructed you to change studies and findings from your research?

Yes. In some cases, I explained the safety implications to them. In other cases, their instructions were *because* they understood the safety implications. For example, instructing me to remove mentions of users under the age of 13 or 10 meant they had to first be aware that underaged users

were being organically mentioned in research. If Meta responds here by saying their legal team didn't have a tidy list of safety risks, I will remind them that Legal's interference was the reason *they did not have that list*.

7. To your knowledge, has Meta ever brought in child health and safety experts to advise on virtual reality products?

Yes. Firstly, I was aware that Meta's VR policy team hosted a regular meeting (I believe it was monthly) with industry experts regarding VR, some of whom had relevant expertise in areas regarding child health and safety. Secondly, Meta *employed* individuals with this expertise, including former tenured professors of developmental psychology.

a. Did Meta's findings or recommendations align with what you were seeing?

No. I consistently saw Meta ignore the recommendations of the experts it consulted. Some of my colleagues who were child health and safety experts even expressed to me that they felt threatened by Legal for expressing concerns about the way Meta was approaching its VR product.

b. Did Meta implement or act on any recommendations from these experts?

I am not aware of Meta acting on any recommendations from external child health and safety experts. Meta has acted on the recommendations from some of its internal experts, but only when those recommendations aligned with Meta leadership's existing goal of quick growth. Otherwise, I know internal experts have had to fight hard to get the company to act on even very basic recommendations regarding child safety - for example, *putting the minimum age of headset use on the outside of the box*.

8. What was Meta Leadership's expressed intention in lowering the minimum age of virtual reality users?

Minimum age was lowered both for Meta's VR headset and for its VR social app Horizon.

With regards to the headset, I was shown a slide deck when "read-in" to this highly confidential project which included leadership rationale for lowering the minimum age. The rationale in that slide deck stated that Meta was seeking to lower the minimum age as a response to increased FTC pressure, and that they believed doing so would increase engagement.

With regards to the Horizon app, I was explicitly told by Tim Loving that leadership believed it would increase adoption and engagement.

9. On January 31st, 2024, Mark Zuckerberg testified that Meta does not instruct teams to focus on engagement.

a. Is this statement true?

No. This statement is false, and Mr. Zuckerberg knows that it is false. Throughout my four years

at Meta, I was embedded in Facebook Marketplace, Facebook Jobs, Buy and Sell Groups, and VR. For every one of these products, our *primary* directive was to increase engagement, many times at the expense of good user experience. Every time, I was told these directives came from Mark Zuckerberg himself.

b. If not, how were these directives shared at Meta?

These directives were shared by leadership in documents, in Workplace “posts,” and in meetings both big and small. Our success metrics usually reflected these directives. For VR specifically, Tim Loving (UXR director) explicitly told our team that Mark Zuckerberg wanted “every team” to focus on engagement.

c. Were they shared company-wide?

It depends on the scope of the directive - Sometimes directives are only relevant for one product (i.e. Just Reality Labs but not Instagram, Facebook, etc). However, (1) the directive from Mark Zuckerberg to focus on engagement was company-wide and (2) even before this specific instance, evidence that the standing directive for *the company as a whole* was to focus on engagement was pervasive.

QUESTIONS FROM SENATOR COONS

1. I co-lead the *Platform Accountability and Transparency Act (PATA)* which is designed to create mechanisms for independent research of social media platforms, their harms, and the effects they are having on users or society at large. In light of what you observed at Meta regarding their approach to internal research, could you elaborate on the value and importance of having effective independent ways to research platform behavior?

Meta has clearly demonstrated that they are *unwilling* to conduct good faith research on the ways their products affect users, particularly when they deem the area of inquiry to be “risky” to them. In example, Meta responded to Frances Haugen’s 2021 whistleblower disclosure by making it *more* difficult to investigate the effects of their products on minors, rather than facilitating this research openly and in good faith.

Given how pervasive social media is, and especially how much time people on average spend on social media, meaningfully understanding the effects these products have on us is critical to identifying risks to our individual health, well-being, and so on, as well as the risks to our health and well-being as societies, for social media impacts us both psychologically and sociologically. Meta’s consistent behavior has shown they are not willing to take responsibility for conducting and communicating research to this end on their own. Independent research would be a powerful tool to hold Meta accountable for the ways their products affect the public.

It is also critical to understand the *cumulative effect* social media technologies have on us (i.e. the use of social media across Instagram, TikTok, etc). This research must be conducted

independently to minimize bias - I would argue that it is impossible for for-profit companies to conduct unbiased research on their own products in a competitive context.

2. During your time at Meta and regarding the businesses you worked on or otherwise had insight into, to what degree did Meta facilitate independent research regarding the harms caused by their products? Was such research permitted or possible?

No, I am not aware of Meta facilitating independent research regarding the harms caused by their products. I *am* aware of independent research being done on the harm caused by Meta's products, but none of this research was done in association with Meta, and I was at times discouraged from sharing such independent research within Meta.

Meta does have programs which facilitate research through third parties, though none of this work is what I would describe as independent, as Meta enacts control over the process, including:

- The kinds of research questions which are prioritized
- The methodology
- How research participants are sampled
- The way questions are asked
- The way findings are represented
- What research findings are represented
- How research findings are prioritized

To be very clear - If there were good-faith independent research on harms caused by Meta's products, Meta's own employees would have a clearer understanding of the harms caused by Meta's products. And yet, there are rarely reports one can point to internally to confidently and concisely say "These are the ways in which our users are being harmed by our products." Instead, employees must often create a patchwork understanding across numerous documents, rely on word of mouth, or share the information with each other in secret. For example, when investigating possible harms children using VR were facing, I spoke with a Facebook researcher who shared a robust, exhaustive document citing research on bullying children experience on Facebook. The researcher cautioned me not to share the document with anyone, and not to tell anyone they had shared it with me.

3. Do you think there is more that Meta could be doing now to facilitate independent research into these products? What might that look like if Meta wanted to cooperate?

Before discussing Meta's facilitation of independent research, I think it is necessary to acknowledge Meta's current relationship to its own internal research. If Meta is actively interfering with good faith research being conducted internally - going so far as to remove findings from reports - I do not believe we can reasonably expect Meta to facilitate independent research in any manner with good faith.

There are ways in which research being conducted independently can protect the fidelity of the findings, but there are other ways in which Meta can actually interfere with the research in even

more significant ways. For example, research being conducted independently means, in theory, that Meta cannot control what research questions are prioritized, but this also means the independent research body will be comparatively limited because they won't have access to Meta's internal data. For example, if the independent research body wanted to investigate bullying on Instagram, they wouldn't have access to Meta's internal data about things like usage of Meta's safety tools (i.e. blocking, reporting, etc) unless, of course, *Meta gave it to them*. Given Meta's interference with its *internal* research, I can't imagine that we could expect them to engage in good faith with requests to reference user data in such ways.

In terms of what cooperation would look like:

- The independent research body would need to be fully in control of the area of inquiry, the specific research questions invested, the methodologies used, the sample used, the research conduct, data analysis, and reporting.
- Meta would need to work with an outside party to determine meaningful, appropriate ways to share existing research and user data with independent research bodies as needed. Data Meta provides would need to include the level of fidelity necessary for the research project, meaning it would not be appropriate for Meta to insist on providing only anonymized or aggregate data for certain studies. Data sharing of this kind is possible to conduct in ways which are respectful of user privacy and is common practice in other areas of research.

4. Based on your experiences, how would you expect Meta to respond to (or argue against) requests to facilitate such independent research, and how would you respond to their contentions?

Firstly, I expect Meta to say that they already work with independent research bodies, and to provide a vague quantification of this (i.e. "We work with over 50 independent bodies") or, at best, to cite a few bodies with no context (i.e. "We work with this NGO."). To this, I would say, whatever they're doing now clearly isn't working, given the known harm Meta products cause, and a conversation about user safety isn't the time to argue semantics.

There are *many* independent research and advocacy groups, as well as independent subject matter experts, who have clearly articulated what Meta needs to do differently regarding the safety of its products. If Meta were willing to listen to independent bodies, those changes would already have been made. For example, if Meta had spoken to Fairplay even briefly about parental supervision for VR, they would have prioritized robust, discoverable parental education. And yet, the parental education Meta chooses to provide remains buried behind a tiny QR code on the bottom of the box.

Secondly, I expect Meta will say that they *can't* share user data with independent research bodies because it would violate users' concerns about privacy. To this I would say, first, Meta's users are already deeply concerned about their privacy in Meta's hands. This is one of the main reasons parents don't give Meta their child's accurate age today. Secondly, I would say that Meta engages in this very behavior *constantly* when working with their third party vendors. Throughout the contractual engagement, the third party vendor may have access to relevant Meta log data, to

users' full names, phone numbers, emails, even addresses if the research is in person. Engaging with independent bodies would be no different.

Thirdly, it is possible that Meta will argue against this by making a defensive claim of its internal researchers. For example, Ms. Lever's response to our assertions in the Washington Post, "We stand by our research team's excellent work and are dismayed by these mischaracterizations of the team's efforts." To this, I would say the six whistleblowers in this disclosure *were* and *are* Meta's research team, and we have come forward precisely because we are concerned about the ways Meta weaponizes and suppresses its own internal research. The reason I am advocating for independent research is not because of any concerns with Meta's internal researchers, but rather it is because *Meta* has demonstrated that it will not let their own researchers conduct investigations in good faith.

5. What would you see as the greatest challenges to creating a process by which vetted independent researchers could study platform behavior in the businesses you have insight into? How could those challenges be addressed?

For platforms with such wide adoption as Instagram or Facebook, conducting research on their users would often be quite straight forward. Many independent bodies already do it. The biggest hindrance in my opinion will be the lack of access to platform/log data, for a few reasons. Firstly, users' perception or memory of their experience or behavior sometimes differ meaningfully from the reality. For example, a user may claim that they blocked another user, when in fact they did not successfully do so. These discrepancies are critical to understand, particularly when considering user safety and well-being. Secondly, having access to "log data" or internal data about how users engage with the product can be critical to identify trends without needing to survey all users (which is not possible). For example, seeing the log data which indicates that adoption of parental supervision features is very low. This information might be necessary for an independent research body to identify that this is a problem area requiring deeper inquiry, as, clearly, Meta cannot be fully trusted to identify the needed areas of inquiry. This particular challenge can be addressed, quite simply, through good-faith cooperation with the independent research body, provided care is taken to protect users' privacy in the handling and sharing of log data.

6. What would you see as most necessary to get right to have as effective a mechanism for independent research as possible?

It is critical that the independent research body be

- Protected as much as possible from Meta's interference, intimidation, and disparagement
- Attractive to researchers as a place to work in order to attract some of those experts who are currently under Meta's employ. This will require funding and tooling to enable high quality, expeditious research.
- Able to "move fast" to keep up with the speed of Meta's decision making, especially given this body would likely find out about decisions retroactively
- Able to meaningfully disseminate this research to appropriate bodies (i.e the public, regulatory bodies, etc)

It will be critical for any independent research body to have consistent, good faith access to Meta's usage and user data as appropriate in a manner which is respectful to users, and that the data Meta makes available to them accurately reflects users' real experiences - Not just the picture Meta wants to paint.

I, and the other whistleblowers taking part in this disclosure, are excited by the prospect of such an independent research body and are eager to support it.

7. Apart from independent research, what transparency (e.g., data, reports, etc.) do you think Meta could and should be providing regarding the businesses you have insight into so that the public, researchers, and policymakers can better understand the effects of its products?

Generally, Meta must stop censoring its own researchers, stop compromising the integrity of internal research findings, and must cease its bad faith usage of numbers/statistics to demonstrate responsible action. For example, Andy Stone's recent claim that Meta had "approved almost 180 studies on safety and well-being on its virtual reality platforms since 2022" belies either a fundamental lack of understanding of or care for research. The number of studies approved is not the same as the number of studies conducted (as we saw from the cancelled age assurance study), and the number of studies conducted is not a sensible metric by which to gauge Meta's dedication to user safety. This is a wholly meaningless response which underscores Meta's lack of willingness to discuss user safety in good faith.

In terms of more specific practices, Meta must shift to having a more open relationship with the public. Their products permeate the lives of individuals across the world, and I believe the public would greet open dialogue eagerly and actively.

- Sharing research: Today, Meta shares selective reports which are positioned to advocate for the company (i.e. Meta's Trust, Transparency & Control Lab). Given Meta's history, I believe a more robust, regular cadence of public disclosure of research would be appropriate, provided proprietary information is not shared, user consent is given, and PII is removed. This should be inclusive of both past and future research.
- Research for the public: I would also advocate for Meta creating a cadence of "research for the public." These would be studies done on topics the public cares deeply about (i.e. Instagram bullying) in which Meta makes public all relevant aspects of the study, including research questions, methods, sampling approach, timeline, discussion guides or survey questions, analysis approach, and final report. Meta should provide explanations for the decisions made about the studies (i.e. "Here's why we used this methodology"). The goal of these studies would be transparency and public education. I should note that Meta does currently make some research publicly available (i.e. their Trust, Transparency and Control Lab), but this research is cherry-picked to demonstrate Meta's good deeds.
- Public tracking of key metrics: Given Meta's history, I believe making public certain metrics related to user well-being and safety is needed. For example, making public the rate of adoption of its VR parental supervision tools overall, as well as the individual features.

- Enabling third party audits of the product development process and the products themselves: Meta must enable third party insight into *how* it develops products, as well as the outcomes of the products it creates.
- 8. Based on your experiences, how would you expect Meta to respond to (or argue against) requests for such transparency, and how would you respond to their contentions?**

Meta consistently employs a playbook in response to whistleblower disclosures such as ours which I expect to be repeated here. Broadly, this will look like Meta critiquing the validity of the ask, rather than engaging with it directly:

- Meta will likely claim that it is already being transparent, providing vague examples such as Mr. Stone’s “almost 180 studies approved.”
- Meta will attack the credibility of the requester, for example claiming the individuals making this request have an agenda or just don’t understand how much Meta allegedly already does.
- Meta will attack the credibility of any evidence provided, claiming it’s being taken out of context, isn’t sufficient, etc without specificity.
- Meta will play the victim. This may look like Ms. Lever’s statement to the Washington Post that our lawful disclosure was a “mischaracterization” of their research team’s excellent work, thereby positioning the critique as one not of the company but of specific employees who need protection. Or it may look like Meta’s internal communications that Frances Haugen’s 2021 disclosure made it difficult for researchers to do their job, thereby positioning the critique as one which unfairly hurts a company just trying to do the right thing.
- But, most importantly, Meta will not acknowledge the validity of the critique, no matter what.

My response to any of Meta’s contentions is this:

To respond to requests for greater transparency with anything other than meaningful engagement (such as, “Absolutely, how can we help?”) is to clarify that the safety and well-being of your users is not your priority. We are no longer having a conversation about the validity of the critique, because the body of supporting evidence and whistleblower accounts of Meta’s bad acts is too comprehensive, consistent and compelling to be ignored. At some point, highly consistent data becomes significant. Whether greater transparency is needed is no longer up for debate, so we ask Meta to stay on topic. Don’t try to distract us with a series of empty percentages or make this conversation about protecting your employees. We know how hard they work. Some of the whistleblowers that have come forward currently work for you. Help the public understand how your products affect them, so we can work *together* to make them better. Your users are telling you what they want. It’s time to listen.



**Senate Judiciary Committee
Subcommittee on Privacy, Technology and the Law**

**Written Statement of Jason Sattizahn
September 9, 2025**

Chairman Blackburn, Ranking Member Klobuchar, and Members of the Subcommittee.

Thank you for having me here. I am here to discuss Meta's manipulation of research to cover up dangers facing billions across Meta's products, and of particular concern, the millions of children using Meta's virtual reality products.

I also want to recognize and thank the five other past **and current** Meta employees – all researchers like me who worked directly on creating Meta's products – who made the brave decision to be a part of the disclosure that brought us here.

My name is Jason Sattizahn. Growing up in the nineties in the middle of Missouri, I saw both the value and problems that fast advances in technology brought the world. After earning a PhD in Integrative Neuroscience, I realized I wanted to use my research experience to make these technologies and products better for people that use them. Most recently, I spent six years as a researcher at Meta. I worked in some of Meta's most sensitive spaces, tasked with understanding users, their needs, and using this to try and make their products safer.

I am here today because it is evident that Meta consistently chooses profit over safety for its users. I am not the first to discuss this, as repeated whistleblowers have shared Meta's reckless disregard for users. However, in the wake of past whistleblowers, Meta has chosen to ignore the problems **they created** and **bury evidence** of users' negative experiences, rather than build safer experiences.

I worked at Meta from 2018 to 2024. During these six years, I witnessed data scandals, multiple disclosures about Meta's disregard for user safety and children's mental health, and mounting public pressure against Meta. I saw the company respond to these pressures by deliberately compromising internal processes, policies, and research to protect company profits over users.

Written Statement of Jason Sattizahn (Continued)

During my first role at Meta, I led integrity research for Facebook Marketplace. The data was clear - Marketplace causes suffering for users, including financial loss from stolen or counterfeit items, and personal safety issues ranging from being sexually propositioned **by strangers** to physical assaults and attempted kidnapping.

My time on Marketplace was my first exposure to how Facebook de-prioritized safety to boost user engagement. Simple safety investments such as not allowing people to message strangers with a single click were flatly rejected because product teams were afraid to do anything that could possibly decrease engagement - the metric largely determining success and bonuses. It was around this time I first saw Facebook make false statements to Congress. Contrary to Mark Zuckerberg's previous testimony before Congress, my research enables the company to estimate the overall rates of various types of harm occurring to Facebook Marketplace users. For instance, we can pair just one of the many studies I lead on this topic, estimating the extent of various harm based on estimates of Facebook's ~1 billion active Marketplace shoppers. For example:

- 9% of Marketplace users reported at least one negative experience in the past month (est. 90 million Facebook users per month).
- 0.5% of Marketplace users reported scams/counterfeit goods per month (est. 5 million reports of scams/counterfeit goods per month).
- 0.44% of Marketplace users reported harassment per month (est. 4.4 million reports of harassment per month).
- 0.3% of Marketplace users reported seeing drugs/alcohol per month (est. 3 million reports of seeing drugs/alcohol per month).
- 0.2% of Marketplace users reported stolen goods per month (est. 2 million reports of stolen goods per month)
- 0.16% of Marketplace users reported physical threats/assault per month (est. 1.6 million reports of physical threats/assault per month)
- 0.4% of Marketplace users reported seeing inappropriate images in Marketplace posts (est. 4 million reports of inappropriate photos per month)

When Facebook launched "Faith" efforts to connect religious communities during the Covid lockdown era, I joined because I was scared that Facebook's pattern of disregard for safety would surface in this already fraught context. Sure enough, my research on the use of Facebook for Faith showed large numbers of harms to Facebook users, including:

Written Statement of Jason Sattizahn (Continued)

- Facebook's own systems for detecting and removing inappropriate content online were faulty, often detecting religious content as "bad" and removing it; this caused multiple faith-groups to see Facebook as religiously persecutorial
- Facebook users' religious spaces would contain harassing, distracting, or otherwise distressing individuals in ways that harm faith-related experiences; this distressing behavior was at times intentional, and other times related to users not having common understanding of proper behavior in these spaces
- Other Facebook Faith users experienced severe physical safety risks, including being lured into public and harassed/assaulted based on their faith

Regardless, recommendations that I made such as creating well-understood community standards and expectations for behaviors in these spaces, and for the company to improve training we give operations teams to detect harm were shut down. Facebook instead focused on features to boost engagement, like an ability to respond to posts with a prayer hands emoji. The explicit reason given for my team focusing on new features rather than safety was because our team was expected to launch something to increase user engagement for the company rather than any other projects. This expectation was so strong that teammates I worked with on the faith team shared a deep fear that if they were not able to quickly build something to increase engagement, they could lose their jobs.

In the Fall of 2021, Frances Haugen disclosed to Congress how Meta's products fuel mental health issues for teens, including body dysmorphia and self-harm. Meta's immediate response to Congressional concern was **not to do the right thing**, but rather, roll out new processes and policies to manipulate, control, and erase data . Researchers were directed how to write reports so that risk to Meta was limited, and internal workplace groups were locked down, making it nearly impossible to share data and coordinate between teams to keep users safe. Mark Zuckerberg disparaged whistleblowers, claiming past disclosures were "...used to construct a false narrative." Meta CTO Andrew Bosworth began arguing 1:1 with researchers that dared question the new restrictions placed on research. Despite Meta's attempts to prevent researchers from collecting necessary insights, the research we were able to do continued to show the dangers of Meta's products on users. This only highlights the sheer scale, severity, and prevalence of harm occurring to those using Meta's products.

Written Statement of Jason Sattizahn (Continued)

What Meta had in effect created was a funnel of manipulation, the ability to review, control, and have retroactive power over all stages of research at the company. This enabled them to prevent, manipulate, or erase any research that could potentially reflect negatively on Meta or its products. This control included:

- **Surveillance by the legal team.** Researchers in sensitive spaces (i.e. integrity, safety, Youth) were given a legal partner they were required to consistently share research plans, data, and reports with for approval at all stages of work
- **Restricting data collection.**
 - Meta controlled topics researched, specific questions asked, and even types of research methods allowed, all to avoid negative findings
 - Meta monitored research when performed, in order to enact stop work orders and halt research if it was seen as too risky or sensitive
 - Meta demanded third-party contactors be used to house reports of user harm so Meta could claim ignorance to “knowing” these findings
- **Whitewashing research findings.** Meta would retroactively review reports to soften statements, edit evidence-backed claims by researchers, or erase findings entirely from reports
- **Research destruction.** Meta would have evidence entirely destroyed (i.e. recordings, notes, etc.) so that the only evidence that really existed of sensitive problems was the knowledge living within researchers’ themselves
- **Research isolation.** Meta would silo or segregate research they felt was too “risky” or sensitive, effectively limiting or disabling the ability for researchers to share their knowledge with others in the company

In early 2022, I moved to Meta’s Reality Labs to lead integrity research and to help improve the product so people were safe while they used Meta’s VR headsets. Generally, virtual reality allows someone to wear a headset and experience an alternate reality where they play games, watch movies, and socialize with others. For Meta, VR is designed to push socialization above all, as Meta saw this as a path to unbridled increases in user engagement and profit. The company invested billions, integrated social media like Instagram into headsets, and even rebranded as “Meta” to align with the future of the company.

