AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

LEGISLATIVE SOLUTIONS TO PROTECT CHILDREN AND TEENS ONLINE

HEARING

BEFORE THE

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

DECEMBER 2, 2025

Serial No. 119–44

Published for the use of the Committee on Energy and Commerce

govinfo.gov/committee/house-energy
energycommerce.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE

62–241 PDF WASHINGTON : 2026

COMMITTEE ON ENERGY AND COMMERCE

BRETT GUTHRIE, Kentucky
Chairman

ROBERT E. LATTA, Ohio
H. MORGAN GRIFFITH, Virginia
GUS M. BILIRAKIS, Florida
RICHARD HUDSON, North Carolina
EARL L. "BUDDY" CARTER, Georgia
GARY J. PALMER, Alabama
NEAL P. DUNN, Florida, *Vice Chairman*
DAN CRENSHAW, Texas
JOHN JOYCE, Pennsylvania
RANDY K. WEBER, SR., TEXAS
RICK W. ALLEN, Georgia
TROY BALDERSON, Ohio
RUSS FULCHER, Idaho
AUGUST PFLUGER, Texas
DIANA HARSHBARGER, Tennessee
MARIANNETTE MILLER-MEEKS, Iowa
KAT CAMMACK, Florida
JAY OBERNOLTE, California
JOHN JAMES, Michigan
CLIFF BENTZ, Oregon
ERIN HOUCHIN, Indiana
RUSSELL FRY, South Carolina
LAUREL M. LEE, Florida
NICHOLAS A. LANGWORTHY, New York
THOMAS H. KEAN, JR., New Jersey
MICHAEL A. RULLI, Ohio
GABE EVANS, Colorado
CRAIG A. GOLDMAN, Texas
JULIE FEDORCHAK, North Dakota

FRANK PALLONE, JR., New Jersey
Ranking Member
DIANA DEGETTE, Colorado
JAN SCHAKOWSKY, Illinois
DORIS O. MATSUI, California
KATHY CASTOR, Florida
PAUL TONKO, New York
YVETTE D. CLARKE, New York
RAUL RUIZ, California
SCOTT H. PETERS, California
DEBBIE DINGELL, Michigan
MARC A. VEASEY, Texas
ROBIN L. KELLY, Illinois
NANETTE DIAZ BARRAGÁN, California
DARREN SOTO, Florida
KIM SCHRIER, Washington
LORI TRAHAN, Massachusetts
LIZZIE FLETCHER, Texas
ALEXANDRIA OCASIO-CORTEZ, New York
JAKE AUCHINCLOSS, Massachusetts
TROY A. CARTER, Louisiana
ROBERT MENENDEZ, New Jersey
KEVIN MULLIN, California
GREG LANDSMAN, Ohio
JENNIFER L. MCCLELLAN, Virginia

PROFESSIONAL STAFF

MEGAN JACKSON, *Staff Director*
SOPHIE KHANAHMADI, *Deputy Staff Director*
TIFFANY GUARASCIO, *Minority Staff Director*

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

GUS M. BILIRAKIS, Florida
Chairman

RUSS FULCHER, Idaho, *Vice Chairman*
NEAL P. DUNN, Florida
KAT CAMMACK, Florida
JAY OBERNOLTE, California
JOHN JAMES, Michigan
CLIFF BENTZ, Oregon
ERIN HOUCHIN, Indiana
RUSSELL FRY, South Carolina
LAUREL M. LEE, Florida
THOMAS H. KEAN, JR., New Jersey
GABE EVANS, Colorado
CRAIG A. GOLDMAN, Texas
BRETT GUTHRIE, Kentucky (ex officio)

JAN SCHAKOWSKY, Illinois
Ranking Member
KATHY CASTOR, Florida
DARREN SOTO, Florida
LORI TRAHAN, Massachusetts
KEVIN MULLIN, California
YVETTE D. CLARKE, New York
DEBBIE DINGELL, Michigan
MARC A. VEASEY, Texas
ROBIN L. KELLY, Illinois
KIM SCHRIER, Washington
FRANK PALLONE, JR., New Jersey *(ex officio)*

C O N T E N T S

Page

Hon. Gus M. Bilirakis, a Representative in Congress from the State of Florida, opening statement 2
Prepared statement 3
Hon. Jan Schakowsky, a Representative in Congress from the State of Illinois, opening statement 5
Prepared statement 6
Hon. Kevin Mullin, a Representative in Congress from the State of California, prepared statement 8
Hon. Brett Guthrie, a Representative in Congress from the Commonwealth of Kentucky, opening statement 9
Prepared statement 11
Hon. Frank Pallone, Jr., a Representative in Congress from the State of New Jersey, opening statement 14
Prepared statement 16

WITNESSES

Marc Berkman, Chief Executive Officer, Organization for Social Media Safety 18
Prepared statement 20
Answers to submitted questions 278
Paul Lekas, Executive Vice President, Global Public Policy and Government Affairs, Software & Information Industry Association 38
Prepared statement 40
Answers to submitted questions 283
Kate Ruane, Director, Free Expression Project, Center for Democracy & Technology 52
Prepared statement [1]
Answers to submitted questions 287
Joel Thayer, President, Digital Progress Institute 53
Prepared statement 56

LEGISLATION[2]

H.R. _____, the Children and Teens' Online Privacy Protection Act
Discussion Draft, H.R. _____, the Kids Online Safety Act
Discussion Draft, H.R. _____, the Reducing Exploitative Social Media Exposure for Teens (RESET) Act
H.R. 2657, Sammy's Law
H.R. 3149, the App Store Accountability Act
H.R. 1623, the Shielding Children's Retinas from Egregious Exposure on the Net (SCREEN) Act
H.R. _____, the Safe Social Media Act
H.R. _____, the Algorithmic Choice and Transparency Act
H.R. _____, the No Fentanyl on Social Media Act
H.R. _____, the Promoting a Safe Internet for Minors Act
Discussion Draft, H.R. _____, the Safeguarding Adolescents From Exploitative (SAFE) Bots Act

[1] Ms. Ruane's statement has been retained in committee files and is available at https://docs.house.gov/meetings/IF/IF17/20251202/118714/HHRG-119-IF17-Wstate-RuaneK-20251202.pdf.

[2] The bills have been retained in committee files and are available at https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=118714.