From my first days in Reality Labs, Meta leadership and legal teams were in complete control of the research I was conducting. The research was crucial since this was a largely untested technology, but I soon learned that Meta had no interest in VR safety unless it could drive interactions, and thus, profit. Despite their efforts to control

Written Statement of Jason Sattizahn (Continued)

research, my first studies showed strong evidence of the harm happening to users of Meta Virtual Reality:

- Just shy of half of all VR users (44%) reported harm in the past three weeks when using their virtual reality headset
- These harms ranged from things like rudeness (39% of VR users) and entering others' personal space (19% of VR users) to racism (17%) and physical sexual advances (14%)
- Of people reporting harm in VR, an overwhelming 70% reported that it occurred in VR experiences meant for socializing – the same apps that Meta is actively and excessively promoting to people using their headsets

In this same research, I discovered that certain harms were worse for women using Meta VR, particularly sexual harms such as harassment, molestation, or worse:

- 26% of women reported experiencing sexism – compared to 14% of men – when using virtual reality
- 23% of women reported experiencing verbal sexual advances (e.g. sexual solicitation) – compared to 9% of men – when using virtual reality
- 17% of women reported experiencing other sexually inappropriate behaviors (e.g. broadcasting audio of pornography, broadcasting audio of actual sexual acts) – compared to 7% of men – when using virtual reality

For these women, this harm they faced in Meta VR also caused worse emotional and psychological harm, as well:

- Harm in VR caused negative anxiety or stress for 47% for women, compared to only 23% of men
- Harm in VR caused negative embarrassment for 39% for women, compared to only 17% of men

When I discovered these disturbing findings of what VR users were facing, Meta demanded that I not write any reports that showed that the harm was specific to Meta or Meta Virtual Reality, despite the data showing that was true. Rather, all reports were to show that this was industry-wide harm and not specify Meta. It was also after these studies that Meta made changes to my research, completely removing questions about psychological or emotional harm to their users. Their reasoning? They didn't "want" the data, as they decided it was too "risky" for them to

Written Statement of Jason Sattizahn (Continued)

know. Effectively, Meta had hard evidence that VR was causing their users – and women – psychological harm, but doctored research to prevent gathering that information in the future.

After Meta's VR sales were banned in Germany for two years over concerns about how Meta treats user data, in 2022, Germany allowed sales to resume. When I was asked to perform research in Germany, I understood that Meta was trying to show that their VR headsets were safe for German users. However, when our research uncovered that underage children using Meta VR in Germany were subject to demands for sex acts, nude photos, and other acts that no child should be exposed to, Meta demanded I erase any evidence of such dangers.

During my time working on Virtual Reality, I repeatedly saw leadership decide to invest resources on boosting social engagement at the direct expense of safety investments. At one point, Meta decided to allow children and people across devices, like phones or computers, to play together in their flagship VR app – Horizon Worlds. Meta had performed no research on how to make this experience safe for children or adults in this new space. As I pushed back and insisted on due diligence to prevent bad actors from hurting people, leadership explicitly told me that Meta had decided to launch without any safety research to “boost user engagement” in Horizon Worlds.

Meta's corruption of research for their own protection isn't limited to a certain product like VR, but rather, it is what defines the past, present, and future of Meta's products. In my work at Meta, I collaborated across multiple areas and saw how Meta had the same purposeful avoidance in addressing user safety across all their future-facing technologies. For example, my discussions with Meta's wearable tech (glasses, wrist technologies) teams showed me they were avoiding investments to proactively address user safety. Even Meta's own law enforcement team admitted internally that they investigated cases such as the use of Meta's Ray-Ban glasses in the 2025 New Years terrorist attack in New Orleans, but that due to internal restrictions, the team was not allowed to share information with product teams that would help Meta build this future hardware safely.

Despite Mark Zuckerberg's bold-faced lie to Congress that teams are not instructed to focus on engagement, that is exactly how the company operates. The pursuit of user engagement was the value that permeated Meta's every decision. For years, our work force was told that the directive to prioritize growth and engagement came from Mark Zuckerberg himself.

Written Statement of Jason Sattizahn (Continued)

Given how zealously Meta undermines reality, they will do their best to publicly undermine our disclosures with a counter narrative reflecting their unique version of “truth”. They’ll offer statistics without context or scale to prop up meager safety efforts. As they have done repeatedly, they may just lie to the government. They’ll clutch their pearls, claiming the whistleblowers are “taking research out of context”. Ironically, in coming forward to protect Meta’s users, I’m still doing the job that Meta originally hired me for. Unfortunately, my own experience and those of current Meta employees part of this disclosure show that Meta’s focus on engagement over safety continues to this day, driving their vision for their future products, such as AI, wearables, and the focus on miniaturizing new technologies to integrate with people’s everyday lives.

Meta is incapable of change without being forced by Congress.

Meta’s leadership will not willingly change their mindset and insatiable appetite for profits and growth at all costs. We are here because when Meta has been given repeated and frankly unearned opportunities to improve their product and take responsibility for suffering they have created, they have chosen to double down, deflect and deceive. To hide evidence. To punish those doing the right thing. To disregard and disrespect government bodies like yours instead of working with you to make positive change.

I believe that Congress can use what I and many others have disclosed to enact legislation and take action to compel Meta’s leadership to create the safe and accessible technology we all deserve.

Thank you again for the opportunity to be with you today and for your commitment to stop the **deliberate** harm for the millions of Americans who use this technology.

Senate Judiciary Committee Hearing
“Hidden Harms: Examining Whistleblower Allegations
that Meta Buried Child Safety Research”

Questions for the Record for Jason Sattizahn

QUESTIONS FROM SENATOR BLACKBURN

1. Was Meta truthful in its responses to the Washington Post story about Meta’s child safety practices in its virtual reality (VR) devices?

No. Meta’s responses to the Washington Post story about Meta’s child safety practices were dishonest, at best. Meta’s responses unsurprisingly follow a PR playbook I previously witnessed Meta use many times in the more than six years I worked at the company.

In the [Washington Post article](#), Meta spokesperson Dani Lever responded to our whistleblower disclosure claims that Meta had erased data on child grooming and sexual harm by invoking COPPA and GDPR, asserting, “Global privacy regulations make clear that if information from minors under 13 years of age is collected without verifiable parental or guardian consent, it has to be deleted.” This is an effort to misdirect attention. Meta claims to comply with COPPA and GDPR. If so, then Meta knows that COPPA and GDPR data regulations *only* apply if a researcher (i) collects data directly from children under 13, or (ii) if personally identifiable information (PII) is collected about someone under the age of 13. Neither apply to the research at issue. Our interviews were carefully planned and implemented to learn about sexual harm to someone under 13 without interviewing them directly, without gathering PII, and without gathering any additional information that could triangulate the identity of the child. Thus, it is not a violation of either COPPA or GDPR to keep the data of harm gathered and learn from it. Meta erased it, because - in their words - it was “too risky.” Even if COPPA or GDPR had applied in this case – which again it did not – the child’s mother gave informed, active, and verifiable consent in the interview to discuss this with our research team.

As cited in the Washington Post, Dani Lever’s statement also claimed that, “...the company has had no blanket prohibition on research about people under 13. Meta has produced research on youth safety in virtual reality...”. This, again, is an attempt to misdirect and mislead by omission. We six whistleblowers never claimed there was a “blanket” prohibition on research, but rather, research on safety, youth safety, and particularly those under the age of 13 are subject to inappropriate and misleading manipulation, misleading revisions and data deletion to cover up Meta’s knowledge of the harms to its users.

It’s also important to note that Meta spokesperson Dani Lever’s statements include her baseless conjecture that the whistleblower disclosure we brought forward was “...stitched together to fit a predetermined and false narrative.” Our disclosure brought forward with sworn declarations from six researchers who (i) were past and current Meta employees, (ii) had worked across all corners of Meta’s hardware and software products, and (iii) had first hand experiences from researchers showing a clear pattern of Meta’s behavior over nearly a decade. Moreover, we six

whistleblowers provided thousands of pages of documentary evidence that illustrate the claims of our disclosure. Calling this whistleblower disclosure either predetermined or false defies credulity, but it is consistent with how Meta regularly attempts to recast reality.

a. A Meta spokesperson stated that Meta added more protections for young people on its VR devices. Are you aware of any protections that Meta added?

The Meta spokesperson (Dani Lever) is again making public statements which are misleading in its omissions.

When Meta makes these vague and sweeping assertions, they are careful to omit context essential for the assertion to have value. There is no way to verify Meta's claims because there is no way for the audience to know *when* Meta "added more protections...". There is no way to quantify the addition of protections without any time frame to know if Meta protections are *more or less* than a prior timeframe. There is no mention at all of whether these protections have been implemented, whether these protections have been adopted or whether these protections are even effective.

To my knowledge, I am not aware of investments Meta made in developing or implementing *effective* or *meaningful* protections for young people in VR, including the research-backed protections myself and other researchers attempted to launch.

However, Meta Spokesperson Dani Lever cited one *specific* protection for young people as an example to validate Meta's claim of investments for child safety: parental supervision/controls and default teen settings. In my original declaration (Alpha Declaration, p.87), I review in detail how not only did Meta's own data show that people in VR overwhelmingly don't use parental supervision tools, but that for years, Meta knew that their parental supervision tools were insufficient for protecting teens. This is despite Meta, Mark Zuckerberg, and their spokespeople frequently touting parental supervision/controls and default teen settings publicly as alleged proof they are properly prioritizing child safety. Similarly, Meta's claims that default teen settings protect young people sidesteps the fact that default teen settings are only effective *if Meta has accurate age data for account holders and users*. As I reviewed in my original declaration (Alpha Declaration, p.141) and my supplemental declaration (p.12), Meta does not have reliable age data. Therefore, public statements using any efforts that are triggered by age as proof of Meta's care for child safety are a red herring and are knowingly misleading.

b. Meta disputed your assertion that lawyers were able to approve or reject research projects, and they said that lawyers never edit results.

- i. Is this statement consistent with your experience at Meta?**
- ii. Would a company lawyer being involved in child safety research interfere with such research?**

[b.i] This statement is not consistent with my experience at Meta, and nor is it consistent with the experiences of other researchers I worked with directly at Meta. In short, this is a falsehood. In spaces Meta deemed as "sensitive" (including child harm and emotional damage), Meta's lawyers reviewed all research at every stage of development, implementation, analysis, and the

sharing of findings to those who need the information. In fact, when Meta’s lawyers reviewed my own work at Meta, I was often told that:

- Entire studies or methods could not be performed because it would be “risky” for Meta to have knowledge of the data collected;
- Research studies could not continue until changes to the study were made to collect less incriminating data about Meta’s products;
- Data could not be analyzed in specific ways, as it ran the risk of producing results that could make Meta’s products look harmful to users
- How reports and analyses needed to be written, framed, or otherwise presented internally, all to limit risk to Meta; and
- To whom reports and findings could be shared to internally;

With rare exceptions, every research report I published at Meta after the 2021 Frances Haugen whistleblower disclosures was reviewed and had results *edited* by Meta’s lawyers.

It is important that in repeated instances where researchers – myself and others – objected to Meta Legal’s inappropriate manipulation of research, we were threatened with retaliation from Meta’s lawyers. Specifically, Meta’s lawyers told researchers that the only way to avoid “*negative outcomes*” for the researcher was to follow Meta Legal’s advice. In one instance of this, I was told that if I didn’t follow Legal’s advice, I may have to answer publicly about the negative aspects of Meta’s products that Legal revealed and that this would be undesirable. I understood that to mean that my public testimony would be undesirable for Meta and therefore I would not desire the consequences for resistance to Legal’s *direction*.

[b.ii] Yes - the result of Meta’s lawyers being involved in child safety research didn’t just add interference to researchers’ work, but it actively harmed our efforts to keep users and children safe. The interference of Meta’s lawyers meant that entire studies that were necessary to keep people safe were not approved. The legal interference meant that instead of using data we collected to learn how to make Meta’s platforms safer, the data was either distorted or erased, meaning that researchers often lacked the explicit evidence they needed to push for building Meta’s products to be safer (e.g. safety features, etc.). The dangerous consequence of this is that Meta does not collect *honest* data about the harm occurring to adults and children across Meta’s products. We researchers understood that Legal’s instructions served the purpose of giving Meta deniability about having knowledge of the harms their products expose users to, because after all, if no data and no truthful research findings survive, the truth only survives in the memory of the researchers.

c. Andy Stone, Meta Spokesperson, stated that Meta approved almost 180 studies on safety and well-being on its virtual reality platforms since 2022. How would you respond to this assertion?

This is yet another example of Meta misrepresenting the facts and misleading by omission. We have not asserted a complete absence of such research. In fact, many of the studies referenced by Andy Stone’s statement were performed by us six whistleblowers (despite the restrictions we

were forced to operate within). Much of this research has been included in our whistleblower disclosure and submitted as exhibits in support of our sworn declarations.

Rather, *our explicit and evidence-supported claim* is that when Meta researchers are able to conduct research deemed “sensitive”, the Legal staff assigned to direct and approve our work manipulate, distort, and maliciously prune data in order for Meta to avoid accountability for the harm their products do. Following a tactic from Meta’s familiar PR playbook, Stone’s comments misstate the claims of our disclosure and offer disingenuous achievements about Meta’s actions that are meaningless in their vagueness.

It is irrelevant how many user safety research projects Meta researchers manage to execute if they are deliberately designed to avoid data on actual harms experienced and are manipulated to give misleading findings.

2. What is the relationship between Meta’s Reality Labs and Instagram?

To the public, Meta has insisted that its products (i.e. Facebook, Instagram, Reality Labs, and WhatsApp) are independent from one another, and Meta has relied on that argument to sidestep congressional inquiry. However, this defensive characterization is a misrepresentation of the reality inside Meta. Internally at Meta, there are no hard divisions between Reality Labs and Instagram (as well as Meta’s other products). While each major Meta product can be framed as a part of Meta’s “Product-Based Divisions”, Meta generally operates like one single integrated company. These divisions share resources, systems, and a top-down strategy employed by Meta. Moreover, every employee at Meta, whether they spend the bulk of their time working on Facebook or Virtual Reality products, all receive a paycheck from Meta. The result is that employees constantly work across Meta’s products, for a number of reasons.

First, employees (and especially researchers) who are assigned to work on product-specific teams frequently work between product areas such as Reality Lab’s Virtual Reality and Instagram. This was the case with myself and my Virtual Reality team at Meta, as we worked directly with Instagram on multiple projects. In fact, employees are repeatedly encouraged and rewarded by Meta for collaboration, as Meta leadership sees this as advanced work.

Second, many teams at Meta are not product-specific, but rather are “horizontal.” The work of employees on a horizontal team inherently impacts multiple products at the same time. For example, employees working on Meta’s Avatars (i.e. digital representations of one’s own body) implement these avatars across Meta’s products. This means that if a VR team like mine collaborated with the Avatars team to change how Avatars function, it will largely impact both Instagram and Virtual Reality at the same time.

Finally, and of even greater concern, Meta is actively combining the experiences between products such as Virtual Reality and Instagram by integrating content from Instagram (e.g. Videos, Photos, Influencer content, etc.) into the Reality Lab’s Virtual Reality experience. This push is Meta’s efforts to have more content for users to engage with while experiencing immersive living in the virtual world. In this context, the experience of Instagram and Virtual Reality are essentially synonymous with one another.

Bottom line: Meta's Reality Labs and Instagram are closely intertwined. (1) Employees work intimately across both spaces, and (2) Meta is purposefully mixing the two together so that users can experience one (i.e. Instagram) within the other (i.e. Virtual Reality).

3. What implications are there for user safety when Instagram or other social media content is integrated into VR?

Meta's integration of Instagram, social media, and other content into Virtual Reality creates opportunity for these unexplored and untested experiences to impact users. Unfortunately, this impact includes safety risks for Meta's users, many of which I saw intentionally overlooked during my time at Meta.

Expectations of Meta's users. Any human experience carries with it an expectation of how that experience will work (e.g. when you go to the grocery store, we understand expectations of how we use carts or baskets), and when everyone shares a common expectation of how things work, things run smoothly (e.g. you return your cart after shopping so someone else can use it). Instagram and Virtual Reality experiences are different from each other and their respective users have different user expectations of what behaviors are appropriate. When Meta simply blends the two together, they're creating an environment where users have mismatching expectations, and it's this type of environment that is rife with risk, safety issues, and real world harm.

For instance, having been led to believe what is okay on one product is okay on the other, users may record content that is allowed in VR (i.e. content from adult spaces), but then share it on Instagram where it is inappropriate. Further to this point, users may not understand how to control their experience or stay safe when using Instagram in VR compared to a mobile phone (e.g. reporting others, using safety features), given that expectations of either experience separately is inherently different than when together.

Enforcement. When you blend Instagram (or any social media feed) into Virtual Reality, efficiently removing violating, offensive, or otherwise unsafe content for adults and children becomes even more complicated and potentially ineffective. For instance, Meta *already* has well-documented problems effectively reviewing and removing harmful content posted on their social media platforms. By enabling yet another surface (Virtual Reality) to distribute their social media content (Instagram), appropriately identifying, reviewing, and removing harmful content becomes more difficult. Another concern in blanket integration of Instagram into VR is that the mix of the two may create new or under-researched content that moderators will need to be able to identify, review and if harmful, remove. Reliance on existing enforcement systems or AI is not sufficient for keeping users safe.

Content & Ranking. Meta's products rely on algorithms called "ranking" to determine what content is appropriate and valuable to show people using their products. When Instagram content is surfaced in a new environment (Virtual Reality), it changes Meta's ability to effectively use ranking to determine if the content they show users is harmful or not. This requires Meta to proactively invest in altering their ranking algorithms to ensure harmful content isn't shown to either children and adults. Based on my experience working inside the company for six years, I

have no knowledge that this due diligence has occurred, nor do I have faith that Meta has done what is needed in this regard. Notably, Meta leadership's response to me raising this concern was, "Horizon Feed [Virtual Reality] content is going to use the same ranking from Instagram."

4. Meta has said publicly that its VR headsets are intended for children aged 10 and older. But based on the internal documents you shared, as many as 80 to 90 percent of users in some virtual rooms were under ten years old.

a. How are underage users able to access Meta VR?

Underage users can easily access Meta's headsets a number of ways:

- Sharing a headset and/or an account with someone who is an older age; again, I saw a long history of this behavior while working on VR, and evidence has been submitted to Congress showing Meta's explicit knowledge of headset and account sharing (SEE: Charlie_27, Charlie_90, Delta_7)
- Misrepresenting or lying about age; this occurs either directly or by linking their VR account to a pre-existing adult account to which they have access; I saw a long history of age misrepresentation across Meta's products and VR in my time there.

b. Why is this problem still ongoing?

Meta would prefer to limit their knowledge of underage users, these users' use of VR, or the strategies they employ for continued use. If Meta removed underage children, engagement in Virtual Reality would plummet, and Meta would be responsible to shareholders.

There are clear paths for Meta to limit the use of VR by underage users (and for that matter, across their products), which Meta simply does not do. For example, Meta could explicitly require verification of any adult account, which is not done at the moment. This would at least address verification at the stage of creating a VR account. This is just one place an intervention could help address the problem.

Verifying adult accounts doesn't stop adults from sharing their headset (and account) with an underage child. To address headset sharing, Meta could use a user's biometric data (e.g. facial layout, expressions, gait, etc.) to validate the user and to determine age. This is unlikely to happen at Meta voluntarily. The crux of the problem of age determination is that Meta would have to value a privacy-first approach to their products and adhere to strict data regulations to follow the law regarding handling sensitive data (rather than consistently trying to skirt triggering those regulations). During my time at Meta, this data was completely off limits for two reasons: (1) Meta wasn't confident in their ability to handle this data while respecting data regulations and (2) Meta knew that the public didn't trust them with sensitive, biometric data.

These are just a couple of examples of many that Meta *could* use to limit underage users' access to VR, if Meta had the will to address the problem. However Meta has demonstrated again and again that user engagement is their north star and handling user data responsibly is simply less important. At the end of the day, solutions require time, money, and effort that Meta doesn't want to spend.

5. What can Meta do to make VR safer? Why isn't Meta implementing these measures?

There is quite a lot Meta could be doing to make VR – and generally, all their products – safer. I'll separate these into two general categories: (i) company direction, (ii) product-specific investments

Company direction. Much of the lack of safety in VR is a symptom of how Meta has consciously decided to operate in order to solely focus on growth at all costs (e.g. user acquisition, user engagement, and achieving market dominance). For instance, one powerful thing Meta could do to make VR safer is simply investing more money into their safety teams. It is that simple. Meta will of course respond by citing the total amount of money they spend on safety and integrity efforts, but to be clear, they are not spending nearly enough to be even minimally effective. Over my six years at Meta, our product teams and operations teams were consistently under-funded, which directly led to important safety investments simply being ignored. With more money, safety teams could have built appropriate and effective tools, had more reliable and accurate moderation of VR spaces, and more. Meta simply does not increase these investments.

Another company direction that could change to increase VR safety is for Meta to simply listen and act on the safety guidance given to them by external experts. As I later outline in detail (see: the answer to question #7), Meta has purposefully ignored recommendations from experts on what Meta should do in order to make their products safer. However, if Meta was to take experts' advice, it would likely slow down product launches or alter products in such a way that limits the growth and engagement Meta desires.

Lastly, there needs to be a strong change in Meta's product culture, specifically in how Meta measures product success and the timescale at which they do so. Meta continues to operate with a "start-up" mentality, meaning that they generally dichotomize every product decision into incredibly small pieces, measure how those pieces change over a small timeframe, and make product decisions to quickly, incrementally boost product engagement metrics. The issue is that Meta's products are complex, nuanced and the experience (and safety) of their products is far from a simple sum of their parts. In order to build products that are safe for users, safety and integrity personnel can't be required to work on a short timeline or have the success of their work related to user engagement metrics. Again, these efforts would require Meta to allow at least some teams to slow down the relentless pursuit of growth, thus hurting their bottom line.

Product-specific investments. One of the most powerful investments Meta could make for safety in VR is collecting accurate age data. I review the importance of this in my original declaration (Alpha Declaration, p.141) and my supplemental declaration (p.12), but accurate age data is a necessary component to making so many safety features effective. Meta does not invest more in collecting accurate age data because if Meta had better age data, Meta would likely have to remove a large number of their accounts (and thus, user engagement would go down). Research Director Tim Loving made this point to me, explicitly.

Other effective safety tools (such as audio tools for users to stop harmful audio in real time) were not invested in, despite being effectively utilized by other tech companies, because Meta claimed

that the investment was “too difficult.” In the example of universal audio controls (like many other examples), Meta would have less difficulty building such features if they had built their products from day 1 with safety in mind. It is only “too difficult” now for Meta to develop and deploy audio controls because they don’t want to invest the necessary time and resources. Safety investments adversely impact product launch timelines and thus are considered a threat to Meta’s bottom line.

6. Did the Meta legal team understand the safety implications when it instructed you to change studies and findings from your research?

Yes. Meta’s legal team made informed decisions to change research studies in a manner they knew would negatively impact and hurt Meta’s users. I repeatedly, directly raised these concerns to Meta’s Legal team making clear that their actions in pre-emptively changing research designs, limiting research methods, altering reports, or erasing data were antithetical to keeping Meta’s users safe.

As an illustrative example, after one of my research studies discovered that experiences in Meta Virtual Reality led to emotional and psychological harm (particularly for women), Kristin Zobel from Meta Legal demanded that I remove all existing survey questions asking about emotion or psychological well-being. I objected to this directive, explaining (i) this was wrong because our past research already showed the relationship of VR and emotional/psychological harm and that (ii) removing it would kneecap our understanding on how to stop harm from happening. In response, Kristin Zobel became visibly frustrated and verbally confirmed my concerns, stating, “I know, this is ridiculous, but we have to do it.”

7. To your knowledge, has Meta ever brought in child health and safety experts to advise on virtual reality products?

Yes. During my time in Virtual Reality, I recall Meta allowing child health and safety experts to give their views and advise on virtual reality products. I also witnessed this occur on other Meta products such as Facebook and Instagram.

Furthermore many Meta researchers *are themselves child health and safety experts* who joined Meta from academic and non-industry backgrounds with the belief they could improve child safety on Meta products. However, this was far from the reality as throughout my time at Meta, I consistently saw Meta place the opinions of third-party experts above the opinions of Meta’s in-house experts, when the outside experts’ opinions bolstered Meta’s ability to shirk accountability.

a. Did Meta’s findings or recommendations align with what you were seeing?

From what I saw, Meta ignored the safety recommendations of child health and safety experts. Meta leadership would not even consider implementing expert recommendations that could potentially slow down the development of Virtual Reality or increase resource allocations for research to understand VR’s impacts on children and adults. Recommendations included taking time to better learn the impacts of VR on users, before lowering the ages allowed in Meta VR to

include those 10-12yo (“Project Salsa”). From Meta’s perspective, I understood that lowering the age floor would have the desired effect of reducing how many children could be considered “under age” as well as expand the market for their product since children drive adoption. Meta did not allow this recommendation to alter their plan to lower the acceptable ages of those in VR to include 10-12yo.

b. Did Meta implement or act on any recommendations from these experts?

No. I do not personally know of any implementations of safety recommendations Meta made to their products where the provenance was solely derived from the child health and safety experts with the goal of improving child health or safety.

8. What was Meta Leadership’s expressed intention in lowering the minimum age of virtual reality users?

Generally, there are two instances of Meta Leadership lowering acceptable ages in Virtual Reality that inform the answer to this question. First was Meta lowering the minimum age allowed in Meta’s flagship Virtual Reality app “Horizon.” In mid-2022, Meta decided to lower the minimum age allowed from 18yo allowing 13-17yo within Meta Horizon.

In August 2022, I asked the VR Research Director Tim Loving why Meta was allowing kids under 18 onto Meta’s Virtual Reality. I raised researcher concerns that this would cause harm to children. Tim Loving flatly told me that the release to wider audiences (i.e. children) would massively boost user adoption and engagement of Horizon.

The second instance of Meta lowering ages in VR is “Project Salsa”, when Meta allowed 10-12yo to begin using Virtual Reality. On one hand, Meta described in their internal documentation that lowering minimum ages allowed in Virtual Reality would be an “alternative” strategy to address the FTC’s increased pressure for Meta to improve the number of children under the age of 13yo on their products. On the other hand, Project Salsa was openly discussed between myself and internal teams as being a move for Meta to increase user engagement by allowing more ages of individuals to use VR. In Meta’s overview deck describing Project Salsa (See: exhibit Charlie_42), Meta makes reference to both:

- Meta describes lowering minimum ages in Virtual Reality as an “alternative” strategy to address increased pressure from the FTC to improve detecting and removing underage accounts. By decreasing ages allowed in VR to 10-12yo, Meta quite literally has to do less work to identify and remove underage users;
- Meta describes that apps we know to drive user engagement (like RecRoom) were blocking Meta’s users under the age of 13 in an undesirable way; and
- In the overview document, Meta even mentions the benefit of growth and retention that will follow as a result of this change to allow children 10-12 to use VR.

Beyond their own written documentation above, both my own management and leadership directly referred to the lowering of minimum ages as something that was happening “no matter

what”, and they referenced the belief that increased audience of child users would drive growth and engagement within Virtual Reality

9. On January 31st, 2024, Mark Zuckerberg testified that Meta does not instruct teams to focus on engagement.

a. Is this statement true?

No. This statement is absolutely contradictory to the reality inside Meta.

I was directly informed by Meta’s leadership that the focus of *all our work* must be tied directly back to user engagement. This engagement-first directive was constant and made repeatedly over the years I worked at Meta. Even as I repeatedly raised the inherent conflict of such a primary imperative to Integrity and Safety work, Meta never relented in basing success on user engagement.

b. If not, how were these directives shared at Meta?

These directives were shared from leadership, directly in meetings. In multiple instances, leadership in Virtual Reality (Director Tim Loving) informed Virtual Reality researchers that Mark Zuckerberg (CEO, Meta) had given this directive to VPs in the company, including Reality Lab’s VP Mark Rabkin. As such, we were expected to find a way to tie our work directly to increasing user engagement.

c. Were they shared company-wide?

To my knowledge, these directives were shared company-wide. In my own experiences, I witnessed individuals across Meta’s products pressured to relate everything they did back to user engagement, regardless of their focus. Additionally, given that Meta Leadership (Tim Loving) stated that this was a mandate from Mark Zuckerberg himself to his VPs, it follows that the directive would have been applied across Meta’s teams.

QUESTIONS FROM SENATOR COONS

1. I co-lead the *Platform Accountability and Transparency Act (PATA)* which is designed to create mechanisms for independent research of social media platforms, their harms, and the effects they are having on users or society at large. In light of what you observed at Meta regarding their approach to internal research, could you elaborate on the value and importance of having effective independent ways to research platform behavior?

The disclosures and the extensive documentary evidence from the six of us whistleblowers makes Meta’s approach to internal research abundantly clear. Meta cannot be trusted to ethically perform their own research internally at the company. Despite Meta’s success in hiring industry-leading researchers, they apply inappropriate control, manipulation, distortion and erasure to pervert research findings they don’t like. Without independent audits, Meta will continue to employ unethical tactics to bury knowledge and data documenting the harm their

products cause. Meta’s historical actions – including those exposed by our whistleblower disclosure – demonstrates that distorting the truth is no impediment when Meta is avoiding responsibility for its actions.

This is especially true in spaces that Meta themselves deemed as “sensitive” such as user experience research on safety and well-being, as well as research pertaining to susceptible or vulnerable users, such as children.

We know that Meta will not take appropriate action to address even their most egregious failures regardless of public pressure. Our whistleblower disclosure directly exposes how Meta responded to Frances Haugen’s 2021 disclosure by doing precisely the wrong thing. The 2021 whistleblower revelations triggered Meta’s systematic locking down and manipulation of research as well as implementing policies to prevent gathering meaningful data to keep children and adults safe. Meta’s compromises of internal researchers and their work needs to stop, but until then, it would be powerful to develop *independent* and *effective* ways to research behavior across Meta’s platforms. Just this one requirement would remove Meta’s ability to fully control and manipulate the research data collected, reports written, and the narratives about Meta product safety that derive from research.

2. During your time at Meta and regarding the businesses you worked on or otherwise had insight into, to what degree did Meta facilitate independent research regarding the harms caused by their products? Was such research permitted or possible?

Meta does have programs to facilitate external research, some of which does include harms caused by Meta’s products. In fact, during my time at Meta, I was directly involved with fielding potential researchers who were considering collaborating with Meta to perform such work. However, based on my direct involvement in these programs, I can confidently say that these programs are neither *independent* nor *efficient* for the purpose of running an independent research program and to produce unbiased research.

At the core, Meta’s facilitates its “independent” research programs in a way that allows Meta to maintain control over data and insights from the research itself. The limitations on potential third-party research studies that I witnessed while working at Meta made clear that Meta did not want to produce unbiased, independent research but rather engaged these projects to appease the public. Even in recent history, the timing of Meta’s announcements around “independent” research point to this. For example, while I worked for the company, Meta announced the “Instagram Data Access Pilot for Well-being Research” with the Center for Open Science (COS) on January 29, 2024. This was only two days before Mark Zuckerberg was forced by subpoena to appear before the Senate Judiciary Committee regarding child safety. The conveniently timed announcement enabled Mark Zuckerberg to make misleading claims of progress before the Senate.

For illustrative purposes, I’d like to actually use Meta’s “Instagram Data Access Pilot for Well-being Research” with COS to highlight issues with Meta’s “independent” research programs. One thing to keep in mind as I review these critiques is that Meta has placed numerous limitations on “independent” research programs and their access to data in the name of user

privacy. Despite us internal Meta researchers having relatively less restricted access to data, Meta *still limited internal researchers* from executing meaningful research on sensitive topics such as well-being. Thus, Meta maintained complete control of research externally and internally.

Approving research. Despite the COS program appearing as if they review and accept research proposals independent from Meta, Meta has a significant amount of control over which research projects can truly move forward in the “independent” research program. COS (and not Meta) are ostensibly responsible for selecting which research studies are approved. However, Meta reserves the right to, “...evaluate and respond to researchers’ Data Request Forms for their Registered Reports.” This effectively gives Meta a veto over research studies and the scope of their work/data they have access to if their study is to move forward. The *impact* is that Meta still retains actual control over what research topics are approved and which researchers ultimately gain access to Meta’s data.

This is *not* an “independent” process.

Controlling the data shared. One aspect of this external Meta research program is that the only data shared with research is “privacy-preserving.” On the surface, this sounds great, because it appears Meta cares about protecting Instagram users’ data. However, in practice, this requirement means that Meta is only giving sanitized data to researchers that limits their ability for researchers to understand the relationship of Instagram and well-being. For example, the explicit restrictions include requirements that:

- the data will not include the content from Instagram that people engage with (e.g. content, posts, or messages), meaning researchers lack context into what Instagram users are experiencing at all and how it’s impacting them; and
- The data will be aggregated or collapse in ways that removes researchers’ ability to know exactly what experiences or behaviors are actually impacting a user’s experience while using Instagram

The *impact* of how Meta is controlling data with this “independent” research program is that it destroys researchers’ ability to gain an accurate, appropriate picture of how Instagram relates to the social and emotional health of teens and young adults. Essentially - if Meta provides limited, poor data to researchers, it will result in limited, poor research findings. This only helps Meta further avoid their responsibility of keeping their users safe.

Just a few examples of how this is the case:

- By Meta not sharing data on the *content* people see (e.g. posts, comments, etc.), researchers will be limited in how they can understand causality between what Instagram users are seeing/experiencing and the impact to their emotional health. There may be overall relationships between variables that researcher may find, but due to Meta’s limited sharing of data, these findings will be high-level and easy for Meta to explain away if the resulting findings are undesirable for the company;

- By Meta sharing select limited, aggregate data, any conclusions that *can* be made would have limited value. Simple behaviors such as sharing a post are very different based on the context of what is being shared (e.g. sharing a meme vs. sharing hate content), and independent researchers making independent research decisions would not choose to limit the context of data being shared. Meta, however, is; and
- The COS' program website states that Meta's program is for "Enhancing Transparency and Reproducibility", but unless the program (i) shares data that internal Meta researchers have access to, and (ii) allows internal and external researchers to compare results, then implications that the program's goals are to enhance "Transparency and Reproducibility" is a farce.

Ultimately, Meta has created a system where they control the research and insights about their products both internally and externally. Our whistleblower disclosure offers both testimonial and documentary evidence that Meta manipulates and controls research internally, to further their narratives to shareholders and to the public. Meta's external, "independent" research programs are no different, as Meta has set them up in a manner to ensure that whatever data is collected reveals the least amount of damning information about Meta as possible.

3. Do you think there is more that Meta could be doing now to facilitate independent research into these products? What might that look like if Meta wanted to cooperate?

Yes, there is much more Meta could be doing to facilitate independent research into their products. It all starts with Meta stopping the manipulation of over research, data, and methodologies in order for researchers and experts to perform unbiased and reliable research.

- In any research program created, independence is required in the determination of: (i) the whole scope of appropriate and acceptable research proposals, (ii) methodologies allowed, (iii) plans for data analysis, (iv) the sharing of appropriate data based on the research question(s) and (v) the final form of research proposals to be executed.
- Meta needs to develop an appropriate, privacy-sensitive way to allow independent researchers access to Meta's data that does not fully remove content, context, or other data necessary to determine the impact of Meta's products on people. This is entirely possible to do safely while ensuring users' privacy - although Meta has failed time and time again to protect user privacy. Such appropriate and responsible approaches to sound research would require increased investment from Meta to develop and deploy procedures, reviews, personnel management, and legal processes.
- Meta could also form stronger bi-directional, undistorted knowledge sharing between internal and external researchers. For transparency and reproducibility, internal Meta researchers should be active in sharing ideas with those externally, and vice-versa.

4. Based on your experiences, how would you expect Meta to respond to (or argue against) requests to facilitate such independent research, and how would you respond to their contentions?

Based on my experience, Meta would likely raise numerous objections and create impediments to prevent or neuter independent research programs developed outside of their control because Meta's biggest fear is losing control over the narrative of their products. Their playbook in arguing against the need for an independent research program would follow the same pattern they have always used when they fear external pressure is weakening the absolute control they have over their product. Meta would likely argue that:

Meta already does enough. Meta would argue that they have created a number of "industry-leading", independent research programs, meaning that any new program or oversight for independent research is unnecessary. Meta would likely cite the overall number of research programs or the total number of studies that the programs have produced, hoping that the large numbers they cite mislead the public that they are doing enough. Unfortunately as I mention above, the total number of Meta's "independent" research programs or studies they've produced is moot without context. What matters is that Meta has retained control over these "independent" programs, undermining the efficacy of even having independent research programs.

Meta is better at understanding their products than anyone on the outside. Meta would argue that "independent" researchers are not as capable as employees internally at understanding the intricacies of Meta's products and the impact they have on users. Meta may cite that external researchers lack context into Meta's products, how they operate, or even lack an ability to perform the work itself - omitting the fact that Meta itself precludes research access to the data needed to perform the research. In fact, as I write my supplementary declaration on September 25, 2025, Meta spokesperson Andy Stone was making this precise argument on Twitter/X. He claimed that a recently released, truly independent third-party assessment of Instagram's safety tools is, "...a highly subjective, misleading assessment that repeatedly misrepresents our [Meta's] efforts..."

Meta is so concerned about user data privacy that it cannot possibly allow independent researchers access to the data they need. Meta would argue that further independent research programs – especially any requiring more transparent sharing of Meta user data to independent researchers – would “put users and their data at risk”. Meta has deployed this false rationale many times in the past, arguing it cares about users’ privacy too much to do this. In response, I would point out that Meta’s long history of violating user privacy would make this argument ridiculous on its face. Meta’s poor track record on user privacy includes but is far from limited to: (i) Cambridge Analytica, (ii) Texas biometric data, (iii) Illinois biometric data, (iv) tracking browsing while logged out and (v) the recent debacle with the Flo period-tracking app. Furthermore, as a multitude of companies and industries have proven, sharing data with independent researchers can be done in ways to mitigate risks to privacy. Sharing less filtered data in a privacy-protected way requires Meta to make significant investments that they have not and will not make voluntarily.

5. What would you see as the greatest challenges to creating a process by which vetted independent researchers could study platform behavior in the businesses you have insight into? How could those challenges be addressed?

Given what I describe above as being necessary for a truly *independent* and *effective* research program such as this, the largest and most immediate challenge I see is Meta themselves. Meta will use every resource – financial and legal – to stop the creation of any independent research program they see as removing direct control over their data and whatever possible research results are produced. The only way around this would be a government mandate.

Past that, the largest challenge I see is creating a way for independent researchers to *safely* gain access to Meta's raw, log data. This data is powerful for researchers to drive stronger, causal inferences between the content and experience of Meta's products and how this impacts Meta's users. There are clear privacy risks involved, but there are also investments that could be made to mitigate said risks. For instance, Meta could make good faith investments to improve research vetting before data is made available to researchers for their work. Increased investments into procedures around data access could be made. For instance, past scrubbing data of explicit PII, data could retain raw or classified content so that researchers understand specific experiences users engage with. When in tandem with controlled data workspaces, the risk of re-identifiable data emerging in a given report would be low.

There are other challenges including the logistics of managing Meta's data itself. From my own work at Meta, I can attest to how poorly managed Meta's user data systems are. I repeatedly found myself trying to hunt down (i) exactly who owned certain data sets, (ii) the provenance of the data collected, (iii) what data was actually included within data sets, and (iv) whether data sets were accurately storing the information they supposedly included. This challenge would require Meta's involvement to interface with any independent research program, all to shepherd them through roadblocks in understanding the data itself.

6. What would you see as most necessary to get right to have as effective a mechanism for independent research as possible?

Most necessary is to divorce Meta from having control over the research being performed. As I describe above, Meta has exerted control at every stage of research internally *and* externally to make sure they can control the narrative from any research output about their products. In their "independent" research programs I discussed, this included (i) what research can be conducted at all, (ii) what data will be made available to researchers, (iii) how that research will be made available.

Any independent research program needs to be developed with explicit, binding policy that leaves no gray area in the planning, execution, and analysis of research where Meta could prevent, alter, bury or otherwise manipulate research to be biased for the sake of Meta and their brand. Based on past experiences, we know that if there is any gap in a program policy, Meta will invariably exploit those loop holes to manipulate research as much as they can.

I need to say - in the advent of any potential independent research program of this sort, I would be more than happy to contribute to helping design it to prevent such exploitation from happening.

7. Apart from independent research, what transparency (e.g., data, reports, etc.) do you think Meta could and should be providing regarding the businesses you have insight into so that the public, researchers, and policymakers can better understand the effects of its products?

In my view, the best steps for transparency that Meta could and should take is becoming transparent with the public, in terms of their research practices, the data they collect, the reports they make (and choose not to invest in), and the ongoing data Meta collects about users' experiences. It is possible for Meta to re-build itself with a more "open research" approach, while also mitigating business risks that the company may be concerned about:

- Report availability. Meta could make internal research reports (redacted of proprietary corporate information and of PII) available for public access. This could look like a public repository with tagged, cataloged reports that helps the public walk through what Meta knows about its users, the data Meta collected, and the conclusions that Meta is making as a result
- Live tracking of metrics and user data. Meta could make public a live feed of metrics and data that they collect about the experiences on their platform. This could be a real-time dashboard including measures such as content removed from Instagram, user reports made in Virtual Reality, or any number of user-facing measurements being tracked by Meta. Of course, specific measurements requiring sensitive handling could be carved out from inclusion.
- Open audits from third party assessors. Meta could make its internal machinations completely open to external audit by independent research assessors. This would allow an unbiased view of Meta's data retention, data management, research processes, and other related items.
- Truly independent research partnerships. Meta could establish bidirectional, good-faith, and truly independent partnerships with researchers external to the company. On one hand – as I discuss in part above – this would require Meta to relinquish the pre-emptive restrictions and limitations that they impose on "independent" research partnerships by either asserting oversight for research design, methods, or overly compromising the integrity of data passed to researchers. On the other hand, this could also look like Meta is committed to building a stronger platform for internal and external researchers to keep each other accountable. Other key elements to enable independent and reliable research would be to allow Meta researchers to share concerns about Meta's research practices or methods (washed of any proprietary data) to an external research body - and - to allow external researchers to directly partner and critique the development of internal studies. There are numerous ways these processes could be built responsibly.