Page

Discussion Draft, H.R. _____, the Kids Internet Safety Partnership Act[2]
H.R. 5360, the AI Warnings And Resources for Education (AWARE) Act[2]
H.R. 6265, the Safer Guarding of Adolescents from Malicious Interactions on Network Games (GAMING) Act[2]
Discussion Draft, H.R. _____, the Assessing Safety Tools for Parents and Minors Act[2]
H.R. _____, the Stop Profiling Youth and (SPY) Kids Act[2]
H.R. _____, the Safe Messaging for Kids Act[2]
H.R. _____, the Don't Sell Kids' Data Act of 2025[2]
Discussion Draft, H.R. _____, the Parents Over Platforms Act[2]

SUBMITTED MATERIAL

Inclusion of the following was approved by unanimous consent.
List of documents submitted for the record 102
Letters from multiple correspondents to Mr. Guthrie, et al.[3]
Letter of November 3, 2025, from Penny Young Nance, Chief Executive Officer and President, Concerned Women for America, to committee members .. 104
Letter of December 1, 2025, from Nicole Smith, President, Dignity Defense Institute, to Mr. Guthrie, et al. 105
Letter of December 2, 2025, from Morgan Reed, President, ACT–the App Association, to Mr. Bilirakis, et al. 107
Letter of November 26, 2025, from Sam A. Cabral, International President, International Union of Police Associations, to Mr. Bilirakis, et al. 113
Letter of December 1, 2025, from Engine to Mr. Bilirakis and Ms. Schakowsky 115
Letter of December 1, 2025, from Association of Ministers in Utah, et al., to Mr. Guthrie and committee members 118
Letter of December 1, 2025, from the Center for Innovation and Free Enterprise to Mr. Guthrie, et al. 120
Letter from Erich Mische, Chief Executive Officer, Suicide Awareness Voices of Education (SAVE), to Mr. Bilirakis, et al. 121
Poll data from Digital Childhood Alliance, May 1, 2025 126
Letter of December 1, 2025, from Indiana University College Republicans to Mr. Guthrie, et al. 129
Letter from Raul Lopez, Chairman of the Board and Cofounder, and Tommy Vallejos, Executive Director and Cofounder, Latinos for Tennessee. to Mr. Guthrie, et al. 131
Letter of December 1, 2025, from the Main Street Privacy Coalition to Mr. Guthrie, et al. 133
Letter of December 1, 2025, from Hilary Ware, Global Head of Privacy, Apple, to Mr. Bilirakis and Ms. Schakowsky 135
Letter of December 2, 2025, from Chan Park, Head of U.S. and Canada Policy and Partnerships, OpenAI, to Mr. Bilirakis and Ms. Schakowsky 139
Statement of Amy Bos, Vice President of Government Affairs, NetChoice, to subcommittee, December 2, 2025 141
Letter of December 2, 2025, from Arjun Bhatnagar, Chief Executive Officer, Cloaked, to subcommittee members 145
Letter of December 2, 2025, from Center for Black Equity, et al., to subcommittee members 146
Federal Trade Commission documents related to app stores 150
Letter of December 2, 2025, from Digital Childhood Alliance, et al., to Mr. Guthrie, et al. 169
Letter of December 1, 2025, from Stephanie Smith, President and Chief Executive Officer, Alabama Policy Institute, to Mr. Guthrie, et al. 173
Letter from Sheriff Michael J. Murphy, Livingston County, Michigan, to committee members 175
Letter of December 1, 2025, from Design It For Us, et al., to Mr. Guthrie and Mr. Pallone 176
Letter of November 24, 2025, from various parents to House Speaker Mike Johnson, et al. 178

---

[2] The bills have been retained in committee files and are available at https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=118714.

[3] The information has been retained in committee files and is included in the Documents for the Record at https://docs.house.gov/meetings/IF/IF17/20251202/118714/HHRG-119-IF17-20251202-SD003.pdf.

Page

Statement by AAJ: "OPPOSE House KOSA & COPPA 2.0" 189
Letter of December 1, 2025, from Hilary Ware, Global Head of Privacy, Apple, to Mr. Bilirakis and Ms. Schakowsky 192
Letter of December 1, 2025, from Tom Kemp, Executive Director, California Privacy Protection Agency, to Mr. Guthrie, et al. 196
Letter of October 15, 2025, from Active Minds, et al., to Senate Majority Leader John Thune, et al. 199
Letter from Holly Grosshans, Senior Counsel, Tech Policy, Common Sense Media 213
Letter of December 1, 2025, from ParentsSOS to subcommittee members 215
Report, "Social Media and Youth Mental Health, The U.S. Surgeon General's Advisory," 2023 [3]
Report, "Health Advisory on Social Media Use in Adolescence," American Psychological Association, May 2023 217
Report, "Teens, Social Media and Mental Health," by Michelle Faverio, et al., Pew Research Center, April 22, 2025 [3]
Statement of Cayce Savage to the Senate Judiciary Committee's Subcommittee on Privacy, Technology, and the Law, September 6, 2025 229
Responses to Senate Judiciary Committee questions for the record from Cayce Savage 235
Statement of Jason Sattizahn to the Senate Judiciary Committee's Subcommittee on Privacy, Technology, and the Law, September 9, 2025 253
Responses to Senate Judiciary Committee questions for the record from Jason Sattizahn 260
Report, "Teen Accounts, Broken Promises: How Instagram is Failing to Protect Minors" [3]

---

[3] The information has been retained in committee files and is included in the Documents for the Record at https://docs.house.gov/meetings/IF/IF17/20251202/118714/HHRG-119-IF17-20251202-SD003.pdf.

LEGISLATIVE SOLUTIONS TO PROTECT CHILDREN AND TEENS ONLINE

TUESDAY, DECEMBER 2, 2025

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 10:18 a.m., in the John D. Dingell Room 2123, Rayburn House Office Building, Hon. Gus Bilirakis (chairman of the subcommittee) presiding.

Members present: Representatives Bilirakis, Fulcher, Dunn, Cammack, Obernolte, James, Bentz, Houchin, Fry, Lee, Kean, Evans, Goldman, Guthrie (ex officio), Schakowsky (subcommittee ranking member), Castor, Soto, Trahan, Mullin, Clarke, Dingell, Kelly, Schrier, and Pallone (ex officio).

Also present: Representatives Joyce and Miller-Meeks.

Staff present: Christian Calvert, Press Assistant; Jessica Donlon, General Counsel; Sydney Greene, Director of Finance and Logistics; Megan Jackson, Staff Director; AT Johnson, Special Advisor; Daniel Kelly, Press Secretary; Sophie Khanahmadi, Deputy Staff Director; Alex Khlopin, Policy Analyst, Commerce, Manufacturing, and Trade; Brayden Lacefield, Special Assistant; Giulia Leganski, Chief Counsel, Commerce, Manufacturing, and Trade; Joel Miller, Chief Counsel; Evangelos Razis, Professional Staff Member, Commerce, Manufacturing, and Trade; Seth Ricketts, Special Assistant; Chris Sarley, Member Services/Stakeholder Director; Matt VanHyfte, Communications Director; Hannah Anton, Minority Policy Analyst; Keegan Cardman, Minority Staff Assistant; Kelly Fabian, Minority Chief Counsel, Commerce, Manufacturing, and Trade; Waverly Gordon, Minority Deputy Staff Director and General Counsel; Tiffany Guarascio, Minority Staff Director; Jackson Hall, Minority Intern; Perry Hamilton, Minority Deputy Director, Member Services and Outreach; Megan Kanne, Minority Professional Staff Member; Phoebe Rouge, Minority FTC Detailee; and Andrew Souvall, Minority Director of Communications, Outreach, and Member Services.

Mr. BILIRAKIS. The committee will come to order.

The chairman recognizes himself for 5 minutes for an opening statement.

OPENING STATEMENT OF HON. GUS M. BILIRAKIS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA

Good morning, and welcome to today's hearing to discuss legislative solutions to protect children online.

Our children are facing an online epidemic. This issue is personal. We have parents on both sides of the aisle, and we all have constituents who have been affected. They are why we are here today.

We are examining almost 20 bills today which together form a comprehensive strategy to protect kids online. Our approach is straightforward: Protect kids, empower parents, and future-proof our legislation as new risks and technologies emerge.

These bills are not stand-alone solutions. They complement and reinforce one another to create the safest possible environment for our children. There is no one-size-fits-all bill to protect kids online, and our plan reflects that.

Parents must be empowered to safeguard their children online. Just as a parent can observe their children's activities and social behaviors at home and at school functions, so should they be able to check on their kids' activities online.

Our bills ensure parents have the tools and resources to keep their children safe in the modern world. A child's life in the 21st century is much more complex than generations past, and parents need the tools to adapt.

Our bills are mindful of the Constitution's protections for free speech. We have seen it in the States: Laws with good intentions have been struck down for violating the First Amendment. We are learning from those experiences, because a law that gets struck down in court does not protect a child. And the status quo is unacceptable, as far as I am concerned.

All our bills employ this strategy, including the Kids Online Safety Act, or KOSA, that I am proud to lead. KOSA sets a national standard to protect kids across America and mandates default safeguards and easy-to-use parental controls to empower families.

It blocks children from being exposed to or targeted with ads for illegal or inappropriate content like drugs and alcohol. It takes on addictive design features that keep kids hooked and harm their mental health. And, most importantly, it holds Big Tech accountable with mandatory audits and strong enforcement by the FTC and State attorneys general.

I made precise changes to ensure KOSA is durable. Don't mistake durability for weakness, folks. This bill has teeth. By focusing on design features rather than protecting speech, we will ensure it can withstand legal challenge while delivering real protections for kids online—kids and their families.

I am proud of the members of this subcommittee for working on legislation to address a myriad of harms and challenges. This issue is personal to every one of us up here. It shows in the number of bills before us today. I know this is a shared, bipartisan goal.

My office is open. Call me or find me on the floor. I think you know that I am willing to listen. Let's find a way to work together. And this is not a partisan issue, folks. Let's find a way to work together and save America's kids from the threats they are facing online. That is the bottom line.

[The prepared statement of Mr. Bilirakis follows:]

Good morning, and welcome to today's hearing to discuss legislative solutions to protect children online.

Our children are facing an online epidemic. This issue is personal – we have parents on both sides of the aisle, and we all have constituents who have been affected. They are why we're here today.

We're examining almost twenty bills, which together form a comprehensive strategy to protect kids online. Our approach is straightforward: protect kids, empower parents, and future proof our legislation as new risks and technologies emerge.

These bills are not standalone solutions. They complement and reinforce one another to create the safest possible environment for children. There is no one-size-fits-all bill to protect kids online--and our plan reflects that.

Parents must be empowered to safeguard their children online. Just as a parent can observe their children's activities and social behaviors at home and at school functions, so should they be able to check on their kid's activities online. Our bills ensure parents have the tools and resources to keep their children safe in the modern world. A child's life in the 21st century is much more complex than generations past, and parents need the tools to adapt.

Our bills are mindful of the Constitution's protections for free speech. We've seen it in the states –laws with good intentions have been struck down for violating the First Amendment. We are learning from those experiences because a law that gets struck down in court does not protect a single child. And the status quo is unacceptable.

All our bills employ this strategy–including the Kids Online Safety Act, or KOSA, that I am proud to lead. KOSA sets a national standard to protect kids across America. It mandates default safeguards and easy-to-use parental controls to empower families.

It blocks children from being exposed to or targeted with ads for illegal or inappropriate content like drugs and alcohol. It takes on addictive design features that keep kids hooked and harm their mental health. And most importantly, it holds Big Tech accountable with mandatory audits and strong enforcement by the FTC and state attorneys general.

I made precise changes to ensure KOSA is durable. Don't mistake durability for weakness – this bill has teeth. By focusing on design features rather than protected speech we will ensure it can withstand legal challenge while delivering real protections for kids and families.

I am proud of the members of this subcommittee for working on legislation to address a myriad of harms and challenges. This issue is personal to every one of us up here, and it shows in the number of bills before us today. I know this is a shared, bipartisan goal – my office is open, call me, or find me on the floor. Let's find a way to work together and save America's kids from the threats they are facing online. With that, I yield back.

Mr. BILIRAKIS. I yield back the balance of my time.

The chairman recognizes the ranking member, Ms. Schakowsky, for her 5 minutes for an opening statement.

You are recognized.

OPENING STATEMENT OF HON. JAN SCHAKOWSKY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS

Ms. SCHAKOWSKY. Thank you, Mr. Chairman.

There is not a single thing that we deal with, in my view, that is more important than to take care of our kids. And I believe that the legislation that has been offered by the Republicans does not do the job. And it is really frustrating, because we have been working on this bill and moving it around here and there for a long time.

Yesterday, I had the privilege of meeting with three women, who are here today in the audience, who have been here for 5 years because their children died not necessarily. They didn't need to die. And it is the kinds of things that we can learn from them that we can do much better.

I mean to say that the—that—who can't—yes, the different States—what is it? The States—States—sorry—cannot do their own bill—cannot do their own bill. I am sorry. We have a long, long way to go to protect our children and to make sure that all are involved.