8. Based on your experiences, how would you expect Meta to respond to (or argue against) requests for such transparency, and how would you respond to their contentions?

Based on past history, Meta's contentions would likely follow a similar pattern to what I outline in question #4 above. I would expect Meta to claim:

Meta already does enough to be transparent. Meta would argue that they already go above and beyond “other companies” to stay transparent, and they would likely attempt to cite their efforts around data (e.g. the Meta Content Library and API) and independent research (e.g. Research Awards and Requests for Proposals (RFPs), collaboration with Center for Open Science, etc.) as a way to convince the public that additional transparency levers are not necessary.

In response as I outlined above, I would point out that Meta’s transparency efforts have been purposefully developed so that Meta retains tight control over what research is executed, the extent of meaningful data shared to be analyzed and who is permitted to even see the research or its findings. The result is that Meta is able to limit researchers’ ability to produce unbiased research that accurately portrays the impacts of Meta’s products on people.

Research and data will be taken out of context. Meta would likely argue that if their internal research and data is made more public and transparent, then their work will be discussed out of “context” and to create “false narratives.” This is a refrain I have heard from Meta repeatedly, especially when the public is given irrefutable evidence showing the harm that Meta’s products do to people. In November 2021 and in response to Frances Haugen’s whistleblower disclosure, Meta circulated documentation internally featuring Mark Zuckerberg himself stating that the disclosure was, “...work taken out of context and used to construct a false narrative.” More recently on September 8, 2025, Meta via spokesperson Dani Lever critiqued this very whistleblower disclosure in the same way. Lever stated that the evidence we present derived from our extensive experience as Meta researchers was, “stitched together to fit a predetermined and false narrative,” and that Meta was, “...dismayed by these *mischaracterizations* of the team’s efforts” (emphasis added).

My first response to this is that as researchers, we hold the context of the research and knowledge produced about users. Meta cannot make the argument that research is being taken out of context if it is researchers themselves who disclose the work, speak about it, or otherwise frame it to the public. Any context Meta would add above that of researchers would be to obfuscate or control the research in order to protect their unethical business practices. This is the same response Meta has to *any* exposure to the public of the negative impacts Meta’s products have on their users, making it clear that Meta is not capable of reliable, unbiased, or truthful narration about their own research.

This could harm user privacy. Again, it is predictable and likely that Meta would hide behind an assertion that Meta is “doing the right thing” by restricting data access, since increased transparency could be a “risk to Meta’s users”. Meta would claim that sharing more detailed data *or* having less oversight into research selection, development, or data handling would inherently put their users’ data and the privacy of said data at risk.

There are two strong responses I have to this. First – as I review in more detail in response to question #4 – Meta has an incredibly long history of *violating their own users’ privacy and improperly handling user data*. Second, the relationship and balance between transparency into Meta research and ensuring privacy of user data is not some zero-sum game. It is possible for Meta to both increase transparency into their research and share more granular user data, and to build mitigations to ensure user data is also handled properly. The core issue is that it would

require Meta to commit to investments in both transparency and user privacy, something that isn't the highest grade on Meta's report card.

This would offer too much risk to Meta. Meta would likely argue that an increase in transparency is an unfair risk to their business model. For instance, they may argue that sharing in greater detail their research and data could expose the company to competitive risk (e.g. information shared could help their competition), legal risk (e.g. information shared could implicate Meta for criminal or civil liabilities), or brand risk (e.g. information shared could make their company look bad).

First, arguments around competitive risk are overblown, to say the least. Not only does Meta have a near two-trillion dollar market cap, but they have arguably achieved a monopoly on global social media use, Messaging services, Virtual Reality, and other emerging technologies and hardware. Second, I would respond that no one should have concern for legal risk to Meta: (i) legal implications from increased transparency would simply be a result of Meta's own behavior, and (ii) as our disclosure clearly shows, Meta has weaponized their own legal team to knowingly perpetuate Meta's misconduct and cover up of the harm of their products. Third, brand risk shouldn't be a concern to Meta, as it doesn't appear that public sentiment of their brand could go any lower.

TEEN ACCOUNTS, BROKEN PROMISES

HOW INSTAGRAM IS FAILING
TO PROTECT MINORS

REPORT BY

**ARTURO
BÉJAR**

**CYBERSECURITY
FOR DEMOCRACY**

 **fairplay**
childhood beyond brands

 **MOLLY ROSE
FOUNDATION**

 **ParentsSOS**
EXPERTS FOR SAFE ONLINE SPACES

WITH SUPPORT FROM

**HEAT
INITIATIVE** 

TABLE OF CONTENTS

4 FOREWORD

6 INTRODUCTION

11 A REPORT ABOUT BROKEN PROMISES AND DANGEROUS DESIGN, NOT CONTENT

13 METHODOLOGY FOR TESTING USER-FACING SAFETY FEATURES ON INSTAGRAM

18 HOW TO BUILD EFFECTIVE SAFETY AND USER REPORTING FEATURES FOR CHILDREN

22 OUR FINDINGS

24 Inappropriate Contact and Conduct

- 25 Meta's Broken Promises: Improper Contact and Conduct
- 26 What Meta Promised
- 27 Key Findings
- 31 Recommendations for Meta
- 32 Questions for Regulatory Inquiry

33 Sensitive Content

- 34 Meta's Broken Promises: Sensitive Content
- 35 What Meta Promised
- 37 Key Findings
- 41 Recommendations for Meta
- 42 Questions for Regulatory Inquiry

43 Time Spent and Compulsive Use

- 44 Meta's Broken Promises: Time Spent and Compulsive Use
- 45 What Meta Promised
- 46 Key Findings
- 48 Recommendations for Meta
- 49 Questions for Regulatory Inquiry

50 Age Verification, Minors and Sexualized Content

- 51 Meta's Broken Promises: Age Verification, Minors and Sexualized Content
- 52 What Meta Promised
- 53 Key Findings
- 56 Recommendations for Meta
- 57 Questions for Regulatory Inquiry

58 CONCLUSIONS

61 APPENDIX

62 Appendix 1: Summary of Detailed Findings

72 Appendix 2: Scoring Rubric Applied During Safety Testing

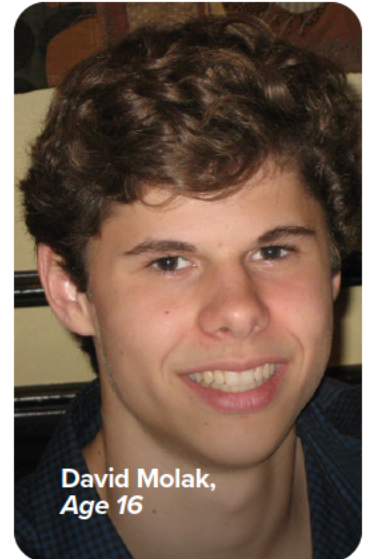
73 Appendix 3: Detailed Findings

76 ABOUT THE AUTHORS

FOREWORD

We are two people who know all too painfully the tragic results that occur when Mark Zuckerberg and his fellow Meta executives choose not to prioritize safety for minors.

Maurine's son David was an outstanding basketball player and avid sports fan, beloved by friends and family alike. But when he injured his back and couldn't play sports, he became addicted to gaming and social media — and endured months of threatening cyberbullying on Meta's Instagram. Even though we made sure he had mental health support and even switched schools to get David away from his tormentors, it wasn't enough. The online attacks continued, and in January 2016, David took his own life.



Ian's daughter Molly was 14 when she was bombarded by suicide, self-harm and depression posts on Instagram. Molly loved music and theatre, but the content she saw online contained a dark vein that made her feel as though she was worthless and encouraged her to end her life. Molly saw more than 2,000 disturbing posts on Instagram alone in the six months before she died. These posts were being algorithmically suggested to Molly to such an extent that the coroner came to an unprecedented conclusion: The negative effects of social media contributed to Molly's death in a more than minimal way.



It's been almost eight years since Molly's death and more than nine since David's. Thanks to a slew of whistleblowers, lawsuits, academic research, and regulatory inquiries, we know a lot more about Instagram and Meta. We understand now that the deliberate design choices made by Meta contributed to the harms experienced by David, Molly, and countless other young people. We understand that courageous individuals within Meta tried on many occasions to sound the alarm on how Instagram's design was contributing to mental health harms for teens, but were rebuffed by senior leadership. We understand there are real steps that companies like Meta could take now to make their platforms safer and less addictive. Steps that would save lives.

Unfortunately, as this report so clearly describes, Meta has chosen not to implement those measures, opting instead for splashy headlines about new tools for parents and Instagram Teen Accounts for underage users. As we have demonstrated, Meta's new safety measures are woefully ineffective. If anyone still believes that the company will willingly change on its own and prioritize youth well-being over engagement and profits, we hope this report will put that to rest once and for all.

Time and time again, Meta has proven they simply cannot be trusted. To prevent future tragedies, we need real regulation. In the US, that means passing new legislation like the Kids Online Safety Act, which would require social media companies to prevent and mitigate the harms to young people caused by platform design. In the UK, that means strengthening the existing Online Safety Act to compel companies to systematically reduce the harm their platforms cause by compelling their services to be safe by design.

We lost our children nearly a decade ago. We implore everyone reading this: Help us make sure that not one more child is lost to Meta's greed, and not one more parent has to live with a grief like ours.



Ian Russell

Chair of Molly Rose
Foundation



Maurine Molak

Co-founder of David's Legacy
Foundation and ParentsSOS

INTRODUCTIONS



Meta has failed to prioritize child safety until they are scrutinized by outside regulators. Then they scramble to develop features they know are inefficient and largely unused, and advertise this as proof of their responsibility.

Meta whistleblower Cayce Savage testifying to the Senate Judiciary Committee on Sept. 9, 2025.

In September 2024, Meta announced that it was introducing Instagram Teen Accounts and that all teenagers would automatically be enrolled in the new program. According to the announcement, the launch was meant to “reassure parents that teens are having safe experiences.” Added Meta: “This new experience is designed to better support parents, and give them peace of mind that their teens are safe with the right protections in place.”

Meta’s announcement came right before an important hearing in the U.S. House of Representatives on the Kids Online Safety Act (KOSA). This timing was almost certainly not coincidental. KOSA is the most important legislation of its kind to make significant progress in Congress in over 25 years. Meta has lobbied extensively to stop KOSA — and to influence in its favor legislation in the United Kingdom, European Union, and elsewhere that would hold the company responsible for its design choices that harm teens.

Meta’s announcement also followed years of revelations from journalists, whistleblowers, and lawsuits that revealed how the company knew Instagram’s design was causing serious harm to young people, but top executives refused

to make changes to make the platform safer. While the ostensible audience for Meta’s announcement was parents who were increasingly concerned about how much time their children spent on Instagram and what they experienced there, Meta also was seeking to reassure lawmakers that the company was addressing those concerns and did not need to be regulated.

According to Meta, Teen Accounts have a number of safety features that differ from regular adult accounts: They are private by default, teens need to accept any new followers, and anyone who doesn’t follow them can’t see the teen’s content or interact with their accounts. Teen accounts are also given the strictest messaging settings and the most restrictive Sensitive Content Controls, Meta says. In addition, if teens are on Instagram for 60 minutes in a given day, they will receive a notification telling them to leave the app. According to Meta, with Instagram’s “sleep mode,” teens’ notifications will be muted, and their direct messages will receive autoreplies, between 10 pm and 7 am.

The launch of Instagram Teen Accounts promoted not just new safety features for teens but a number of new promises for parents. According to Meta, teen account holders under the age of 16 need a parent's permission to change the settings of any of the built-in protections for Teen Accounts. If your teenager is over 16, you can simply turn on parental supervision, which allows you to approve or deny their requests to change their account settings.

According to Meta, the supervision feature also gives parents other ways to get involved with their child's experience on Instagram. This includes parents being able to see whom their teen has messaged in the past seven days; set daily time limits for Instagram usage; block teens' access to Instagram for a specific time period; and see what topics their teens are looking at.

To parents and other interested observers who did not rigorously validate these claims, it would appear from these statements that Meta had fully addressed these hazards and children were again safe. But children are not safe on Instagram.

We undertook a comprehensive review of Meta's Teen Accounts and all of the safety tools in Instagram listed on Meta's website. Many of these safety tools preceded the announcement of Teen Accounts, while others were introduced when Teen Accounts launched. Our review included both these longstanding tools, which have been aggregated under Teen Accounts, as well as the new tools.

Meta's list includes 53 entries about Instagram's safety features. The list is immediately misleading, given that it includes tools that have been discontinued (for example "Take a Break"), or fundamentally changed so as to not serve their original purpose (hiding view counts on posts). Some of the announcements are ostensibly improvements on existing safety tools. Our comprehensive reviews of Teen Accounts and safety tools included testing 47 of Instagram's 53 listed safety features (the reasons are outlined in the Research Note by Cybersecurity for Democracy).

47

SAFETY FEATURES TESTED

RATED RED

RATED YELLOW

RATED GREEN

64%

19%

17%

Using a three-tier framework — red, yellow, and green — our researchers systematically evaluated each of the 47 Instagram safety features. Each safety feature was assessed according to its effectiveness, usability, and visibility. **We rated 64% of the safety tools as “red” (30 tools) because they were either no longer available or ineffective. Another 19% of safety tools (9 tools) reduced harm, but came with notable limitations. Only 17% of the safety features (8 tools) worked as advertised, with no limitations.** Many of the safety tools that were ineffective are the foundation of Teen Accounts, including Sensitive Content Controls, inappropriate contact safety, and tools for kids to manage the time they spend on the platform. The minority of tools that worked address limited use cases and hazards. Given that several ineffective tools were announced years ago, we cannot estimate the harm that teens have experienced as a result. These findings are discussed at length in the report and our “red, yellow, green” rubric is discussed at length in the appendix.

We hope this report serves as a wake-up call to parents who may think recent high-profile safety announcements from Meta mean that children are safe on Instagram. Our testing reveals that the claims are untrue and the purported safety features are substantially illusory. But we also urge regulators and lawmakers to consider the substantial evidence that the majority of Meta’s safety initiatives have been little more than PR efforts. We cannot waste any more time, or allow more children to be harmed, by Meta’s self-regulation.

In the United States, those interventions include passing KOSA, which would create a duty of care for social media companies to ensure that the design of their products is not contributing to serious harms for minors, including addictive use of platforms. It also means that the Federal Trade Commission and state attorneys general hold Meta accountable for violating the Children’s Online Privacy Protection Act and Section V of the FTC Act.

In the UK, the Government should strengthen the Online Safety Act to ensure that regulation is more effectively focused on achieving measurable harm reduction, alongside other structural remedies that will put the onus more directly on platforms to identify and take effective steps to mitigate reasonably foreseeable harm. The regulator, Ofcom, must also become bolder and more assertive in enforcing its regulatory scheme.

Note: Cybersecurity for Democracy did not participate in writing this section and by policy does not endorse any legislation.

RESEARCH NOTE FROM CYBERSECURITY FOR DEMOCRACY

For many years, Meta and other companies have responded to growing concerns about youth safety by rolling out new user-facing safety tools. These announcements often arrive at moments of public scrutiny or looming regulation. As researchers, we had a simple question: **Do these tools actually work?**

To answer it, we borrowed from established practices in cybersecurity. Our team partnered with Arturo Béjar to apply “red team” style scenario testing to user safety tools on Instagram, taking a well understood security methodology into a new domain. To do that, we systematically identified every announced Instagram safety feature, designed controlled test scenarios for each to reflect real teen, parent, and adversary behaviors, and ran those scenarios with realistically configured test accounts. We also developed a taxonomy of the key dimensions of user-facing safety tools, to allow us to analyze these tools and features in a more systematic way.

In March 2025 Arturo Béjar undertook an initial round of testing, and in June and July 2025, we worked with Arturo to independently perform this scenario testing, performing a comprehensive review of Meta’s Teen Accounts and all 53 descriptions of Instagram safety tools listed on Meta’s website under “Our tools, features, and resources to help support teens and parents”. It’s important to note that this is a list of press releases, not a list of currently active tools, however. For example, several of the features listed have since been discontinued, a fact which isn’t noted on this page. Additionally, several announcements describe changes to existing safety tools, rather than separate tools.

Ultimately, our scenario testing of Teen Accounts and safety tools included 47 of these 53 listed items. Two safety features were not analyzed for methodological reasons, and four others on the list did not primarily relate to safety objectives and so were not included in our analysis.

More research into social media user safety tools is urgently needed. Our findings show that many protections are ineffective, easy to circumvent, or have been quietly abandoned. User safety tools can be so much better than they are, and Meta’s users deserve a better, safer product than Meta is currently delivering to them. Yet rigorous testing of user safety tools can tell us not only what is broken, but also point the way to solutions. The same methods that reveal failures can also show us the way forward: toward safety tools that are default-on, resilient against evasion, and genuinely useful for teens and parents.

Going forward, we believe independent scenario testing should become a standard practice, carried out not just by researchers but also by regulators and civil society to answer questions about platform functionality. Treating safety tools with the same rigor that cybersecurity applies to other critical technologies is the only way to know whether platforms are keeping their promises — and to ensure that future tools are designed to deliver real protection, which is verified through independent testing, as are most safety features in society today.

A REPORT ABOUT BROKEN PROMISES AND DANGEROUS DESIGN, NOT CONTENT

This report aims to assess safety features relative to Meta's promises to parents and regulators. Our focus is on product design, not on content or how it is moderated. Even when we discuss content-related features, such as Sensitive Content Controls, our focus is on the effectiveness of the promised feature, rather than the content itself.

This distinction is critical because social media platforms and their defenders often conflate efforts to improve platform design with censorship. However, assessing safety tools, and calling out Meta when these tools do not work as promised, has nothing to do with free speech. Holding Meta accountable for deceiving young people and parents about how safe Instagram really is, is not a free speech issue.

Recommendation-based features like Home, Reels, Discover, and Search should be fundamentally safe and age-appropriate by design. When Meta recommends content to a young person on these product features, typically through its personalized recommender algorithms, the choices that inform these recommendations are a product design issue. Meta has promised to ensure teens are "seeing content that's appropriate for their age." Meta should keep that promise, and it's entirely possible for the company to do so without limiting the ability of adults to share sensitive content with other adults.

Our testing of Teen Accounts and Meta's safety tools found a combination of tools that were no longer functional, tools that were buggy, and tools that by their own design would not prevent the harm they claimed to address. In several cases, we found that Meta's own design circumvented its own safety tools. These are all product design issues.

The lack of effective Time Spent tools to deal with issues including problematic time spent on Instagram or usage late at night that may interfere with sleep is a product design issue.

The delivery of rabbit holes of self-harm, suicide-related accounts, and Meta's search features recommending these kinds of content and accounts even when they are not what the teen is searching for, is fundamentally a product design issue.

Meta measures everything it does. The company knows how many users it has, how much time they spend on its products, and how often they interact with every one of its product features.

In contrast, Meta measures its safety tools in terms of the sheer number of tools the company has rolled out. Meta should measure and share how effective the tools are, the extent to which teenagers are adequately protected when the tools are in force, and whether specific tools are particularly helpful to address the safety and well-being risks that children face when using Instagram.

Meta could, of course, easily measure and publicly report on the impact and efficacy of its Teen Accounts measures if it wanted to. Questions may legitimately be asked about why the company consistently chooses not to do so.

METHODOLOGY FOR TESTING USER-FACING SAFETY FEATURES ON INSTAGRAM

In March 2025 and again in June and July 2025, we assessed Instagram’s safety tools for teens using testing scenarios featuring test accounts.

Testing scenarios are an approach widely used by engineering and security professionals to understand and evaluate how a system behaves. This kind of testing is also called “red team” or “black-” or “gray-box” testing, depending on test conditions. Conceptually, it is similar to crash testing a car, where a tester sees how a car’s crash protections actually behave under different controlled conditions. This kind of scenario testing is a standard systems engineering security practice.

A secondary goal of this report is to demonstrate the utility of scenario testing for understanding the efficacy of user-facing safety systems and user experiences more generally. We encourage academic institutions, independent organizations, and regulators to develop their own avatar test scenarios of all social media products and their safety features, and we encourage independent security auditors to develop a series of test scenarios to evaluate the efficacy of safety tools. We believe that testing safety features is essential, as these are products used by hundreds of millions of teenagers across the world. As such, independent red team testing should be a core element of their development process.

STEP 1

FEATURE IDENTIFICATION

We began by systematically reviewing Meta’s public safety press releases to identify user-visible features implemented on Instagram. Each press release was examined for references to tools, interface elements, or settings that were claimed or implied to directly affect end-user safety. To ensure comprehensiveness, we included both new feature launches and updates to existing safety mechanisms. Features were included if they (a) were described as safety-related either explicitly or implicitly, (b) were accessible to end-users through the Instagram interface, and (c) had measurable or observable functionality that could be tested empirically.

STEP 2**TEST SCENARIO DEVELOPMENT**

For each identified feature, we developed a structured testing scenario designed to simulate realistic user behavior. Scenarios specified the conditions under which the feature should activate, the type of account used (e.g. teen vs. adult, follower vs. non-follower), and the expected safety intervention. The design of scenarios was guided by threat-modeling principles, with a focus on three perspectives: (1) usage, search, and commenting without seeking to intentionally circumvent protective measures, (2) self-directed circumvention attempts, and (3) external adversaries seeking to bypass protective measures. This step ensured that tests reflected plausible use cases rather than artificial or contrived interactions.