[The prepared statement of Ms. Schakowsky follows:]

Committee on Energy and Commerce

Opening Statement as Prepared for Delivery
of
Subcommittee on Commerce, Manufacturing, and Trade Ranking Member Jan Schakowsky

Hearing on "Legislative Solutions to Protect Children and Teens Online"

December 2, 2025

Congress has to ensure the internet is a safe place. Big Tech continues to make billions by exploiting and manipulating our children. These bills are not enough! Congress must pass a comprehensive privacy bill to protect all Americans. Until then, blocking states from protecting kids is a shameless handout to corporations and billionaires.

I yield to Rep. Mullin.

Ms. SCHAKOWSKY. Now I want to yield at this point to Congressman Mullin to continue in this discussion.

Mr. MULLIN. Thank you, Ranking Member Schakowsky, and thank you, Mr. Chair, for convening this hearing on a very important topic.

Protecting kids is perhaps the single most unifying, bipartisan issue we have here in Congress. We all want to keep our kids safe. I myself am the father of two small boys who aren't yet—but will be before I know it—an age when they will be navigating the internet on their own. To say I am worried for them is an understatement.

But the country and Congress is not without tools to keep people safe online. In fact, more than 100 years ago, the Federal Trade Commission was set up to prevent harms to consumers of all kinds, including kids. Indeed, most of the bills we will be discussing today rely on the FTC to enforce them.

So that is why it has been stunning to see the contempt in which the Trump administration has held the FTC. Rather than seeking from Congress a change in the law, President Trump has simply attempted to unlawfully fire two of its Commissioners, eliminating bipartisan input.

Meanwhile, the Chair of the FTC has attempted to dramatically reduce the Commission's staff through buy-outs and other drastic measures. He has actually bragged that he wants to get the Commission's staff size to its lowest level in 10 years.

The Chair has also been using the tools of the FTC to wage a culture war against medical professionals and parental choices he disagrees with. This is more than a harmful deviation from the Commission's mission. It undermines consumer protections for all of us by taking cops off their normal beat.

Yet today we will be talking about all the things we want and need the FTC to do to protect kids online. But who will be doing that work? The remaining employees at the FTC, who are already stretched too thin?

As evidenced by this long list of bipartisan bills, there is clearly a lot of alignment across the parties about the role we want the FTC to play. In that spirit, I hope that, as we discuss the legislative proposals today, we acknowledge the need to fully fund the FTC, protect its bipartisan commission structure, and ensure the FTC is focused on the mission Congress gives it.

I look forward to a robust discussion today.

[The prepared statement of Mr. Mullin follows:]

Committee on Energy and Commerce

Opening Statement as Prepared for Delivery
of
Subcommittee on Commerce, Manufacturing, and Trade Member Kevin Mullin

Hearing on "Legislative Solutions to Protect Children and Teens Online"

December 2, 2025

Thank you Ranking Member Schakowsky, and thank you Mister Chair for convening this hearing on such an important topic.

Protecting kids is perhaps the single most unifying, bipartisan issue we have here in Congress. We all want to keep our kids safe. I myself am the father of two young boys who aren't yet – but will be before I know it – an age when they will be navigating the Internet on their own. To say I am worried for them is an understatement.

But the country – and Congress – is not without tools to keep people safe online. In fact, more than one hundred years ago, the Federal Trade Commission was set up to prevent harms to consumers of all kinds, including kids. Indeed, most of the bills we will be discussing today rely on the FTC to enforce them.

So that is why it has been stunning to see the contempt in which the Trump Administration has held the Commission. Rather than seeking from Congress a change in the law, President Trump has simply attempted to unlawfully fire two of its commissioners, eliminating bipartisan input.

Meanwhile, Chair Ferguson has attempted to dramatically reduce the Commission's staff through buyouts and other drastic measures. He bragged that he wants to get the Commission's staff size to its lowest in 10 years. The Chair has also been using the tools of the FTC to wage a culture war against medical professionals and parental choices he disagrees with. This is more than a harmful deviation from the Commission's mission – it undermines consumer protections for all of us by removing cops from their normal beat.

Yet today we will be talking about all of the things we want and need the FTC to do to protect kids online. But who will be doing that work? The remaining employees at the FTC who are already stretched thin?

As evidenced by this long list of bipartisan bills, there is clearly a lot of alignment across parties about the role we want the FTC to play. In that spirit, I hope that, as we discuss the legislative proposals on today's agenda, we acknowledge the need to fully fund the FTC, protect its bipartisan commission structure, and ensure the FTC is focused on the mission Congress gives it.

I look forward to a robust discussion today. I yield back.

Mr. MULLIN. With that, I yield back.

Mr. BILIRAKIS. The gentleman yields back.

I now recognize the chairman of the full committee, Mr. Guthrie, for his 5 minutes.

OPENING STATEMENT OF HON. BRETT GUTHRIE, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF KENTUCKY

Mr. GUTHRIE. Thank you, Chairman Bilirakis. Thanks for having this hearing today. And thank you to our witnesses for being with us here today.

Tragedy strikes children every day online. In March, I shared the story of a constituent who took his life due to a sextortion scheme. I know each of us here today and many others have similar stories to share. And while we passed the TAKE IT DOWN Act into law earlier this Congress to address sextortion, countless other harms persist, and it is our responsibility to find a solution.

That is why we are here today. We have almost two dozen bills before us that take a broad approach to create a comprehensive strategy to protect children online.

Imagine a 14-year-old child trying to download a social media app on their phone. There are many different layers needed to protect them from harm. And we are discussing a comprehensive approach today, where different types of legislation could work in harmony to address various concerns.

For example, age verification is needed first and foremost, including appropriate parental consent, even before logging in. Once a user's age is known, privacy protections under COPPA 2.0 would be triggered.

We also have a range of bills to further address issues like parental monitoring of online activity, restrictions on the types of apps kids can access, how information is presented to kids in apps, and how children's data is used by online platforms.

And, finally, the Kids Online Safety Act provides robust parental controls and limitations on harmful design features to ensure that platforms live up to these standards.

Now, I would note that we went to great lengths to address concerns that Members of the House on both sides of the aisle raised regarding KOSA in the last Congress, as well as concerns that the previous version would not pass a legal challenge and, thus, not protect a single child. The KOSA we are considering today still holds platforms accountable while addressing these concerns.

Further, when it comes to AI chatbots, we learned about this in committee a couple of weeks ago. The SAFE Bots Act and AWARE Act will ensure users are appropriately informed in their using AI and that there are educational resources for kids, parents, and educators on the safe use of AI chatbots.

These exemplify our strategy that Chairman Bilirakis has highlighted. The online world is large and complex, and there is no silver-bullet solution to protect kids. Each bill we are looking at today could be a piece of a puzzle designed to work together to create the safest possible environment for children online.

They empower parents through parental consent mechanisms, standards for parental tools, and educational resources. They are

curated to withstand constitutional challenges. A law that gets struck down protects no one, and, if that happened, would fail to protect the very children we are here to protect.

We have a unique opportunity to work together to craft a multi-faceted solution to protect children online.

Thank you again to our witnesses for being here. We really appreciate the efforts you made to be here. We greatly look forward to the discussions.

[The prepared statement of Mr. Guthrie follows:]

Chairman Brett Guthrie Opening Statement
December 2, 2025
Legislative Solutions to Protect Children and Teens Online
Subcommittee on Commerce, Manufacturing, and Trade

Thank you, Chairman Bilirakis. Thank you to our witnesses for being here.

Tragedy strikes children online every day. In March, I shared the story of a constituent who took his life due to a sextortion scheme. I know each of us up here, and many others, have similar stories to share. While we passed the TAKE IT DOWN Act into law earlier this Congress to address sextortion, countless other harms persist, and it is our responsibility to find a solution.

That is why we are here today. We have almost two dozen bills before us that take a broad approach to create a comprehensive strategy to protect children online.

Imagine a 14-year-old child trying to download a social media app on their phone. There are many different layers needed to protect them from harm, and we are discussing a comprehensive approach today, where different types of legislation could work in harmony to address various concerns.

For example, age verification is needed first and foremost, including appropriate parental consent, even before logging in. Once a user's age is known, privacy protections under COPPA 2.0 would be triggered. We also have a range of bills to further address issues like parental monitoring of online activity, restrictions on the types of apps kids can access, how information is presented to kids in apps, and how children's data is used by online platforms.

And finally, the Kids Online Safety Act provides robust parental controls and limitations on harmful design features to ensure that platforms live up to these standards. Now, I would note that we went to great lengths to address concerns that Members of the House on both sides of aisle raised regarding KOSA in the last Congress, as well as concerns that the previous version was would not pass a legal challenge, and thus not protect a single child. The KOSA we are considering today still holds platforms accountable, while also addressing these concerns.

Further, when it comes to AI chatbots we learned about in this committee a couple weeks ago, the SAFE BOTS Act and AWARE Act, will ensure users are appropriately informed that they're using AI and that there are educational resources for kids, parents, and educators on the safe use of AI chatbots.

These exemplify our strategy that Chairman Bilirakis highlighted. The online world is large and complex, and there is no silver bullet solution to protect kids. Each bill we are looking at today could be a piece of a puzzle, designed to work together to create the safest possible environment for children online.

They empower parents through parental consent mechanisms, standards for parental tools, and educational resources

They are curated to withstand constitutional challenges. A law that gets struck down protects no one – and if that happened, we've failed the very children we are trying to protect.

We have a unique opportunity to work together to craft a multi-faceted solution to protect children online. Thank you again to the witnesses for being here. I'm greatly looking forward to the discussion and I yield back.

Mr. GUTHRIE. And I would yield back.

Mr. BILIRAKIS. The gentleman yields back.

Now I will recognize the ranking member of the full committee, Mr. Pallone, for his 5 minutes.

OPENING STATEMENT OF HON. FRANK PALLONE, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY

Mr. PALLONE. Thank you, Chairman Bilirakis.

Today, we are discussing the important topic of youth online safety. And as more of our lives are lived online, there have been tremendous changes in how we communicate, socialize, and learn. And with these changes come new challenges to ensuring the health and wellbeing of all Americans but particularly our youngest and most vulnerable.

We can all agree that we want our kids and teens to be safe online. Congress, along with parents, educators, and States, can and should play an active role in keeping minors safe. And that role must include prioritizing strong, comprehensive data privacy legislation, which unfortunately is not included in the 19 bills we are considering today.

Comprehensive data privacy legislation is something I have cared about for many years. But in the absence of data privacy legislation, companies will continue to collect, process, and sell as much of our data and the data of our kids as possible. And this data allows companies to exploit human psychology and individual preferences to fuel invasive ads and design features, without regard to the harm suffered by those still developing critical thinking and judgment.

Artificial intelligence is only accelerating existing incentives because, like social media, AI relies on the exploitation of our data.

Without such a strong legislative solution for children, teens, and all Americans, we must recognize that the measures we take in Congress will not address the full scope of the problems perpetrated by an online ecosystem fundamentally built on reckless and abusive data practices. We can and should do more for our children and for all consumers.

But if comprehensive privacy legislation was easy, it would already be law. And the urgency of addressing harms to children and teens presents an opportunity to make progress towards ensuring the internet is a safer place for all Americans.

This is why I am pleased we will be discussing my bill that will prevent shadowy data brokers from selling minors' data and allow parents and teens to request the deletion of any data already in the hands of brokers.

We simply should not allow nameless data harvesters to profit off of our kids' data. Our kids deserve the right to enter adulthood with a clean slate, not a detailed dossier that will follow them throughout their adult lives.

They also deserve online safety legislation that will make the internet safer, not put their data and physical safety more at risk. And I am concerned that mandating third-party access to children's data and requiring additional collection and sharing of sensitive data before accessing content, sending a message, or downloading

an app would move us in the wrong direction in the fight for online privacy.

Congress must also remember that, unfortunately, many kids find themselves in unsupportive or even abusive or neglected households. There can be real-world harm from allowing parents complete access and control over their teens' existence online.

Instead of shifting ever more burden onto parents and teens and putting ever more trust in tech companies, we can give everyone safer defaults and more control over their digital lives.

We can also require companies to evaluate their algorithms for bias and harms before making our kids the guinea pigs.

And we can resist efforts to preempt existing protections and let States continue to respond to rapidly evolving technologies, like AI chatbots, and enforce their existing child safety and privacy laws.

And we can all stand up for an independent Federal Trade Commission.

Now, the FTC, under both Republican and Democratic leadership, has consistently been Americans' strongest champion against the abuses of all who seek to exploit our Nation's children and adults for profit both on- and offline. When President Trump attempted to illegally fire the FTC's Democratic Commissioners, he made our children less safe online.

If my Republican colleagues want to further empower the FTC to protect kids and teens, they must join Democrats in standing up for a bipartisan and independent FTC. They should join us in demanding that the Democratic Commissioners be reinstated.

So I look forward to the discussion today on this important issue.

[The prepared statement of Mr. Pallone follows:]

Committee on Energy and Commerce

Opening Statement as Prepared for Delivery
of
Full Committee Ranking Member Frank Pallone, Jr.