STEP 3**TEST ACCOUNT CONFIGURATION**

To accurately evaluate the behavior of safety features, we established a set of controlled test accounts or “avatars.” Accounts were configured to reflect the adversary models defined in our framework:

Teen user model: Accounts were created with an age designation under 18 and configured with exploratory but non-malicious use patterns to simulate a teen attempting to circumvent restrictions placed on their own account. The account creation process mirrored the process of a parent giving their teen a new phone: Accounts were created using all privacy and safety defaults. To ensure testing captured regular conditions, the accounts were tested right after creation, and then tested after two weeks.

Supervising user model: Accounts were created as a user with a parental, supervisory relationship to the teen user model.

Targeting user model: Adult and teen accounts were established to simulate malicious actors attempting to interact with or contact teen users, with follower/non-follower and public/private account variations included to capture different relationship dynamics.

These controlled accounts provided a consistent and repeatable basis for executing the testing scenarios. By aligning account characteristics directly with user models, we ensured that observed outcomes could be clearly interpreted within the threat-model framework.

STEP 4**FEATURE TESTING**

Initial testing was performed in March 2025, with a second round of follow-up testing in June and July 2025. Testing for all scenarios was done on iPhones installed with iOS with versions 16.6.1 (March) and 16.7.8 (June and July) and the most recent version of Instagram available at the time of testing. Each testing scenario was executed using the test accounts relevant to the test scenario. During testing, we carefully observed whether the safety feature functioned as described in Meta’s public materials. All findings were documented through contemporaneous screen recordings and screenshots, which provide verifiable evidence of the product’s behavior. Images and screen captures were not altered in any way. Where relevant, repeated trials were conducted to confirm consistency of outcomes.

STEP 5**EVALUATION**

During testing, each feature or tool was evaluated to determine if it was currently functioning as described in Meta’s public materials and if it was resistant to circumvention by accidental or trivial efforts. Additionally, each tool or feature was classified along five dimensions: the user target, the harm approach, the safety scope, the risk category, and the implementation style. Definitions and rubrics for each of these dimensions are in Appendix 3.

After testing, each tool or feature was graded using a three-tier rubric — red, yellow, and green — to classify the overall effectiveness and usability of safety features visible to users on Instagram. A red rating was given when a safety feature was found to be no longer available or, in a realistic testing scenario, was trivially easy to circumvent or evade with less than three minutes of effort. A yellow rating was made when a safety feature was functional and offered some level of protection but came with one or more serious limitations along a classified dimension. For example, if a tool was functional, but only reduced instead of prevented harm (see Harm Approach in Appendix 3), it would receive a yellow rating. A green rating was given when a safety tool worked effectively and as described. The full rubric used in the scoring process is described in Appendix 2.

LIMITATIONS

Please note this report makes no measurements of the frequency of harmful experiences or content being shown through algorithmic feeds. For example, we make no claims about the frequency of harmful content being algorithmically targeted to teens through Reels or Discover, or how often teens message with adults they would not know if not for Instagram’s recommendations of whom to follow.

The focus of this report is to better understand the effectiveness of the safeguards that Meta claims to have put in place, rather than to measure the broader prevalence of harm on its platforms. Our goal was to better understand the effectiveness of the safeguards that Meta claims to have put in place relative to the kinds of harms that young people and parents are concerned about, and to test whether the Teen Account safeguards adequately prevent exposure to them.

Scenario testing is a well-established methodology for understanding foreseeable risks and to assess the efficacy of user-facing systems and tools. However, it cannot tell us about how frequently risks are exploited in practice. The frequency with which teens experience different kinds of harm can be determined by large-scale surveys of users, such as Meta’s own Bad Experiences and Encounters Framework (BEEF) survey. Independent academic efforts like the USC Neely Social Media Index can measure this as well. We encourage Meta to undertake a comprehensive analysis of the frequency of exploitation of the risks we identify and circumvention of user safety tools with critical vulnerabilities, and to release the questions, methodology, anonymized data, and results publicly so that parents, regulators, and the general public can decide for themselves how safe Instagram is for children and teens.

HOW TO BUILD EFFECTIVE SAFETY AND USER REPORTING FEATURES FOR CHILDREN

Before detailing our findings of Meta’s existing safety features, it is important to describe how social media platforms can achieve truly impactful safety-by-design by building safety measures and reporting mechanisms that are thoughtfully designed, built in an age-appropriate fashion, and driven by an overarching emphasis on achieving harm reduction.

SAFETY TOOLS

Truly effective safety tools should have four primary attributes: prevention, protection, resiliency, and ease of use.

- 1. Prevention:** Safety tools must strive to effectively prevent teens from being exposed to harm in the first place.
- 2. Protection:** If and when harm does take place, an effective safety tool should immediately provide help and support — for example, by allowing a teen to easily indicate when they have experienced unwanted sexual advances. The tool should automatically block users to prevent a further recurrence of harm, and should proactively record information that will help find criminals and other bad actors. Capturing this information also supports the development of stronger protections for other teens.
- 3. Resiliency:** Safety tools must be resilient to active manipulation. If there is an easy workaround that a teen can figure out, the feature is essentially a safety tool in name only.
- 4. Ease of use:** Safety tools should either be switched on by default or be used with a single click. Meta knows that default settings and ease of use directly determine the likelihood that a user will go on to use a feature. That is precisely why features that actively increase engagement are usually turned on by default, or users are proactively incentivized to turn them on. Safety tools should be designed in exactly the same way.

A good way to think about Safety Tools is to think of them like safety features in a car. It doesn’t matter if a car has 50 airbags if they don’t effectively protect the people inside when an accident happens.

Under robust regulatory oversight, safety features built into a car are independently tested to make sure the safety mechanisms work as intended. Likewise, Meta’s safety features need to be resilient under duress, and the efficacy of every measure should be robustly and independently evaluated to ensure they offer the highest possible standards of protection to children.

EFFECTIVE REPORTING

It's easy to tell when a social media platform wants you to use one of its features. A platform will typically turn the feature on by default or proactively encourage you to turn it on, for example, through in-app prompts. In contrast, platforms typically seek to frustrate users from turning on features and settings that may not be in their commercial interests.

In such cases, platforms may deliberately choose to make certain settings and features hard to set up, confusing, or difficult to find. Over recent years, extensive research has catalogued the way Meta and other companies use these techniques, relying on so-called “dark patterns” and “friction” in the user experience to make it harder, and therefore less likely, for users to adopt certain features.

Meta's reporting tools for Instagram are an excellent example of intentional friction-by-design. Many of Meta's safety features, including some of the features analyzed in this report, typically require many steps to open and lodge a report. Users may be asked to go through multiple fields, or even to leave the app they are using to make their complaint.

For products used by teens, it is critical to have effective reporting. There are a number of criteria that reporting tools must meet in order to be helpful for teens.

REPORTING TOOLS SHOULD

- Be easy and rewarding to use: The user should feel that the tool helped them with the issue that they were experiencing.
- Use language that teens relate to the harm they are experiencing.
- Capture what happened (harm), where it happened (context), and how bad it was (i.e., intensity and severity). These steps should not be required, but they should be available and rewarding to use.
- Provide immediate support and protection to the user, independent of any content moderation considerations.

Providing immediate relief and support at the time a teen asks for help is critical to reducing harm in cases of harassment, bullying, grooming, self-harm, and other areas. In these cases, the messages sent or comments made are likely not going to be found to violate rules about content. In reviewing comments and content reported for bullying, more than 90% did not violate any policies, and in 50% of the most severe cases of bullying, the content looked benign or positive to the reviewer, who did not have the context.

Meta also continues to use language that is age-inappropriate and that the company understands may be actively likely to deter young people from making reports. Meta understood as early as 2012 that labeling tools as “report” had a significant negative impact on young users’ confidence and willingness to share bad experiences, often because they worry that they, or the other person, may get in trouble. At the time, Meta also found the importance of using language that matches the teen’s experience. Without the correct language, the majority of teens would not submit reports, even though they were having harmful experiences.

Meta continues to design its Instagram reporting features in ways that will not promote real world adoption. As a result, it was estimated by Meta that less than 1% of users report harmful experiences, and only 2% of those who submit reports get help. In other words, only two out of 10,000 people who have a harmful experience on Instagram actually get help from the platform.

We call on Meta to provide much needed transparency about the rate at which teens use the reporting tools relative to the harms they experience, the action rates (i.e. if a teen submits a report, what is the likelihood that it will be acted on), and whether the tool helped the teen with the issue they were experiencing.

0.02%

**OF PEOPLE WHO HAVE HARMFUL
EXPERIENCES ON INSTAGRAM GET
HELP FROM THE PLATFORM**

OUR FINDINGS

30 OF THE 47

**SAFETY FEATURES WERE EITHER
NO LONGER AVAILABLE OR WERE
SUBSTANTIALLY INEFFECTIVE**

Our analysis of 47 safety tools for teens found that the overwhelming majority were woefully ineffective, with over 60% receiving our worst red rating.

30 of the 47 safety features were either no longer available or were substantially ineffective. As a result, these safety features received a red rating. Nine of these safety features could not be triggered during our research and appear to have been discontinued. We also found that a further 20 safety measures could either be trivially circumvented or evaded, whether accidentally or with less than three minutes of effort.

9 of the 47 safety features offered some level of functionality, but came with notable limitations or flaws. As a result, these safety features received a yellow rating. Safety features were classified as yellow if they were not enabled by default and required the user to take steps to proactively find, activate, use, or configure them; or if they reduced harm rather than effectively preventing it.

8 of the 47 safety features analyzed were found to be fully functional and offered proactively or as a default. These measures received a green rating. The green rating was given to safety features that were wholly and demonstrably functional; offered proactively so that users didn't have to locate and set them up; and were found to be capable of improving user safety at both the individual and community levels.

Meta's promises around safety features and Teen Accounts are clustered around four main areas: Inappropriate Contact and Conduct, Sensitive Content, Time Spent and Compulsive Use, and Age Verification.

In the following sections, we explore and test Meta's safety features for each of these categories. In our analysis we:

- Detail the promises Meta has made to parents and regulators.
- Provide an overview of the findings from our testing.
- Outline a series of questions that regulators with discovery powers could pose to Meta about its safety tools and their efficacy.
- Provide recommendations for how each of these areas could be addressed by Meta and similar companies.

Our recommendations come from an understanding of the company's capabilities and the specific safety measures that would be straightforward to implement. All of the issues found in this report can be addressed by Meta — it has the technology and people to develop features that would effectively reduce the harms experienced by young people on its platforms.

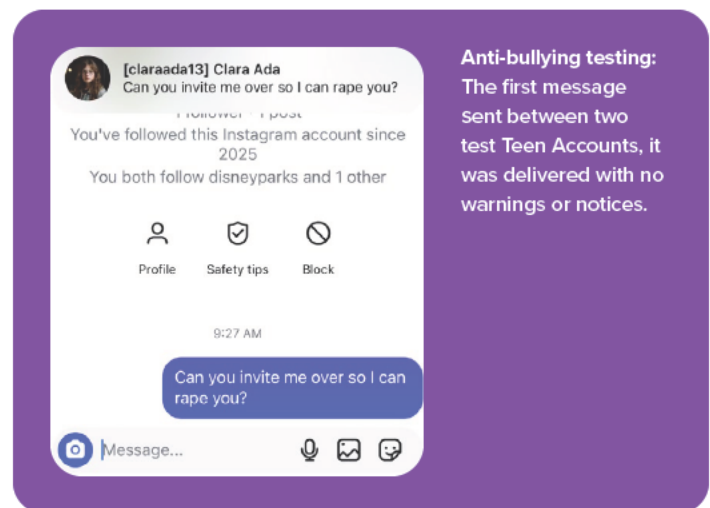
INAPPROPRIATE CONTACT AND CONDUCT

Inappropriate Contact and Conduct includes unwanted sexual advances, bullying and harassment, contact with strangers, etc.

Adults can communicate with minors through many features that are inherent in Instagram's design. In many of these cases, the adult strangers were recommended to the minor by Instagram's features: Reels, People to Follow, etc.

Most significantly when a minor experiences unwanted sexual advances or inappropriate contact, Meta's own product design inexplicably does not include any effective way for the teen to let the company know of the unwanted advance. The conscious absence of a tool that captures this information creates a state of "willful blindness" for Meta and means it is effectively impossible to manage or reduce this harm.

In another troubling design choice, Meta has implemented an animated reward or incentive for underage users to activate Disappearing Messages, and rewards their use with an animation. Disappearing Messages can be used for grooming, drug sales, etc., and leave the minor account with no recourse.



Anti-bullying testing:
The first message sent between two test Teen Accounts, it was delivered with no warnings or notices.

SUMMARY — IMPROPER CONTACT AND CONDUCT

META’S BROKEN PROMISES

Meta implies that its safety tools and Teen Accounts make messaging between adult strangers and minors impossible and greatly reduces the likelihood of children being exposed to bullying and inappropriate comments. However, our results found that:

While Meta explicitly claimed that adults could not message users with Teen Accounts that did not follow them, it was in fact possible for an adult to message a teen who did not follow them when we first tested in March 2025.

The Hidden Words feature — which is supposed to hide or filter out common offensive words and phrases in order to prevent harassment — is largely ineffective, as are all similar features.

Multi-block, a tool to preemptively block new accounts that someone may create and a tool to prevent harassment, was not working when tested.

To this day, teens are actively encouraged by Instagram to follow adults they do not know. Once they do, those adults can message them.

Teens can message adults who do not follow them, and we did not encounter the promised safety notices encouraging teens to be cautious.

Teens are rewarded for selecting Disappearing Messages, making them vulnerable to predation and to accounts involved in illicit activities.

Teens remain unable to quickly or effectively report inappropriate or sexualized messages or comments they have received, including from adults.

Of the 24 safety announcements relating to Inappropriate Contact and Conduct, our testing found that 13 were either no longer available and/or contained significant flaws. These received a red rating.

A further six announcements received a yellow rating, while five announcements were rated green.



WHAT META PROMISED

In its current policy on Child Sexual Exploitation, Abuse, and Nudity, Meta states that it does “not allow content or activity that sexually exploits or endangers children.” In October 2024, the company announced that it was launching a new campaign to “help teens spot sextortion scams and help parents support their teens in avoiding these scams.”

For teens, the campaign — which Meta said it worked on with the National Center for Missing and Exploited Children (NCMEC) and Thorn — includes an educational video to help them recognize if someone may be a sextortion scammer. Meta also said it was working with parent creators to inform parents on “what steps to take if their teen becomes a victim of” sextortion.

According to Meta, Instagram Teen Accounts allow only people the teens already follow or are connected with to message them, tag them, or mention them. In addition, the accounts feature the “most restrictive version” of Meta’s anti-bullying feature Hidden Words “so that offensive words and phrases will be filtered out of teens’ comments and DM requests.”

Meta says it recognizes that bullying and harassment can have a greater emotional impact on minors, “which is why our policies provide heightened protection for anyone under the age 18, regardless of user status.” On Instagram, Adam Mosseri, the head of the platform, said in 2019, “We are committed to leading the industry in the fight against online bullying, and we are rethinking the whole experience of Instagram to meet that commitment.”

In March of this year, Meta launched the Instagram School Partnership Program to “help address ongoing concerns about online bullying in schools by giving teachers, educators and administrators an easier way to report instances of teen safety issues directly to Meta.”



KEY FINDINGS

Of the 53 press releases issued by Meta relating to youth safety, more than half of these relate to Inappropriate Contact and Conduct on its platforms. We tested 24 purported safety features described in these announcements. Thirteen of the features (54%) were either no longer available and/or featured significant flaws, and therefore received a red rating. Six features (25%) offered some protection but had some notable limitations and were rated yellow. Only five safety features (21%) worked as advertised and were rated green.

In our analysis, we found significant issues with many of the claims made by Meta, with substantial concerns about the efficacy of its messaging restrictions, account privacy, and anti-bullying tools. Taken together, these issues and shortcomings may actively exacerbate the risks faced by children and young people when using the company's products, as described below.

You are a whore. Kill yourself now.

Reply Message Hide

Testing anti-bullying features such as Hidden Words. The comment did not receive any warnings and was not hidden.

Messaging Restrictions

Messaging restrictions are important means through which platforms can protect children and young people from Inappropriate Contact and Conduct, including unwanted contact from unknown adults.

Meta claims that it has actively introduced a number of important measures that prevent adults from contacting children and that provide additional friction in the user experience. However, our analysis suggests that the impact of these measures is at best deeply uneven, and at worst may be actively ineffective, with substantial risks associated with Meta's product changes not doing what the company claims.

Perhaps most troublingly, at the time of our testing earlier this year, we found that it was actively possible for adults to initiate conversations with minors who did not follow them. While it appears that Meta subsequently fixed this issue, this was a major lapse in Meta's messaging restrictions.

We found no evidence that Meta took steps to address the potential harm that may have occurred as a result of its messaging restrictions not working as described. During our analysis, we were readily able to send direct messages from an adult avatar account to our child avatar accounts, and no observable action has been taken to either block these contacts or delete conversations that should not have been able to take place.

Inappropriate Contact and Conduct

Sensitive Content

Time Spent and Compulsive Use

Age Verification, Minors and Sexualized Content

Given the number of threat actors who will seek to exploit Meta's services, as well as the scale of the service, it is therefore entirely possible that tens of thousands, if not hundreds of thousands, of inappropriate, high-risk interactions may have taken place while this issue went unresolved.

During our analysis, we identified a number of other ways in which inappropriate contact could be initiated or the overall impact of teen safety features could be undermined.

For example, despite restrictions on adults being able to proactively contact children under age 16 who do not follow them, Meta's algorithms continually recommended adult accounts as suggested follows to young people with Teen Accounts. This included adults whom the child did not know and who were located in other countries.

It also remains actively possible for a minor to initiate messaging conversations with adults who do not follow them on Reels, now one of the most used parts of the Instagram product.

It is also troubling that Instagram's user experience on Teen Accounts appears to actively incentivize the adoption of higher-risk account settings. For example, when the test Teen Account first opened direct messages, we received on-screen prompts that actively encouraged us to turn on Disappearing Messages, a high-risk option that has been widely observed to increase the risk profile for teens and that can be readily exploited by threat actors, including child sexual abusers. In addition, once messages disappear, it is no longer possible to report them.

A rain of emojis rewards a teen for selecting Vanish Mode, which was recommended on the first use of messages by our test Teen Accounts.



When we accepted the prompt to turn on Disappearing Messages, this generated an on-screen rain of emojis, a gamified response that had the effect of celebrating the teen activating the Disappearing Messages function. One could reasonably foresee this implying to the user that they had made the correct choice, with Disappearing Messages likely to be understood as a feature that would elevate or improve their overall user experience.

It is also likely that this reward-based approach may encourage the user to accept other prompts of a similar design or nature in the future, a type of persuasive design practice that — similar to dark patterns — may result in teenage users being encouraged to accept product outcomes that may be commercially advantageous to the platforms, even if they are contrary to the best interests of the child.

Private Accounts

Meta has actively promoted Teen Accounts as offering a more protective, privacy-focused experience. According to Meta, both new and existing accounts for children under 16 are defaulted to private, as are new accounts for 16- and 17-year-olds. Children under 16 need their parents' permission to make their accounts public, while older teens can make the change themselves.

Public accounts are considerably more likely to receive unwanted sexual advances and may experience more intense forms of bullying and harassment. Yet children may understandably want to make their accounts public so they can gain more followers and have their content seen by more people.

We found that neither children or parents were provided any guidance to encourage them to keep their accounts private. For example, Meta does not highlight the safety and well-being benefits of private accounts, nor does it offer any kind of nudge when users go to change this setting (e.g., "Warning: Private accounts protect young people from unwanted and potentially abusive contacts from strangers. Are you sure you want to make your account public?").

Bullying, Inappropriate Comments and Sexualized Contacts

Instagram claims to have made a number of product changes that reduce the risk of teenagers being exposed to bullying and inappropriate comments from other users, and that provide teenagers with greater agency and control over the messages they receive.

Our analysis suggests that the impact of these measures is somewhat limited, if not wholly ineffective. For example, in 2021, Instagram announced the rollout of its Hidden Words function, a tool that is turned on by default and that claims to automatically hide or filter out comments with common offensive words, phrases, or emojis.

However, we found the Hidden Words function to be substantially ineffective. Grossly offensive and misogynistic phrases were among the terms that we were freely able to send from one Teen Account to another. For example, "you are a whore and you should kill yourself" was sent and received without any prompts to reconsider, or filtering or warnings being provided to the recipient.

We also found that Multi-block, a feature announced in 2021 to preemptively block new accounts created by someone you've blocked, was not functioning correctly, as linked accounts in a multi-blocked device were not blocked. This feature is important because it prevents harassment and stalking by people who create new accounts on their device to get around being blocked.

Teen Accounts still seem poorly positioned to deal with the risks associated with unwanted sexual encounters and inappropriate sexual contact in comments or messages, including from adults and other teens.

During our testing in March 2025, adult accounts were able to initiate messages with minors who didn't follow them back. This was four years after Meta announced that adults would no longer be able to send messages to under 18s who didn't already follow them. During our second round of testing in June and July, this issue had been fixed, and we found that adults were unable to message minors who do not follow them.

In the same announcement, Instagram announced it had started using safety prompts to encourage teens to be cautious in conversations with adults with whom they are already connected. While this type of safety-by-design measure is excellent in principle, in most circumstances, we were unable to trigger prompts or warnings during our safety testing. We also found that some follow requests sent directly from adult strangers triggered a warning, yet no warnings were shown when Instagram algorithmically recommended adult strangers for a teen to follow.