Hearing on "Legislative Solutions to Protect Children and Teens Online"

December 2, 2025

Today we are discussing the important topic of youth online safety. As more of our lives are lived online, there have been tremendous changes in how we communicate, socialize, and learn. With these changes come new challenges to ensuring the health and well-being of all Americans, but particularly our youngest and most vulnerable.

We can all agree that we want our kids and teens to be safe online. Congress, along with parents, educators, and states, can and should play an active role in keeping minors safe. And that role must include prioritizing strong, comprehensive data privacy legislation, which unfortunately is not included in the 19 bills we are considering today. Comprehensive data privacy legislation is something I've cared about for years.

In the absence of data privacy legislation, companies will continue to collect, process, and sell as much of our data – and the data of our kids – as possible. This data allows companies to exploit human psychology and individual preferences to fuel invasive ads and design features – without regard to the harm suffered by those still developing critical thinking and judgment. Artificial intelligence is only accelerating existing incentives, because like social media, AI relies on the exploitation of our data.

Without such a strong legislative solution for children, teens, and all Americans, we must recognize that the measures we take in Congress will not address the full scope of the problems perpetrated by an online ecosystem fundamentally built on reckless and abusive data practices. We can and should do more for our children, and for all consumers.

But if comprehensive privacy legislation was easy, it would already be law. And the urgency of addressing harms to children and teens presents an opportunity to make progress towards ensuring the internet is a safer place for all Americans.

This is why I am pleased we will be discussing my bill that will prevent shadowy data brokers from selling minors' data and allow parents and teens to request the deletion of any data already in the hands of brokers. We simply should not allow nameless data harvesters to profit off of our kids' data. Our kids deserve the right to enter adulthood with a clean slate, not a detailed dossier that will follow them throughout their adult lives.

They also deserve online safety legislation that will make the internet safer – not put their data and physical safety more at risk. I am concerned that mandating third party access to children's data and requiring additional collection and sharing of sensitive data before accessing content, sending a message, or downloading an app would move us in the wrong

direction in the fight for online privacy. Congress must also remember that unfortunately many kids find themselves in unsupportive or even abusive or neglectful households. There can be real world harms from allowing parents complete access and control over their teens' existence online.

Instead of shifting ever more burden onto parents and teens, and putting ever more trust in tech companies, we can give everyone safer defaults and more control over their digital lives. We can also require companies to evaluate their algorithms for bias and harms before making our kids the guinea pigs. We can resist efforts to preempt existing protections and let states continue to respond to rapidly evolving technologies, like AI chatbots, and enforce their existing child safety and privacy laws. And we can all stand up for an independent Federal Trade Commission.

The FTC, under both Republican and Democratic leadership, has consistently been Americans' strongest champion against the abuses of all who seek to exploit our nation's children and adults for profit both on and offline. When President Trump attempted to illegally fire the FTC's Democratic commissioners, he made our children less safe online. If my Republican colleagues want to further empower the FTC to protect kids and teens, they must join Democrats in standing up for a bipartisan and independent FTC. They should join us in demanding that the Democratic commissioners be reinstated.

I look forward to the discussion today on this important issue and I yield back the balance of my time.

Mr. PALLONE. And I thank you, Mr. Chairman, and yield back the balance of my time.

Mr. BILIRAKIS. The gentleman yields back. We appreciate that.

And now we are going to introduce our witnesses for today.

Mr. Marc Berkman, CEO of the Organization for Social Media Safety, welcome, sir.

Mr. Paul Lekas, executive vice president, Software & Information Industry Association, welcome.

Ms. Kate Ruane, director of the Free Expression Project, Center for Democracy & Technology, welcome.

And Mr. Joel Thayer, who is president of the Digital Progress Institute.

Welcome to all our witnesses.

So, Mr. Berkman, you are recognized for your 5 minutes of testimony.

STATEMENTS OF MARC BERKMAN, CHIEF EXECUTIVE OFFICER, ORGANIZATION FOR SOCIAL MEDIA SAFETY; PAUL LEKAS, EXECUTIVE VICE PRESIDENT, GLOBAL PUBLIC POLICY AND GOVERNMENT AFFAIRS, SOFTWARE & INFORMATION INDUSTRY ASSOCIATION; KATE RUANE, DIRECTOR, FREE EXPRESSION PROJECT, CENTER FOR DEMOCRACY & TECHNOLOGY; AND JOEL THAYER, PRESIDENT, DIGITAL PROGRESS INSTITUTE

STATEMENT OF MARC BERKMAN

Mr. BERKMAN. Thank you, Mr. Chairman.

Good afternoon and thank you to the distinguished members of this committee for the opportunity to offer my organization's social media safety expertise at this historic legislative hearing to protect our children from online harms.

My name is Marc Berkman, and I am the CEO of the Organization for Social Media Safety, the first national nonpartisan consumer-protection organization focused exclusively on social media.

The reason for this legislative hearing must be explicitly clear: Social media is harming children. It is harming millions of America's children.

Up to 95 percent of youth ages 13 to 17 report using a social media platform, with more than a third saying they use social media almost constantly. Nearly 40 percent of children ages 8 to 12 use social media. In our own study with the UCLA School of Education including over 16,000 teens, we have found that 50 percent self-report using social media for more than 5 hours daily.

The evidence, based on credible research and testimony in this very chamber, shows severe, pervasive harms related to adolescent social media use: cyberbullying, harassment, predation, human trafficking, drug trafficking, violence, fraud, sextortion, suicide, depression, cognitive impairment, eating disorders, and more.

Social media-related harm is far reaching, impacting homes in every congressional district, families of every demographic. But to understand the true toll, we need look no further than the many parents here with us today who have tragically lost a child to a social media-related threat.

Sitting behind me is Rose Bronstein. Her son, Nate Bronstein, forever 15, died by suicide after suffering severe cyberbullying over social media. And Samuel Chapman. His son, Sammy Chapman, forever 16, died after ingesting fentanyl-poisoned drugs that he easily acquired from a drug dealer operating on social media.

Rose and Sam and the many other angel parents who traveled from across the country to be here today have collectively spent years fiercely and bravely advocating for urgently needed legislative reform in the hope that Congress acts to ensure that other families do not have to suffer such tragedies. We owe them a debt of gratitude.

The record on the extent and severity of the social media-related harm impacting our children is clear, yet the social media industry continues to fail to protect our children.

Thank you to the brave work of whistleblowers and attorneys general across the country.

We know that the industry has an entrenched, durable conflict of interest when it comes to safety. Even in the face of mounting child fatalities, social media executives have prioritized growing the number of child users and engagement on their platforms over our children's safety, making a Federal legislative response absolutely essential and critically urgent. The social media industry has been too slow, their solutions too ineffective, their apathy, sadly, too apparent.

And so we are grateful that the committee today recognizes that a broad approach with multiple tactics are needed: resources for education; accountability and rules for platforms; research; privacy reforms; and, critically, safety technology.

I would like to highlight Sammy's Law.

One of the most effective ways for parents to protect children is by using third-party safety software, which can provide alerts to parents when dangerous content is shared through children's social media accounts, enabling lifesaving interventions at critical moments.

For example, if a child is suffering severe cyberbullying via social media, then a parent who has received an alert through third-party safety software can immediately provide critical support.

We know that this intervention is highly effective. Over the last several years, safety software companies have provided alerts to parents that have protected millions of children, saving numerous lives.

Sammy's Law will finally provide families with this option on all major social media platforms, while also substantially increasing data security and child privacy over the status quo. We urge this committee to pass this bipartisan, commonsense legislation that will save lives.

American families have sat for years living in quiet despair, watching social media steal from their children's potential and wellbeing. We are hopeful that this year this committee can join together and deliver the solutions families so desperately need.

Thank you, and I look forward to your questions.

[The prepared statement of Mr. Berkman follows:]

Testimony before Subcommittee on Commerce, Manufacturing, and Trade

Committee on Energy and Commerce

United States House of Representatives

Hearing:

December 2, 2025

Marc Berkman

Chief Executive Officer

Organization for Social Media Safety

Good afternoon. Chairman Bilirakis, Ranking Member Schakowsky, Chairman Guthrie, Ranking Member Pallone, and the distinguished members of the Committee, thank you for the opportunity to testify on this critical issue.

My name is Marc Berkman, and I am the CEO of the Organization for Social Media Safety (OFSMS), the first national, nonprofit consumer protection organization focused exclusively on social media. Through education, advocacy, technology, and research, we seek to make social media safer for families. We conduct cutting-edge research on social media safety. We advocate on a nonpartisan basis to improve public policy regarding social media safety. We collaborate with K-12 schools nationwide to educate students, caregivers, and educators on essential social media safety skills. OFSMS works with hundreds of thousands of families and

educators each year, giving us a uniquely comprehensive view into the emerging and ongoing threats related to social media use.

OFSMS expresses its sincere appreciation to the leadership and membership of this Committee for your strong bipartisan efforts to protect families from the dangers associated with social media use.

Social Media-Related Harms Are a Public Health Crisis

Today, this Committee examines legislation seeking to protect America's children from online harm. A reasoned analysis of these proposals requires a review of the threats posed to children that are caused or exacerbated by social media. While time and space constraints preclude an exhaustive analysis, even a cursory review demonstrates, with clarity, the severity and pervasiveness of social media-related injury amongst our children.

Since 2007, social media use has surged across the world with the number of social media users reaching about 4.76 billion in 2024. 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."[1] Nearly 40% of children ages 8–12 use social media.[2] In our own research in partnership with UCLA's School

[1] Vogels, E., Gelles-Watnick, R. & Massarat, N. (2022). Teens, Social Media and Technology 2022. Pew Research Center: Internet, Science & Tech. United States of America.
https://www.pewresearch.org/internet/2022/08/10/teenssocial-media-and-technology-2022/
[2] 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.
https://www. commonsensemedia.org/sites/default/files/research/report/818-census-integrated-report-final-web_0.pdf

of Education and Information Studies, including over 16,000 teens, we have found that about 50% self-report using social media for more than 5 hours daily.[3]

With this mass adoption of social media, numerous, serious social media-related dangers have emerged. Here is a sample of the available research showing that social media is harming millions of American children:

- **Cyberbullying:** About 58% of youth have experienced cyberbullying in their lifetimes.[4] Cyberbullying victims are about **2.5 times more likely to attempt suicide.**[5] Longer time spent on social media increases the likelihood of encountering cyberbullying.[6]
- **Self-Harm:** According to one study, about 43% of young adults had seen self-harm content on Instagram. About 32.5% indicated that they had performed the same or similar self-harming behavior consequently.[7] In a 2021 internal Meta survey, more than 8% of respondents aged 13 to 15 reported having seen someone harm themselves, or threaten to do so, on Instagram during the past week.[8]
- **Disordered Eating:** According to one study, new TikTok accounts set up by a 13-year-old were recommended self-harm and eating disorder content within minutes of

---

[3] Ding, Z., Hansen, M. & Ong, C. (2025, April 23-27). Adolescents' exposure to cyberaggression and desensitization to cyberhate on social media [Poster session]. American Educational Research Association 2025 Conference, Denver, CO, United States. https://doi.org/10.3102/IP.25.2197337

[4] Patchin, J. W., & Hinduja, S. (2025). *2025 Cyberbullying data*. Cyberbullying Research Center. https://cyberbullying.org/2025-cyberbullying-data

[5] John, A., Glendenning, A.C., Marchant, A., Montgomery, P., Stewart, A., Wood, S., Lloyd, K. and Hawton, K., (2018). Self-harm, suicidal behaviours, and cyberbullying in children and young people: Systematic review. *Journal of medical internet research, 20*(4), e9044.

[6] Ding, Z., Hansen, M. & Ong, C. (2025, April 23-27). Adolescents' exposure to cyberaggression and desensitization to cyberhate on social media [Poster session]. American Educational Research Association 2025 Conference, Denver, CO, United States. https://doi.org/10.3102/IP.25.2197337

[7] Arendt, F., Scherr, S., & Romer, D. (2019). Effects of exposure to self-harm on social media: Evidence from a two-wave panel study among young adults. *New Media & Society*, *21*(11-12), 2422-2442. https://doi.org/10.1177/14614448198501

[8] Spinks, R. (2025, November 22). *Court filings allege Meta downplayed risks to children and misled the public*. TIME. https://time.com/7336204/meta-lawsuit-files-child-safety/

scrolling the app's For You feed. Eating disorder content was recommended within 8 minutes.[9] An internal research document from Meta reporting that teens who expressed body dissatisfaction were sent 3 times more body-image related / eating disorder adjacent content.[10]