Teenagers remain unable to quickly or effectively report inappropriate or sexualized comments or messages they have received, including from adults.



RECOMMENDATIONS FOR META

- Perform a regular methodical and thorough red-team testing of messaging controls and limitations across all product features.
- Perform a regular, methodical, and thorough red-team testing of block, restrict, and Multi-block across all product surfaces.
- Investigate and give appropriate notice for any contact of accounts that should have been blocked by Multi-block.
- Provide an easy, effective, and rewarding way for teens to report inappropriate contact or conduct in direct messaging. It should be very easy for a teen to indicate when they received unwanted sexual advances or intimate images, or if they believe the account contacting them is fake.
- When a teen deletes a comment, or blocks or restricts an account, give them an easy option (one or two steps) to indicate the reason they blocked the account. The reporting function in WhatsApp, or for junk in iMessage, are examples of a one-step block and report flow.
- Establish proportionate response measures based on frequency for individuals who initiate inappropriate contact or conduct.
- Investigate and give appropriate safety notice during conversations between an adult and a teen who does not follow the adult, and give appropriate tools to the teen.
- Make it clear in the Teen Account product, supervision tools, and communications that Meta recommends adult strangers for teens to follow (which enables direct messaging), and that a teen can initiate a conversation with adults who do not follow them back.
- Publish the rates and reasons for which teens report inappropriate contact or conduct, or the rates and reasons provided for using block, restrict, or other similar mechanisms teens use to deal with harmful conduct. This will allow parents and regulators to assess safety and progress.



QUESTIONS FOR REGULATORY INQUIRY

Regulators should ask Meta (and other social media companies):

What percentage of teens who indicate on surveys that they had a harmful experience (e.g. unwanted sexual advances) end up successfully submitting a report? (completion rate)

What percentage of submitted reports result in an action? (action rate)

What percentage of teens were recommended unwanted sexual content in the last seven days?

- With what frequency?
- How intense/bad was it?
- What did the teen do? Did they block or report or scroll away?

What percentage of teens were recommended self-harm content in the last seven days?

- With what frequency?
- How intense/bad was it?
- How did they resolve it?

Of the teens who experience harmful content:

- What percentage open the reporting tool?
- What is their completion rate?
- Of the teens who submit a report, what is the action rate?

How many conversations are there between teens and adults who were not followed by the teen?

- What steps are you taking to address this issue?

SENSITIVE CONTENT

Sensitive Content is about ensuring that the account gets recommended age-appropriate content, and that there are effective measures around search and discovery of certain classes of content.



SUMMARY — SENSITIVE CONTENT

META’S BROKEN PROMISES

Meta claims it makes sure teens are seeing content that’s appropriate for their age. However, our test Teen Accounts were still recommended:

Sexual content, including graphic sexual descriptions, the use of cartoons to describe demeaning sexual acts, and brief displays of nudity.

Violent content, including Reels, of people getting hit by cars, falling to their deaths, and graphically breaking bones.

Content that promotes self-harm and self-injury.

Body image content that would likely have a negative impact on teens.

In addition, using the “not interested” feature did not significantly alter the type of content recommended by Instagram.

Of the eight announced safety features we tested related to sensitive content, all eight were found to contain significant flaws or to have been discontinued. Consequently, every measure received a red rating.



WHAT META PROMISED

Meta first announced Sensitive Content Control in July 2021, and said it would default teens into the most protective setting. According to the company, Sensitive Content Control allows users to decide how much sensitive content shows up in Explore. Meta says it began defaulting all users under age 16 into the “Less” setting in Sensitive Content Control on Instagram “to make it more difficult for them to come across potentially sensitive content in Search, Explore, and Hashtag Pages, Reels, Feed Recommendations and Suggested Accounts.”

In a policy document that was last updated on June 11, 2025, Meta says it wants teens to have “safe, positive experiences” on its platforms, which includes “making sure they’re seeing content that’s appropriate for their age.” The company claims it prevents teens from seeing sensitive or mature content in three ways: 1) removing content that violates Meta’s rules; 2) hiding sensitive or mature content from teens 3) and avoiding recommending “an even broader set of content.”

One of Meta’s promises for Teen Accounts is to “address parents’ biggest concerns,” including what content their teenagers see. According to Meta’s announcement about the launch of Teen Accounts, Teen Account users are automatically placed in the most restrictive setting of the company’s Sensitive Content Control, which limits the sensitive content (including content that shows fighting or promotes cosmetic surgery) that teens see in Instagram features like Explore and Reels.

In addition, with Teen Accounts, Meta claims that parents can “view the age-appropriate topics their teen has chosen to see content from.”

“We recognize parents are concerned that their teens might see mature or inappropriate content online,” the company says, “which is why we have stricter rules around the kinds of content teens see on our apps.”

Yet despite Meta’s repeated insistence that the company is responsive to concerns about the content it recommends to minors, researchers have consistently demonstrated that Instagram pushes sexualized content to minors.

In June 2024, The Wall Street Journal described how, according to tests run by the newspaper and an academic researcher, “Instagram regularly recommends sexual videos to accounts for teenagers that appear interested in racy content, and does so within minutes of when they first log in.”

In response to those findings, a Meta spokesperson dismissed the findings as “an artificial experiment that doesn’t match the reality of how teens use Instagram.” The spokesperson told the Journal: “As part of our long-running work on youth issues, we established an effort to further reduce the volume of sensitive content teens might see on Instagram, and have meaningfully reduced these numbers in the past few months.” Meta provided no evidence to support these claims.

In May 2025, Accountable Tech and Design It For Us tested Teen Accounts and found that 100% of their test accounts were recommended sexual content, violating Meta’s own prohibitions around sensitive content for teen account holders.

In September 2022, a coroner found that harmful content on Instagram (and other platforms) played a “not insignificant contributory role” in the death of 14-year-old Molly Russell, the first time that social media was directly found to be partially responsible for the death of a child.

Following media coverage of Molly’s death, the Head of Instagram Adam Mosseri pledged that Instagram would address the safety risks that contributed to her death. “We are committed to publicly sharing what we learn. We deeply want to get this right and we will do everything we can to make it happen,” he told UK media.

However, research undertaken by Molly Rose Foundation earlier this year found that harmful suicide, self-harm and depression content continued to be recommended to teens on Instagram at an “industrial scale”, despite the introduction of Teen Accounts. On an account opened in the guise of a 15-year-old girl, 97% of Reels recommended to it contained content that was likely to be harmful, particularly when viewed cumulatively or in large amounts.

Meta did not go on to publish any of the findings that it promised. In response to Molly Rose Foundation’s analysis, Meta claimed that the company “disagrees with the assertions of this report and the limited methodology behind it.” However it provided no rationale or data to set out its position or to explain how Teen Accounts allowed large volumes of harmful suicide and self-harm content to be algorithmically recommended.

Despite these consistent findings, Meta’s promises around sensitive content persist. In its policy on “Helping Teens See Age-Appropriate Content” (last updated July 11, 2025), Meta says that for teens, it not only removes content from its platforms that contains nudity or explicit sexual activity, but it hides “images and videos that don’t contain explicit nudity or sexual activity but could be considered sexually suggestive because of a pose suggesting sexual activity or if people are near-nude. Teens can’t see this content even when posted by someone they know.”



KEY FINDINGS

Meta has issued eight separate press releases announcing the introduction or enhancement of product features designed to prevent exposure to sensitive content on Instagram, and the company has given considerable emphasis to Sensitive Content Controls built into its Teen Accounts. All eight features were found to contain significant flaws or to have been discontinued. Consequently, every measure related to sensitive content received a red rating.

Product changes announced include:

Sensitive Content Controls: a range of tools intended to limit inappropriate content recommended in feed and search surfaces.

Feed or recommendation surface feedback controls: measures designed to give teens the ability to indicate that content is “not interesting” to them or to reset the algorithm.

Search protections: tools that limit access to content when searching for certain topics, and where appropriate provide links to third-party help and resources.

Overall, we found that Teen Accounts were still algorithmically recommended a broad range of harmful content, even when the strictest Sensitive Content Controls were in place.



Instagram issued a press release touting that it had blocked the hashtag #edrecovery as part of its safety efforts. But when the hashtag was partially typed as “#edrecov,” Instagram recommended alternatives that led to similar eating disorder content. This issue was first publicly identified by a [BBC investigation in 2018](#).

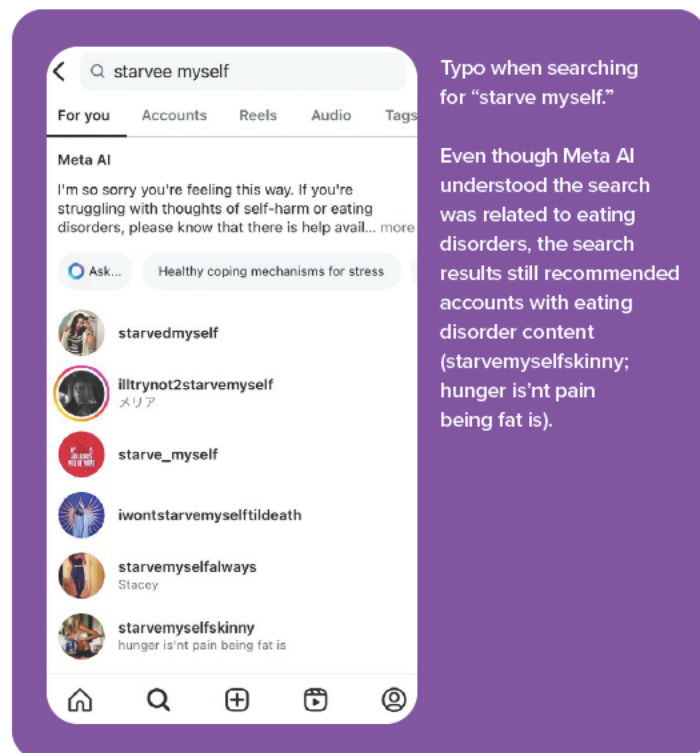
During safety testing, our avatar accounts were recommended age-inappropriate sexual content, including graphic sexual descriptions, the use of cartoons to describe demeaning sexual acts, and brief displays of nudity. We were also algorithmically recommended a range of violent and disturbing content, including Reels of people getting struck by road traffic, falling from heights to their death (with the last frame cut off so as not to see the impact), and people graphically breaking bones.

Instagram also recommended a range of self-harm, self-injury, and body image content on Teen Accounts that would be reasonably likely to result in adverse impacts for young people, including teenagers experiencing poor mental health, or self-harm and suicidal ideation and behaviors.

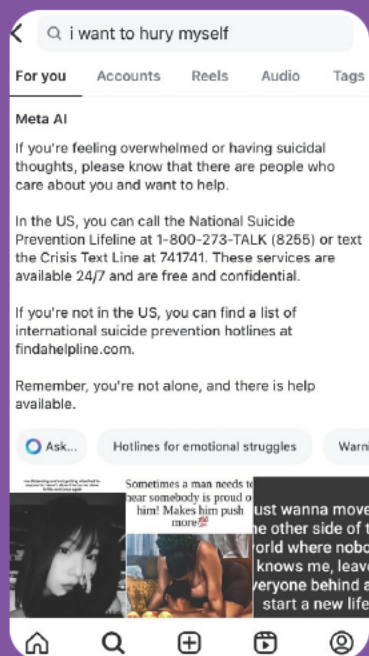
It appears that the Instagram algorithm was attempting to show us a broad range of potentially harmful category types, with the reasonable assumption that this was to gauge our interest in seeing further content if we engaged with it, whether out of curiosity, interest, or disgust.

Research shows a palpable risk of cumulative harm where children are algorithmically recommended harmful content in large volumes and/or quick succession. The death in 2017 of 14-year-old Molly Russell (whose inquest determined that exposure to harmful content on Instagram played a not insignificant contributory role in her death), and who engaged with over 2,000 harmful posts on Instagram in the six months before her death, exemplifies this risk.

Other measures designed to prevent children being able to access sensitive and age-inappropriate content also seemed to work inconsistently, if at all. Often, Meta's own auto-complete or recommendations circumvented the safety measure. Search protections for suicide and self-injury, eating disorder and body image content, often failed to prevent potentially harmful content from being recommended or discovered. Queries that were slightly misspelled were directed to harmful content (even while on the same screen, an AI response interpreted the query as related to self-harm).



Typo when searching “I want to hurt myself.” Even though Meta AI understood the search was related to self harm, the search results still recommended accounts with self-harm content. Meta first promised to address this issue in 2019.



Auto-complete actively recommended search terms and accounts related to suicide and self-injury, eating disorders, and illegal substances, even though these content categories are self-evidently potentially harmful. To make matters even more concerning, once the harmful content was viewed, other parts of Instagram like Reels, Home, etc., started recommending similar harmful content.

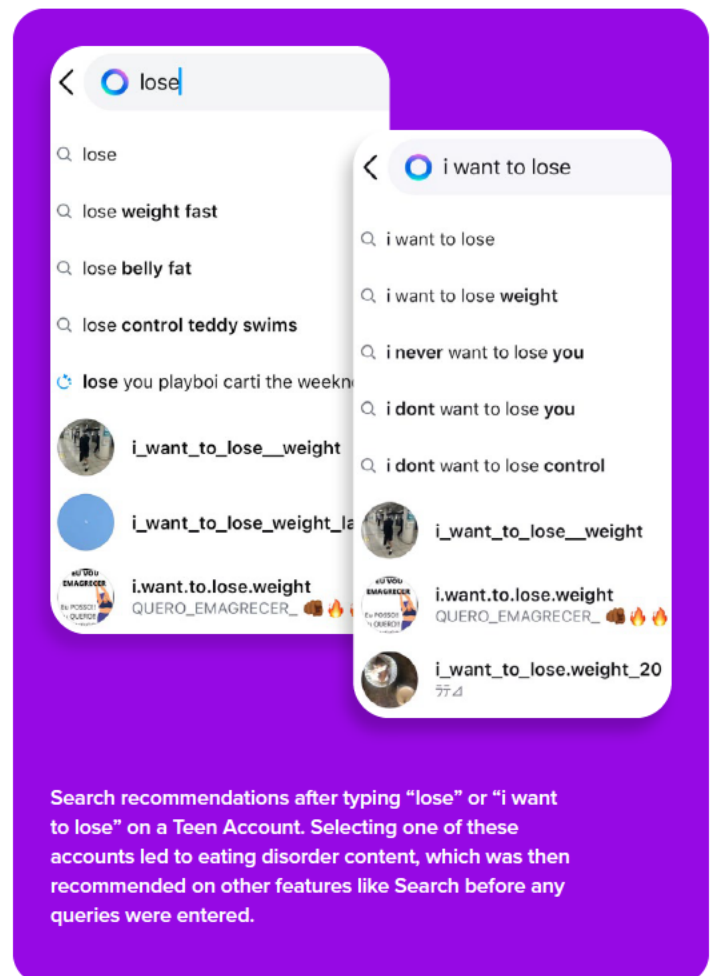
Instagram’s introduction of a Not Interested feature is potentially an important step forward that could give young people greater agency and autonomy over their feeds, if it worked as advertised.

However, our safety testing found that the introduction of the Not Interested option did not seem to have any meaningful effect on the type of content we were subsequently served. For example, in one of the avatar tests, we indicated we were not interested in a series of Reels showing graphic injury, but we were subsequently shown further videos of a similar nature, including content of people sustaining broken bones.

In effect, the limited impact of the rollout of Not Interested means that the only option available to a teen who wishes to be shown less harmful content may be to reset their entire algorithm. For entirely understandable reasons, many teens may be reluctant to do this. In any event, there is an increased cognitive load associated with this option, and it can be a complex and challenging option to undertake. It also seems highly likely that a reset will essentially prove to be a temporary measure at best, and that similar harmful content will soon be recommended to a teen again.

Concerningly, we found a clear disconnect between the content being algorithmically recommended on Teen Accounts and the overview being provided to parents (where the Teen Account was paired with a supervisory parental account). Specifically, parental accounts were not provided with any indication that potentially harmful and age-inappropriate categories of material had been recommended to the Teen Account, including the violent, graphic, and suicide and self-injury material outlined above. This worrying disconnect raises a palpable risk that parents may experience a false sense of security as a result of the way in which the Teen Accounts supervisory function is being operated.

Regulators and lawmakers may wish to closely examine the reasons for this discrepancy, including whether this suggests Meta has chosen not to track certain categories of content being algorithmically recommended to teens or has instead chosen not to disclose these category types to parents using the supervisory function.





RECOMMENDATIONS FOR META

The recommendations made to a 13-year-old Teen Account should be reasonably PG rated. They should not include: unwanted sexual content, graphically violent content, content that causes body image issues or eating disorders, or self-harm content.

The effectiveness of Sensitive Content Controls should be measured by asking teens about their experience of sensitive content they have been recommended, including frequency, intensity, and severity.

There should be an easy and effective way for a teen to request that certain kinds of content not be recommended to them. The Not Interested feature should be as easy to use as liking or swiping and measured by whether the user finds it to be effective.

It appears that the search safety tools are implemented as a narrow blacklist of search terms. This approach has many known issues and is fundamentally ineffective. A blacklist results in harmful content getting accidentally recommended to minors, and is easy to circumvent. Instead, Meta should follow the search safety approach of many search engines, where a wide variety of self-harm queries, misspelled or otherwise, across different languages, deliver help and resources.

Every one of these features should be tested for effectiveness and resilience by independent auditors, and external entities.



QUESTIONS FOR REGULATORY INQUIRY

Regulators should ask Meta (and other social media companies):

How do you know when a teen experiences unwanted sexual, violent, eating disorder, or self-harm content on your different product surfaces?

What percentage of teens report experiencing unwanted sexual, violent, eating disorder, or self-harm content in the last quarter?

When a teen experiences any of the sensitive content categories:

- What actions can they take?
- What actions do they take?

What percentage of teens who experience any of the sensitive content categories submit a report?

- What reporting options do they select?
- What percentage of the reports are acted on?
- How many views does violative content have prior to being removed?
- What is your analysis of reported content that is not removed?

How regularly do you perform red-team testing of your search safety features?

- Is the testing done by independent third parties?
- Are the results of independent search testing published?

TIME SPENT AND COMPULSIVE USE

Time Spent and Compulsive Use is about providing effective tools to help teens manage the amount of time and the quality of the time they spend on the platform. This includes areas like limiting how much time per day they spend in the app, avoiding downward spirals or rabbit holes of content, the amount of notifications teens receive, or the number of times a kid opens the app in a given day. Time Spent and Compulsive Use also helps parents ensure their teen is not succumbing to addiction to the platform.

SUMMARY — TIME SPENT & COMPULSIVE USE

META'S BROKEN PROMISES

Meta claims it has implemented a number of features to help parents limit the amount of time their children spend on Instagram, as well as features that encourage teens to take breaks. However:

Teens cannot set time limits to restrict how much time they spend on Instagram. There is only a time limit reminder that can be snoozed for the day.

A feature that was heavily promoted to hide Like and View counts was changed by Meta so that it's no longer possible to hide View counts.

Our test accounts did not receive Meta's promised Nighttime Nudges when we used Instagram for more than 10 minutes late at night.

Our test accounts did not receive any topic or surface nudges after spending between 45 minutes to an hour on a topic or surface.

Our test accounts did not receive any reminders to turn on the Take a Break feature, despite Meta's claims that teens would be regularly prompted to do so.

Reducing notifications was incredibly burdensome, requiring a review of 50 toggles across 10 screens.

As part of the research, we tested seven of Meta's announcements relating to the time that young people spend on its platforms. We determined that five of these safety features had either been discontinued or contained significant flaws, meaning they were given a red rating.

Two safety features worked well and were accordingly rated green.



WHAT META PROMISED

When Meta launched Instagram Teen Accounts in 2024, it said it wanted to address parents' top concerns, including "whether their [teens'] time is being well spent." Accordingly, Teen Accounts give parents tools to restrict their teens' time on the app. One of these tools allows parents to set a daily limit for how much time their child can spend on Instagram each day. Another tool lets parents block their teens from using Instagram during a particular time, such as at night or during a set time period. Parents can also "set up days and times when your teen's account will be in sleep mode." This mode mutes notifications and sends autoreplies to direct messages.

Teen Accounts also limit teens' time on Instagram even without parental action. The accounts automatically go into sleep mode from 10 am to 7 pm. In addition, after 60 minutes on Instagram, teens get a notification telling them to leave the app. In order to change either of these settings, teens under 16 need their parents' approval.





KEY FINDINGS

Seven of Meta's press releases relate to Time Spent measures, features that are promoted as a set of tools and prompts that can address excessive time spent on Instagram and support young people to use the platform in a more balanced way. Five of these safety features had either been discontinued or contained significant flaws and were given a red rating. Two safety features worked well and were accordingly rated green.

The announcements cover a wide range of safety-by-design features, including:

Time spent reminders: reminders that let a child know when they've spent a fixed period on the platform, typically one hour.

Time limits: a parental control that allows the parent or guardian to limit the amount of time their child spends on the app.

Topic or surface nudges: tools that nudge the Teen Account user away from content once a certain amount of time has passed.

Quiet Mode: a tool that limits notifications a teenager is sent overnight.

Take a Break: prompts that encourage the user to take a break when they've used the product for an extended period.

While many of these features appear outwardly positive and respond to the increasing concern expressed by parents about the time children are spending on Instagram, we found that many of these features offered only limited effectiveness at best.

Troublingly, Instagram's Take a Break feature, which was heavily promoted at the time it was first announced, appears to have been discontinued. Despite Instagram's claims that teens would be actively shown notifications suggesting they turn these reminders on, we did not receive a single notification prompt in the testing done in March, June, or July, and there is no option to enable Take a Break in settings.

In May 2021, Instagram announced a setting to hide Like and View counts, a project known as "Daisy." Adam Mosseri said that its purpose was to create "a less pressurized environment where people feel comfortable expressing themselves." Meta made no announcement when it took away the ability to hide View counts and replaced it with the ability to hide Shares. View counts can create pressure on a teenager to create exploitative content, so this change was significant.

In addition, there is considerable friction that makes it less likely a teen will actually hide Likes or Shares. In order for a teen to hide their Like or Share count, they have to post first, then go to the settings of that post and select to hide one or the other. They are unable to hide Like and Share counts at the same time, and there is no way for a teen to make hiding counts the default option across all their posts.

We were also unable to find any evidence that Instagram's Nighttime Nudges feature was either in place or effective. In January 2024, [Meta](#) announced that teens would receive a notification when they had spent more than 10 minutes on a particular Instagram feature late at night. The prompts would remind teens that it's late and encourage them to close the app.

However, during our safety testing, we were unable to trigger any of these prompts across multiple product surfaces that we tested during nighttime hours.

We also found that it was difficult for teens to exercise agency if their desire was to reduce interactions, notifications, or time spent on the platform. For example, teenagers themselves cannot place a limit on how much time they spend in the app — a time limit can only be set by adding a parent or guardian that supervises their Teen Account.

It is also exceptionally hard for a teenager to limit the amount of notifications or prompts they may receive. For example, if a teen wishes to only receive notifications when they're messaged by a friend, the teen is expected to navigate 50 toggles over 10 different screens — a highly complex and unnecessarily burdensome user journey.

Instagram's Quiet Mode did generally appear to be effective.



RECOMMENDATIONS FOR META

New Teen Accounts should have a time limit default built in, and the parent or guardian account should be required to change it.

Features should be implemented that effectively nudge the teen away from downward spirals, rabbit holes, or overuse of the product. There should be independent audits, and transparency about how effective the nudges are.

Features should also be implemented that check on the well-being of teens — for example, a simple check-in on whether the amount of time is having a positive or a negative effect on the teen. Companies know how to design and implement this feature so that a teen would use it, and that they would get accurate data when product changes are having a negative effect on well-being.

View counts should be hidden by default for Teen Accounts. There should be a simple, single setting for teens to hide Likes, Views, and Shares. It should not be required for the teen to select this as an option for each post they make.

There should be a very quick and easy way — an option in notification delivery or a simple setting — for Teen Accounts to only get notified when a friend messages, or a similar high-priority notification setting.



QUESTIONS FOR REGULATORY INQUIRY

Regulators should ask Meta (and other social media companies):

Provide detailed statistics including distribution of:

- Time spent on Instagram by Teen Accounts by age.
- Number of daily notifications delivered to Teen Accounts by age.
- The amount of times Instagram is opened in a given day for Teen Accounts by age.

How effective are reminders of time limits?

- For Teen Accounts that get shown reminders of time spent, how many close the application?
For how long?
- What percentage of reminders are snoozed by the user?
- What percentage of teens snooze the reminders for the day?

What percentage of Teen Accounts have added a parent or guardian?

- What percentage of those have set a time limit?

What percentage of Teen Accounts have hidden Like and Share counts?

Minors and Sexualized Content is about accounts whose content is videos of children who appear to be under 13, who sometimes post about their age, and about the inappropriate amplification of videos where the minors are incentivized to post sexualized or other forms of detrimental content by the platform.



SUMMARY — AGE VERIFICATION, MINORS, AND SEXUALIZED CONTENT

META'S BROKEN PROMISES

Meta claims it is using artificial intelligence to assess users' ages and to take appropriate action if that assessed age is different than the age the user entered at signup. However:

Instagram is rife with users who appear to be, and often affirmatively state, that they are under 13.

Our test accounts were repeatedly recommended Reels that featured children claiming to be as young as 6.

Instagram's recommendation-based algorithm actively incentivized children under 13 to perform risky sexualized behaviors. When young girls whose posts typically got hundreds of views posted videos of them lifting up their shirts to show their bellies, or similar behaviors, these posts often garnered tens of thousands to hundreds of thousands of views.

Of the eight product features relating to age assurance or Teen Accounts, four of the features had significant flaws. These were rated red. Three announcements were rated yellow, while one feature worked as described and was rated green.



WHAT META PROMISED

Testifying before the US Senate in 2021, Instagram Head Adam Mosseri said, “If a child is under the age of 13, they are not permitted on Instagram.” Three years later, when Meta launched Instagram Teen Accounts, the company claimed that it would automatically place teens in these more restrictive accounts to shield them from dangerous content and unwanted contacts. Nevertheless, in April 2025, the company seemed to acknowledge that not all teens on the platform are actually in Teen Accounts, saying “we want to make sure as many teens as possible are enrolled.”

To that end, Meta said it was notifying parents on Instagram about the importance of teens using their correct ages online. In addition, the company said it was sending parents tips to check and verify their teens’ ages on Meta apps. These tips were informed by guidance from experts like pediatric psychologist Ann-Louise Lockhart.

While the tips put the responsibility on parents to make sure their children are using their correct ages on Meta apps, the company assured parents that they “don’t have to go it alone.” Meta said it was beginning to use artificial intelligence in the US to “proactively find accounts we suspect belong to teens, even if the account lists an adult birthday, and place them in Teen Account settings.”



KEY FINDINGS

Meta has issued eight press releases relating to Age Verification, and the launch of its Teen Accounts on Instagram, Facebook, and Messenger. Four of the features had significant flaws and were rated red; three offered some protections but had significant limitations and were rated yellow. One feature worked as described and was rated green.

Extensive evidence has shown that millions of children under age 13 use Instagram in the US and UK, with limited evidence that the platform has attempted to enforce its rules against children that age using the platform consistently or at scale. Meta claimed in 2022 that it was already “investing heavily in research and technology to better understand people’s ages across our platforms,” but that its efforts would be significantly bolstered by a new AI model that could detect whether someone is a teen or an adult.

Our safety testing demonstrated not only that Instagram’s attempts at age assurance were evidently ineffective, but that the platform’s engagement-based design was actively identifying and promoting content from children who claimed to be under the minimum joining age.

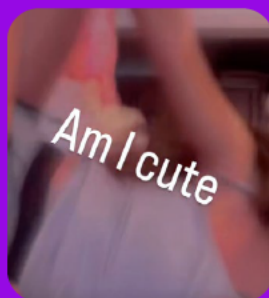
For example, we were repeatedly recommended meme-style Reels where children share their actual ages, with videos of children claiming to be only 6-, 7-, 8- or 9-years-old. Further investigation revealed that tens of thousands of children had posted similar videos.

In June 2023, the Wall Street Journal reported that Instagram was connecting a vast network of pedophiles.

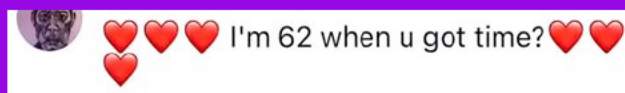
In the article, the search term “Gymnastics” led to accounts of young children and a network of predators and predatory comments. In June 2025, Meta announced that it removed hundreds of thousands of accounts related to predatory behavior. In July, our testing found that while “Gymnastics” no longer led to finding accounts of young children, Instagram’s search autocomplete recommended searching for “Gymnastics girls young,” which led to accounts of young girls similar to the ones reported in 2023. These girls’ posts were met with predatory comments, such as, “The younger the soul the tighter the hole.”

We also found evidence that suggested Instagram’s recommendation-based algorithm actively incentivized children under 13 to perform risky sexualized behaviors.

Videos where girls of this age group raised their shirts to show their bellies attracted tens of thousands to over a hundred thousand Views, far in excess of the usual Views generated by their posts (with Views typically in the hundreds). Other posts included young girls singing sexually suggestive song lyrics, many of which had attracted hundreds of thousands of Views and Likes. In turn, some of these posts attracted deeply distressing and suspicious comments from adult users, including sexually suggestive messages and references to and images of condoms.



Very young girl in a tank top reel with 35.2k views, 10 times her other videos. An example of inappropriate content incentivized by Instagram through inappropriate amplification. Public reel counts can teach other children to copy the behavior for views. (Public content, cropped to protect the minor's privacy.)



One of the top comments left on the account of what appears to be an 11 year old girl, who is asking to be rated. That video had over a million views, and over fifty thousand comments, most of them calling her ugly.

Instagram's algorithms effectively reward minors who expose themselves, and predators who may be actively looking for minor sexualized content and/or children to target for the purposes of child sexual abuse.

In other cases, Instagram's recommendation algorithms were promoting Reels in ways that were likely to be substantially detrimental to the mental health and well-being of underage and younger users. For example, we identified videos posted by young children that asked other users to rate them, specifically whether they were "fine, cute or ugly." One video of a young girl, whom we estimate to be only 9- or 10-years-old, had received over 1 million Views, with over 50,000 comments, most of which rated her as "ugly."

These are all examples of the circulation risk, which is the inappropriate amplification of content outside of its intended context (see Appendix 3). It is Instagram's inappropriate amplification that incentivizes, endangers, and ultimately teaches young children to create content that is exploitative and demeaning and exposes them to harassment.

While Meta's own attempts at proactive enforcement have clearly been wholly ineffective, it is equally difficult for users to report accounts that they believe breach the platform's minimum age policies. Users wishing to report an underage account cannot do so on the Instagram app, but must instead click through seven separate steps, get redirected to a separate webpage, and then fill out a detailed form where the details of the underage account must be re-entered.

Given Meta's extensive history of deploying dark patterns across its' platforms architecture, some may suspect that Meta has been actively seeking to embed as much friction into the reporting flow for under-13 accounts as possible, with the explicit intention of frustrating the discovery of underage accounts in ways that might subsequently be publicly reported, for example through regulatory transparency or legal disclosure.

Whatever the reason, as it stands, it is virtually impossible to report the account of a young person under age 13, while Instagram's engagement-based algorithms and other high-risk design features simultaneously exacerbate the risk that those children will be exposed to otherwise preventable content- and contact-based harm.

In its policy on Child Sexual Exploitation, Abuse, and Nudity, Meta states that it does "not allow content or activity that sexually exploits or endangers children." The unequivocal and absolutist nature of this assurance would lead a reasonable parent to infer that the Instagram app had been designed to prevent and eliminate such harms from the platform. But our testing revealed that there are no effective controls for these harms, and Meta's own internal research has revealed that underage users are constantly exposed to sexual exploitation and related harms.



RECOMMENDATIONS FOR META

Social media companies have created a confusing narrative around Age Verification technologies by invoking false extremes. Claims that it is necessary for everyone to provide a government ID in order to verify age simply aren't true.

While Age Verification technology is important, it is just one element of an effective age assurance program. Other elements include detecting accounts that appear to be lying about their age and implementing product interventions when an account is under suspicion.

Detection should be a combination of effective reporting tools and automated detection. For example, today, if you find an audio trend used by 10,000 accounts that are talking about being 6- to 12-years-old, there is no way to submit a report that the trend is primarily used by kids under 13, which could be invaluable in detecting those kinds of accounts.

The tools that most social media companies have are able to detect, with enough precision, when an account is run by someone who could be under 13.

The key here is a principle: when in doubt, verify. When you have reason to believe an account is under 13, you can ask them to get their parent or guardian to verify their age. If the parent, with the appropriate warnings, notes the account is under 13, you delete the account, or you let the parent enter the accurate age. When you have reason to believe an adult is pretending to be a teen, you can ask them to age verify through a similar process.

For accounts of minors that are parent-run, provide a clear feature indicating that it is a parent-run account, and that the parent has been verified.

Work with an independent third party to perform and then publish a review of the distribution of content that features minors. In particular, evaluate when a minor's content gets tens or hundreds of thousands of views, and evaluate that for inappropriate amplification.

These processes should be put through independent testing and auditing. There should be an independent audit of the detection methods and processes of the company. And there should be independent testing of reporting, or detection of accounts.



QUESTIONS FOR REGULATORY INQUIRY

Regulators should ask Meta (and other social media companies):

What is the completion rate and action rate for reporting an under-13 account?

.....

Why is it not possible to report them in one click?

.....

Given some of the accounts provided, can you provide an explanation for each of them of why your automated systems did not detect them in the first place?

.....

Describe your process for assessing age based on a user's posts and activities that might indicate that a user is likely a different age than what they listed at signup.

.....

Does Meta assign an age or age-range based on a user's activity for the purposes of targeting content or advertising? If so, is this same data used to remove accounts that appear to be under 13 and to offer additional protections to teens?

.....

Can you provide a study of Reel views of accounts where the content seems to primarily feature kids who appear to be under 13?

CONCLUSIONS

Over the past year, Meta has actively sought to capitalize on the launch of Teen Accounts, and it routinely points to its 50+ safety tools when seeking to underscore its commitment to child safety on Instagram.

Our comprehensive review of Meta's Teen Accounts finds that there is a substantial gap between the protections promised in the company's public relations efforts and the actual protections afforded to teens. Our analysis suggests that a majority of Meta's safety features do not work as intended. Our research demonstrates that teens using Teen Accounts are still the recipients of inappropriate contact and conduct; are encouraged to connect with strangers; and lack tools to effectively manage how they spend their time or to curb compulsive use. In addition, we found that young children who shouldn't be allowed on the platform are encouraged to post content that others view as sexualized.

Meta's claims to both parents and lawmakers are directly contradicted by this independent, systematic testing. With only 1 in 5 of its safety tools working effectively and as described, many may conclude that its rollout of Teen Accounts has been driven more by performative PR than by a focused and determined effort to make Instagram safe for teens.

Our research demonstrates the palpable failure of self-regulation: With large-scale advertising campaigns in Washington, DC, London and other major markets, Meta has invested heavily in the reputational and brand benefits of Teen Accounts, but has failed to design, build, and test safety features that actually improve the experience of teens or better protect them from preventable harm.

In the US, regulation cannot come soon enough. This analysis not only substantially undermines Meta's claims to be proactively and comprehensively developing children's safety-by-design, it palpably demonstrates that under its current leadership, the company appears to be fundamentally unwilling to tackle the child safety risks that blight its products.

Congress should pass the wildly popular and bipartisan Kids Online Safety Act, which would hold Meta accountable for design-caused harms and force the company to engage in real mitigation efforts.

In addition, the Federal Trade Commission should hold Meta accountable for both the prevalence of accounts of children under 13 — a violation of the Children’s Online Privacy Protection Act — and for deceiving parents about the efficacy of its safety tools, a violation of Section V of the FTC Act.

In the UK and EU, regulators must actively investigate and interrogate each and every safety claim that the company now makes. It cannot be enough for Meta to claim that child safety measures are being rolled out. The impact and efficacy of any safety tools must be independently tested and verified.

Meta can, of course, choose to react to the findings in this report positively and constructively. Every recommendation in this report is proportional and reasonable. If Meta’s senior leadership wants to address the shortcomings highlighted by this research, we have made a series of proportionate recommendations that could enable its safety features to work effectively, and Teen Accounts to live up to the promise of Meta’s PR claims.

Meta could also commit to publicly reporting on the efficacy and impact of its safety tools, rather than simply measuring its approach on the number of tools it rolls out. Meta also could support independent testing and auditing of its safety features. This would require a shift toward meaningful transparency and oversight, with a willingness to test the extent to which safety measures work accompanied by a commitment at the highest levels of the company to take meaningful action to make Teen Accounts deliver as promised.

Meta talks the talk, but its rhetoric and the reality are very different things.







Until we see meaningful action, Teen Accounts will remain yet another missed opportunity to protect children from harm, and Instagram will continue to be an unsafe experience for far too many of our teens.

Note: Cybersecurity for Democracy did not participate in writing this section and by policy does not endorse any legislation.









APPENDIX

SUMMARY OF DETAILED FINDINGS








Inappropriate Contact and Conduct

SAFETY MEASURE	TESTING SCENARIO	RESULTS	IMPLEMENTATION STYLE	STATUS
<u>Block feature</u> October 2010 (tool t01)	Does the feature work as described?	While the block feature works, users cannot provide reasons why they wish to block e.g. because of inappropriate sexual behavior. The option for users to provide a reason when blocking would be an invaluable signal to detect malicious accounts.	User activated	
<u>Swipe to delete inappropriate comments</u> September 2016 (t02)	What happens when you delete a comment?	In cases of bullying and harassment, this feature offers limited benefits i.e. the account can simply comment again. Users cannot provide reason for deletion.	User activated	
<u>Comment keyword filters that allow filtering out of offensive or inappropriate comments</u> September 2016 (t03)	What happens when you make different kinds of aggressive comments between avatar accounts?	Uses a blacklist not whitelist approach, which requires a user being harassed to enter the slurs they're concerned about. The feature can be easily circumvented by mis-spelling. User has to configure by entering different slurs and their spellings. Where offensive terms are sent, there were no notices or repercussions i.e. when sending messages including 'you're not pretty', 'you look ugly and dumb'.	Needs configuration	
<u>Ability to turn off comments</u> December 2016 (t04)	Does the feature work as described?	Works as described, although teens might not want to turn off comments because they want more interaction on their posts	User activated	
<u>Offensive content filter controls, allowing users to automatically hide certain offensive comments</u> June 2017 (was later expanded to include terms related to bullying and harassment) (t07)	What happens when you make different kinds of aggressive comments between avatar accounts?	We were unable to find offensive comments that were automatically filtered, when testing between two teen accounts.	Needs configuration	
<u>Users able to choose who can comment on their posts</u> September 2017 (t08)	Does the feature work as described?	Works as described.	User activated	




Inappropriate Contact and Conduct

SAFETY MEASURE	TESTING SCENARIO	RESULTS	IMPLEMENTATION STYLE	STATUS
<u>Comment warnings prompting people to reconsider comments that may be hurtful.</u> July 2019. This feature was later expanded to include an additional stricter warning to discourage posts from being sent (t11)	What happens when you make different kinds of aggressive comments between avatar accounts?	Feature could not be triggered. Comments including 'You are a whore. Kill yourself now' and 'you are so ugly and stupid' (which was example provided by Meta in the announcement article) that did not result in any prompts or warnings.	User activated	
<u>Restrict, a feature that allows people to control their Instagram experience without notifying people who may be attempting to target them</u> October 2019 (t12)	Does the feature work as described?	Feature works as described, it is a good safety feature. Users are not able to provide the reason for restricting someone, which would be valuable to identify someone who is being restricted by multiple users.	User activated	
<u>Caption warnings, prompting people to reconsider posting images and captions that may be offensive or hurtful</u> December 2019 (t13)	What happens when you make different kinds of aggressive comments between avatar accounts?	Couldn't be triggered in March, was triggered in July. When working, this feature can be easily circumvented e.g. 'I hate dumb whores' triggered a prompt, but 'I h8 dumb putas' did not. Which is a fundamental issue with blacklist based tools.	Default on	
<u>Ability to delete multiple comments at once</u> May 2020 (t14)	Does the feature work as described?	Works as described.	User activated	
<u>Ability to block or restrict multiple accounts at once.</u> May 2020. Later improvements included 'multi-block', an option for people to both block specific accounts and pre-emptively block new ones (t15)	Does the feature work as described?	Using a Teen Account, this feature failed to block another account in a 'multi-blocked' user's device.	User activated	
<u>The option to pin comments, giving people an easy way to amplify and encourage positive interactions</u> May 2020 (t16)	Does the feature work as described?	Works as described. Positive feature that helps to set norms and encourages a positive environment.	User activated	
<u>Users can optionally manage the tags and mentions them, to help protect from targeted bullying</u> May 2020 (t17)	Does the feature work as described?	People you know can bully you through tagging. The only other option would be to completely turn tagging off or block the person who is bullying you but then the damage is already done.	User activated	
<u>Adults over 18 are prevented from starting private chats with teenagers they are not connected with</u> March 2021 (t20)	Can an adult initiate a private conversation with a teen account that does not follow them? Can a minor initiate a conversation with an adult that they are not connected to?	In March, if an adult followed a teen, who did not follow them back, they could comment on their Instagram Story, which started a private chat. This issue was fixed by April, conversations that were initiated through this issue were not deleted or given any safety notice. We found that teens can initiate private chats with over 18 accounts that are verified or monetized, and can send message requests to adults they do not follow.	Default on	


Inappropriate Contact and Conduct

SAFETY MEASURE	TESTING SCENARIO	RESULTS	IMPLEMENTATION STYLE	STATUS
<u>Prompts and/or safety notices used to encourage teens to be cautious in conversations with adults they are already connected to</u> March 2021 (t21)	In which conversations to the safety notices show up?	Could not trigger this feature in testing.	Default on	
<u>Hidden Words tool gives people the option to filter DM requests containing certain offensive words, phrases and emojis (t22)</u> April 2021 (t22)	What happens when you make different kinds of aggressive comments between avatar accounts?	Could not trigger this feature in testing.	Needs configuration	
<u>Potentially suspicious accounts prevented from finding and following teens in places like Reels, Explore or Suggested for You (t24)</u> July 2021 (t24)	Can an adult find and follow teen accounts?	We did not find any evidence of this in testing. An adult account can easily find and follow teens. Instagram will even suggest teen accounts to follow suspicious accounts. We were recommended accounts that promote self-harm and just suspicious accounts overall.	Default on	
<u>'Limits' tool enables accounts to automatically hide comments and DM requests from people that don't follow them or that only recently started following them</u> August 2021 (t24)	Does the feature work as described?	This feature was not designed for teenagers, but for content creators who experienced more extreme surges of abuse	User activated	
<u>Users cannot tag or mention teens that don't follow them, and can't include their content in Reels Remixes or Guides, when first joining Instagram</u> December 2021 (t29)	Does the feature work as described?	Works as described	Default on	
<u>User nudges to promote kindness in DM requests and discourage offensive or inappropriate DMs (t41)</u> October 2022 (t41)	When does the nudge appear?	Nudges could not be activated, even when using phrases including: 'you're ugly and stupid', 'you are a horrible person', 'I hate you', 'you are a whore' and 'you are a b*tch.'	User activated	
<u>Prompting teens to report accounts after they block someone</u> November 2022 (t42)	Does the feature work as described? Is the reporting tool designed such that a teen would use it?	Found that block and report interface is not available in Profiles and in different Messages. The safety banner with the report and block function was only present in some messaging chats. Reporting options in messages and profiles do not include 'Unwanted Contact' category which is present in posts and is important in those contexts. The reporting flow is not designed for use by a teenager, and is likely to result in very low usage and report submission. The language used for categories is written for adults and the reporting tool makes it onerous to submit a report.	User activated	





Inappropriate Contact and Conduct

SAFETY MEASURE	TESTING SCENARIO	RESULTS	IMPLEMENTATION STYLE	STATUS
<p>A requirement to send an invite seeking permission to connect in DM's. Message request invite is text only, so people can send photos, videos voice messages until a request is accepted</p> <p>June 2023 (t52)</p>	<p>Does the feature work as described?</p>	<p>In some instances we were able to send images, videos and voice notes between two teen accounts that did not follow each other. In other cases, message invites could be sent but were not always received.</p>	<p>Default on</p>	
<p>Gave people the option to manually hide comments, to give them greater control over comments that they may find upsetting and unwelcome. This is in addition to the Hidden Words tool.</p> <p>October 2023 (t54)</p>	<p>Does the feature work as described?</p>	<p>The feature worked as described, however this places a clear onus on the recipient to hide comments, and does not allow the user to state a reason. In cases of sustained bullying and harassment, the damage is already done.</p>	<p>User activated</p>	
<p>Stricter default message settings for teens under 16 (under 18 in certain countries), meaning that only people they follow or are connected to can message them or add them to group chats</p> <p>January 2024 (t61)</p>	<p>Can an adult initiate a private conversation with a teen account that does not follow them?</p> <p>Can a minor initiate a conversation with adults that they are not connected to?</p>	<p>In March, adults were able to direct message a teen by responding to their Instagram Story (see earlier comment.)</p>	<p>Default on</p>	








Sensitive Content

SAFETY MEASURE	TESTING SCENARIO	RESULTS	IMPLEMENTATION STYLE	STATUS
<p><u>Anonymous reporting of accounts that may be struggling with their mental health, directing these accounts to resources on Instagram</u></p> <p>December 2016 (t05)</p>	Does the feature work as described?	Removed and no longer working	User activated	
<p><u>Ability to file an anonymous report potential self-injury in Live, with resources provided to those affected</u></p> <p>September 2017 (t09)</p>	Does the feature work as described?	Feature removed.	User activated	
<p><u>Links to trusted resources added at the top of search results for terms related to suicide or self-injury. Search results not displayed</u></p> <p>November 2020 (t19)</p>	How does the product behave when you try to search sensitive content?	<p>While this works for specific queries, when fully typed and then submitted. The way search is designed means this feature was accidentally or easily circumvented. For example partially typed queries would recommend accounts with sensitive content. For example, starting to type 'I want to hurt' would recommend accounts with self-harm content. Or misspelling words or search terms, like typing 'I want to hurry myself' would result in the AI recommendation understanding the query was about self-harm. Results included suggestions for accounts that promote suicide and self-injury content.</p> <p>We found similar behavior for eating disorder content.</p> <p>The way this is implemented we believe it is likely that Teen Accounts will be recommended self-harm, eating disorder, and other kinds of sensitive content even if that is not what they are searching for.</p> <p>Search terms that were blocked in English did not get blocked in Spanish, an issue that likely affects other languages.</p>	Default on	
<p><u>Expert backed resources when someone searches for eating disorders or body image related content.</u></p> <p>February 2021. Subsequently, a dedicated reporting option for eating disorder content was launched (t19)</p>	<p>How does the product behave when you try to search for sensitive content?</p> <p>Is the reporting flow designed to be used by a teen?</p>	<p>Only very specific searches are completely blocked, and it is easy to access design content through misspellings, phasing in a different way, or through using other languages. For example, we were able to search the content through search terms including 'I don't want to eat', 'stravee myself'.</p> <p>The reporting flow for eating disorder content is poorly designed and not age-appropriate because of the language it uses. The flow gave access to trusted help sources</p>	Default on	


Sensitive Content

SAFETY MEASURE	TESTING SCENARIO	RESULTS	IMPLEMENTATION STYLE	STATUS
<p><u>Sensitive Content Control</u>, with under 16's defaulted to the highest sensitivity settings</p> <p>July 2021 (t26)</p>	<p>What are examples of sensitive content they get recommended when Sensitive Content Controls are on the most conservative setting?</p>	<p>In March, test accounts were recommended violent, sexual content, and content made by children under 13 with sexually exploitative comments.</p> <p>In June and July, with a different set of newly created test accounts, we were initially recommended sensitive content on the home feed and after doing the searches (that the search safety feature is intended to prevent), recommendations included suicide, self-harm and body image material.</p> <p>After two weeks the test accounts were then recommended harmful content across multiple product surfaces, including: home feed, searches (prior to searching), explore page and Reels.</p>	Default on	
<p><u>Teens given the option to choose to hide multiple pieces of content in Explore, the option to add keywords or search terms they wish to avoid, and to report they are 'not interested' on posts seen in Explore (this will then prevent similar content recommendations on other surfaces,)</u></p> <p>January 2023 (t47)</p>	<p>If the teen account is getting recommended sensitive content, what impact does 'not interested' have all the recommendations?</p>	<p>Pop-ups were sometimes observed where we were asked whether or not we were interested in certain content types.</p> <p>In cases where we specified 'not interested', there was no discernible effect and we continue to be recommended similar content.</p>	User activated	
<p><u>Additional types of age-inappropriate content being hidden</u></p> <p>January 2024 (t57)</p>	<p>What are examples of sensitive content they get recommended when Sensitive Content Controls is on its most conservative setting?</p>	<p>During testing, we observed content that promoted self-harm and eating disorders.</p> <p>We encountered several posts that appeared to be created by under 13's, including accounts that showed minors performing age inappropriate dances, seeking likes and followers, and sometimes explicitly lying about their age to gain more attention. Adults were visibly interacting with the children in the comments, with predatory comments including 'you're so fine' and 'you're so sexy.' Others openly insulted or mocked them.</p> <p>Instead of blocking or limiting access to such accounts, the algorithm often amplified this type of content once it had been engaged with, making it even easier for harmful interactions to occur and harmful content to be recommended.</p>	Default on	
<p><u>More results hidden in Instagram Search relating to suicide, self-harm and eating disorders, with links to expert resources</u></p> <p>January 2024 (t58)</p>	<p>How does the product behave when you try to search for sensitive content?</p>	<p>Only very specific searches are blocked. It is easy to circumvent this through misspellings or using different word choices. Auto complete search results will yield hashtags of accounts with sensitive content.</p>	Default on	






Time Spent and Compulsive Use

SAFETY MEASURE	TESTING SCENARIO	RESULTS	IMPLEMENTATION STYLE	STATUS
Activity dashboard that includes a daily reminder and a new way to limit notifications August 2018 (t10)	Does the activity dashboard work as described?	Works as described (Teen Accounts).	User activated	
Users can hide public like counts, to give them more control over their experience May 2021 (t23)	How easy is it for a teen to hide like and a view counts?	Originally this was a setting to hide likes and views (Project Daisy). Without an announcement Meta changed it to hiding like and share count. It is no longer possible to hide view counts, which are prominent on reels, this design can encourage risky or exploitative behavior, the circulation risk, as seen in young children reels. We found intentional friction to deter teens from using this feature i.e. In order for a teen to hide their like or share count they have to first make a post then go on the post settings and select the option. You cannot hide like and share count at the same time. Intentional friction.	User activated	
'Take a Break' feature that enables teens to receive notifications when using the platform for a specified period of time. Teens will receive notifications to suggest they turn this feature on. December 2021 (t28)	Does spending time in different surfaces on the product and result in reminders? Are reminders designed to help a teenager to limit their usage?	Appears to be removed. We did not receive notifications encouraging us to turn this feature on. Despite looking at Reels for extended time periods (45 mins to 1 hr 15). We could not identify the feature in the account settings.	User activated	
Nudges that encourage teens to switch to a different topic if there were repeatedly looking at the same type of content on Explore June 2022 (t38)	After spending time on a topic or surface, is there a nudge as promised?	Feature could not be triggered during testing.	Default on	
Quiet Mode, which helps teens focus and encourages them to set boundaries with their friends and followers. Teens prompted to turn on Quiet Mode when spending a specific amount of time on Instagram late at night January 2023 (t45)	Does feature work as described? How easy is it for a teen to manage the kinds of notifications they get?	Feature works as described. However, there is significant friction when trying to customize the feature e.g. it required 50 toggles over 10 different screens to only get notifications of messages from people we were connected to.		
Night-Time nudges that show up when teens have spent more than 10 minutes on a particular Instagram surface e.g. Reels January 2024 (t60)	Does spending time in different product surfaces result in reminders?	The feature could not be triggered during testing.	Default on	
Testing of a new feature that allows people, including teens, to reset their content recommendations in Explore, Reels and Feed. This builds on content creation techniques, including 'interested' and 'not interested' feedback options. November 2024 (t68)	Does selecting 'not interested' result in changes to content recommendations?	Using the 'not interested' had either no or a temporary effect, with the same content showing up again in a few minutes. We did not test the recommendation reset.	User activated	



Age Verification

SAFETY MEASURE	TESTING SCENARIO	RESULTS	IMPLEMENTATION STYLE	STATUS
<p><u>New ways to verify people's age on Instagram</u>, including privacy preserving selfie videos</p> <p>June 2022 (t39)</p>	<p>How easy is it to report an account that is under 13?</p> <p>Under which scenarios does age verification technology engage?</p>	<p>Age assurance kicks in if you try to amend the age on a Teen Account.</p> <p>It extremely difficult to report someone who you suspect to be aged under 13, with a complicated and extended reporting flow, friction by design.</p>	Default on	

Teen Accounts and parental controls

SAFETY MEASURE	TESTING SCENARIO	RESULTS	IMPLEMENTATION STYLE	STATUS
<p><u>Default private account settings for under 16s and notifications encouraging existing under 16s to switch to a private account</u></p> <p>July 2021 (t25)</p>	<p>What kind of disclosure does the product give when changing between public and private accounts?</p> <p>Does Instagram adequately warn teens of the risk of going public?</p>	<p>Prior to Teen Accounts this was a toggle that a teen could change with no disclosure about the risks involved.</p>	Default on	
<p><u>Family Center and Parental Supervision Tools on Instagram</u></p> <p>March 2022 (t32)</p>	<p>Are parental controls, as currently designed, helpful for parents and teens to manage the different risks and issues around being online?</p> <p>Do parental controls present an accurate picture of the teen's experience?</p> <p>Do parental controls address known risks such as finstas?</p>	<p>As a user activated setting, this was unlikely to be adopted by a substantial percentage of parents.</p> <p>Parental controls do not present accurately what a teen is experiencing.</p> <p>Parents are not notified by default if their child reports either a post or account.</p> <p>Children could easily open a finsta (a secondary account on their device), and the parent would not receive any indication in the parental supervision tools.</p>	User activated	
<p><u>Parental Supervision Tools were given additional options, including the option to set specific times when parents can limit their child's use and to receive additional info about when their child makes a report</u></p> <p>June 2022 (t37)</p>	<p>Are parental controls, as currently designed, helpful for parents and teens to manage the different risks and issues around being online?</p> <p>Do parental controls present an accurate picture of the teen's experience?</p> <p>Do parental controls address known risks such as finstas?</p>	<p>As a user activated setting, this was unlikely to be adopted by a substantial percentage of parents.</p>	User activated	
<p><u>Started prompting teens to update their privacy settings with one tap.</u></p> <p>January 2024 (t59)</p>	<p>Does the feature work as described?</p>	<p>Single tap safety or privacy settings do not currently exist.</p>	User activated	
<p><u>Parents using supervision tools will now be prompted to approve or deny changes to their child's default settings.</u></p> <p>January 2024 (t62)</p>	<p>Is the parental approval process triggered?</p> <p>Does this process appropriately disclose the potential risks to the parent?</p>	<p>Works as described, although the feature to change an account to public does not disclosed to parents or teens the increased risks that come with public accounts.</p>	User activated	

Teen Accounts and Parental Controls

SAFETY MEASURE	TESTING SCENARIO	RESULTS	IMPLEMENTATION STYLE	STATUS
<u>Teen Accounts launched</u> September 2024 (t67)	Do Teen Accounts deliver the set out in Meta's initial announcement?	<p>See notes on all safety features, in testing we found significant flaws with the implementation of almost every feature of Teen Accounts and Parental Controls including: sensitive content controls, messaging restrictions, and anti-bullying features. Each of these components was found to be flawed or ineffective during testing.</p> <p>Teen Accounts promises parents can see topics their teen is looking at, but that is misleading, parents only see if a teen selected a topic from a list, while the teen account got recommended sexual, violent, self-harm, and eating disorder content.</p> <p>Still no indication for parents of other accounts in the Teen's phones, 'finstas'.</p> <p>Positive: changing settings, including public to private did require approval.</p> <p>Negative: Still no appropriate disclosure of the risks of public accounts.</p>	Default on	
<u>Teen Accounts are being rolled out to new teens joining Instagram in the European Union</u> December 2024 (t69)	Are EU Teen Accounts different from the accounts elsewhere?	This announcement merely confirmed extended geographical scope of Teen Accounts, not new safety features	Default on	

Please note that 2 Meta announcements were not tested.

This was because testing would require uploading of harmful content.

4 measures were discounted from our analysis because they were primarily content curation and privacy features. In our assessment, these could not reasonably be considered safety features.

SCORING RUBRIC APPLIED DURING SAFETY TESTING

This rubric uses a simple three-tier system — red, yellow, and green — to classify the effectiveness and usability of safety features visible to users on Instagram

RED CATEGORY

Definition:

Features that are either no longer available or are ineffective.

CRITERIA TO CLASSIFY AS RED:

- The feature has been removed OR;
- In a realistic testing scenario, the feature is trivially easy to circumvent or evade in a way that can be done accidentally or with less than three minutes of effort.

YELLOW CATEGORY

Definition:

Features that are functional and offer some level of protection but come with important limitations.

CRITERIA TO CLASSIFY AS YELLOW:

- The feature is present and is effective as described BUT has one or more of the following limitations:
 - The feature reduces harm rather than preventing it
 - The feature does not enhance the broader community's safety.
 - The feature is not enabled by default and requires the user to take steps to proactively find, activate, use, or configure it.

GREEN CATEGORY

Definition:

Features that are effective, proactive, and contribute to both individual and community-level safety.

CRITERIA TO CLASSIFY AS GREEN:

- The feature is effective and has not been removed AND
- It actively prevents harm rather than just mitigating it AND
- It improves overall system safety and is beneficial at a community level AND
- It is enabled by default, so users do not have to seek it out.

DETAILED FINDINGS

We are providing a [link to a spreadsheet that contains the complete list of tools and the questions used for the test scenarios](#). We also analyzed the tools relative to the taxonomy below in order to help further independent study. For our research please visit <https://fairplayforkids.org/resources/> or <https://mollyrosefoundation.org/resources/online-safety/> or <https://cybersecurityfordemocracy.org/research>.

TAXONOMY OF USER-FACING SAFETY TOOLS ON SOCIAL MEDIA

This taxonomy provides a structured framework for categorizing safety tools that are visible and actionable in the user interface (UI) or user experience (UX) of social media platforms. We do not include broader network security or safety efforts that have no user-visible component.

DIMENSION 1: USER TARGET

This dimension describes the user model of the feature or tool.

CATEGORY	DESCRIPTION
Individual	Designed for the individual user’s self-management or protection.
Interpersonal	Manages interactions between users; often used to mitigate abuse or harm.
Supervisory	Enables oversight or controls by a third party (e.g. parents or guardians).

Examples:

- **Individual:** Screen time reminders, blocking undesired content, warnings about potentially violating actions
- **Interpersonal:** Blocking, muting, restricting contact
- **Supervisory:** Parental dashboards, approval workflows

DIMENSION 2: HARM APPROACH

This dimension describes the intended impact of the intervention.

CATEGORY	DESCRIPTION
Harm Prevention	Aims to stop harm before it occurs.
Harm Reduction	Focuses on reducing or mitigating harm after it has begun.

This category does not apply to tools with a ‘Supervisory’ user target, as these tools are not inherently harm-oriented.

Examples:

- **Harm Prevention:** Setting private profiles by default, nudges during risky actions
- **Harm Reduction:** In-app reporting, safety alerts after exposure to harmful content

DIMENSION 3: SAFETY SCOPE

This dimension describes the target of focus for the feature or tool.

CATEGORY	DESCRIPTION
Individual Safety	Primarily benefits the user enabling the tool.
Community Safety	Contributes to the overall safety of the platform and community.

This category does not apply to tools with a ‘Supervisory’ user target, as these tools are not inherently harm-oriented.

Examples:

- **Individual:** Blocking DMs, turning off comments
- **Community:** Reporting or flagging tools, feedback that reduces viral spread of harmful trends

DIMENSION 4: RISK CATEGORY (4 + 1 CS)

This dimension categorized the type of risk that the tool or feature aims to prevent or reduce. The 4 C's are a commonly used youth online risk framework developed by Livingstone et al.¹ A forthcoming work by Renkai Ma, Dominique Geissler, Stefan Feuerriegel, Tobias Lauinger, Damon McCoy, Pamela J. Wisniewski extends this framework to add Circulation risk, which we adopt as well. Finally, we also add Compulsivity risk, to describe tools intended to limit overall excessive or mis-timed usage.

RISK TYPE	DESCRIPTION
Content	Exposure to harmful content (e.g. graphic violence, misinformation)
Contact	Harmful interactions with other users (e.g. grooming, harassment)
Conduct	Risk from behavior (e.g. oversharing, bullying)
Contract	Commercial exploitation (e.g. manipulative ads, hidden purchases)
Compulsivity	Excessive or mis-timed use that is problematic or for which a user doesn't feel agency
Circulation	Inappropriate amplification of content outside of its user-intended context.

DIMENSION 5: IMPLEMENTATION STYLE

This dimension describes the default activity the tool is implemented with.

CATEGORY	DESCRIPTION
Default-On	Enabled automatically; requires no user action.
Prompted	Suggested or surfaced in context, but user must opt in.
User-Activated	Available for user to enable, but not suggested by default.
Needs Configuration	Available for user to enable, but requires non-trivial effort to configure, use, or maintain once activated.

Examples:

- **Default-On:** DM filters for unknown contacts.
- **Prompted:** In-app prompts to turn on a privacy setting.
- **User-Activated:** App usage dashboards in settings.
- **Needs Configuration:** Comment blocking based on user-configured block lists.

¹ Livingstone, S., & Stoilova, M. (2021). The 4Cs: Classifying Online Risk to Children. (CO:RE Short Report Series on Key Topics). Hamburg: Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI); CO:RE - Children Online: Research and Evidence. <https://doi.org/10.21241/ssoar.71817>

ABOUT THE AUTHORS

ARTURO BÉJAR

Arturo Béjar was the senior leader at Facebook responsible for engineering, product design, and research for security, safety, child safety, and customer care from 2009 to 2015. From 2019 to 2021, Arturo returned to Meta as a consultant to work on well-being issues at Instagram. During his second stint, Arturo led research, documented, and briefed the executive team on material harms experienced by teens on Instagram. It was the willful disregard of those harms that led Arturo to blow the whistle on Meta and advocate for the safety of young people online.

CYBERSECURITY FOR DEMOCRACY

Cybersecurity for Democracy is a research-based, nonpartisan, and independent effort to expose online threats to our safety, health, democracy and social fabric — and recommend how to counter those threats. We are a multi-university research project of the Center for Cybersecurity at the NYU Tandon School of Engineering and the Cybersecurity and Privacy Institute at the Northeastern University Khoury College of Computer Sciences. Learn more at cybersecurityfordemocracy.org.



Fairplay is the leading US nonprofit committed to helping children thrive in an increasingly commercialized, screen-obsessed culture. Since our founding 25 years ago, we have grown from a small group of concerned parents, health professionals, and educators into a powerful force for children and families. Fairplay is truly an independent voice — we do not accept donations from Big Tech or any corporation. Our unique approach helps put kids' well-being first at home, in communities, and in corporate boardrooms. Learn more at fairplayforkids.org.



Molly Rose Foundation exists to prevent suicide in the under-25s. Acting at the intersect of online safety, suicide prevention and mental health we hold tech companies, governments and regulators to account to make the online world safe for young people. We also offer education, help and support to give young people the tools and voice they need to live long and stay strong. Find out more at mollyrosefoundation.org.



Parents for Safe Online Spaces (ParentsSOS) is an educational initiative created by families who have lost children as a result of online harms. The initiative's goal is to raise awareness about the importance of the Kids Online Safety Act (KOSA), a piece of legislation addressing growing concern about the impact of online and social media platforms on children and teens. The initiative can be found on X as @Parents4SOS, on Facebook as Parents for Safe Online Spaces, and online at parentssos.org.



This report was produced with support from **Heat Initiative**, a nonprofit working to hold the world's most valuable and powerful tech companies accountable for failing to protect kids from online sexual exploitation.