- **Sexting:** About 20% of teens have sent or posted a nude or semi-nude photo or video of themselves with high rates of reported pressure and coercion.[11] Amongst adolescents, the prevalences of forwarding a sext without consent and having a sext forwarded without consent were 12.0% and 8.4%, respectively.[12] (Receiving unwanted sexts or coerced sexting is linked to mental health challenges like depressive symptoms and suicidality, as well as lower self-esteem.) [13]
- **Drug Trafficking:** One in four young people see illicit drugs advertised for sale on social media**.**[14]
- **Sextortion and Sexual Exploitation:** Approximately 5% of middle and high school students reported that they had been the victim of sextortion.[15] In 2024, NCMEC received more than 546,000 reports concerning online enticement, a 192% increase compared to reports in 2023. NCMEC received nearly 100 reports of financial sextortion

---

[9] Center for Countering Digital Hate. (2022). *Deadly by design*.Cente for Countering Digital Hate Inc. https://counterhate.com/wp-content/uploads/2022/12/CCDH-Deadly-by-Design_120922.pdf
[10] Reuters. (2021). *Viewing content on IG: Internal research document* (Redacted). Reuters Investigates. https://www reuters.com/investigates/special-report/assets/usa-tech-meta-teens/Viewing-Content-on-IG_Redacted.pdf
[11] S., P. J. (n.d.). *The nature and extent of sexting among a national sample of Middle and high school students in the U.S*. Archives of sexual behavior. https://pubmed ncbi nlm nih.gov/31309428/
[12] Madigan S, Ly A, Rash CL, Van Ouytsel J, Temple JR. Prevalence of Multiple Forms of Sexting Behavior Among Youth: A Systematic Review and Meta-analysis. JAMA Pediatr. 2018 Apr 1;172(4):327-335. doi: 10.1001/jamapediatrics.2017.5314. PMID: 29482215; PMCID: PMC5875316.
[13] Wachs, S., Wright, M. F., Gámez-Guadix, M., & Döring, N. (2021). How are consensual, non-consensual, and pressured sexting linked to depression and self-harm? The moderating effects of demographic variables. International journal of environmental research and public health, 18(5), 2597.
[14] McCulloch, L., & Furlong, S. (2019). *DM for details: Selling drugs in the age of social media*. Volteface. https://volteface me/dm-details-selling-drugs-age-social-media/
[15] Patchin, J. W., & Hinduja, S. (2020). Sextortion among adolescents: Results from a national survey of US youth. *Sexual Abuse*, *32*(1), 30-54. https://doi.org/10.1177/1079063218800469

each day in 2024. Since 2021, NCMEC has identified 36 boys who have died by suicide because of being victimized by this financial sextortion. Further, NCMEC shared a 200% increase in reports involving sadistic online exploitation by violent online groups that encourage youth to cause harm to themselves and others; these groups manipulate children into behaviors such as self-harm; creating CSAM and sexually exploiting other children (including siblings); harming animals; committing murder; and suicide. [16] About 25% of nine-to-twelve year olds have experienced an online sexual interaction with someone that they believe to be an adult; applications where the most minors reported having had an online sexual experience were Facebook (14%), Instagram (13%), Messenger (13%), Snapchat (12%), and TikTok (11%).[17]

- **Human Trafficking:** Many child trafficking and sex crimes now originate from social media sites where predators gain knowledge of their victims' likes and habits.[18]

These findings, among many others, indicate acute, verifiable harm related to adolescent social media use. The extent of social media-related harm is not mere theory; it is proven and ongoing, and it is distinct from similar threats that impact children in the non-digital world.

Reviewing just a few of the millions of cases of harm, while horrifying, is necessary to understand the scope of the human toll. Here are some of the recent tragedies:

---

[16] National Center for Missing & Exploited Children. (2025). *CyberTipline report 2025.* https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata

[17] Thorn. (2024). *Youth experiences with online image-based abuse and digital risks: 2024 youth monitoring report.* https://info.thorn.org/hubfs/Research/Thorn_24_YouthMonitoring_Report.pdf

[18] United Nations Office on Drugs and Crime. (2020). *Global Report on Trafficking in Persons 2020*. United Nations publication, Sales No. E.20.IV.3. https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_Chapter5.pdf

- After suffering severe cyberbullying over social media, Nate Bronstein, forever 15, died by suicide.[19]
- Sammy Chapman, forever 16, died after ingesting Fentanyl- poisoned drugs that he easily acquired from a drug dealer operating on social media.[20]
- Mason Bogard, forever 15, died after imitating a dangerous challenge he saw on social media.[21]
- Gavin Guffey, forever 17, died by suicide after being sextorted over social media.[22]
- Becca Schmill, forever 15, was raped by a man she met on social media. Cyberbullying followed. To cope, Becca started self-medicating with drugs purchased over social media which tragically were Fentanyl poisoned.[23]
- In April of this year, a 10-year-old girl was abducted by a 27-year-old-man she met on social media.[24]

In addition, to the quantitative and qualitative evidence of acute social media-related harms, many studies suggest a strong link between social media use and negative mental health outcomes, especially among adolescents. The former Surgeon General issued a public health on social media and youth mental health on May 23, 2023.[25] The advisory, in our opinion,

---

[19] *About Nate Bronstein*. Buckets Over Bullying. (2023, June 23). https://bucketsoverbullying.org/nates-story/
[20] TodayShow. (2021, March 21). *Dad of teen who overdosed with drugs from Snapchat recalls moment he discovered son*. TODAY.com. https://www.today.com/health/dr-laura-berman-s-husband-recalls-finding-teenage-son-after-t212415
[21] Bogard, J. (2024, August 4). *After her 15-year-old son died trying a viral choking challenge, this mom is fighting for a safer internet*. People. https://people.com/mom-wants-safer-internet-after-son-died-in-a-viral-choking-challenge-8689773
[22] U.S. Attorney's Office for the District of South Carolina. (2025, January 27). *Nigerian man extradited to the U.S. after being indicted for sextortion scheme that caused death of S.C. teen*. U.S. Department of Justice. https://www.justice.gov/usao-sc/pr/nigerian-man-extradited-us-after-being-indicted-sextortion-scheme-caused-death-sc-teen
[23] Becca Schmill Foundation. (n.d.). https://beccaschmillfdn.org/
[24] Rose, A. (2025, April 17). *10-year-old girl kidnapped by man she met on Roblox, police say*. CNN. https://www.cnn.com/2025/04/17/us/california-kidnapping-roblox-girl-hnk
[25] Office of the Surgeon General (OSG). (2023). *Social Media and Youth Mental Health: The U.S. Surgeon General's Advisory*. U.S. Department of Health and Human Services. https://www.ncbi nlm.nih.gov/books/NBK594759/]

accurately provides a compelling overview of the available research, including the following highlights:

- A longitudinal cohort study of U.S. adolescents aged 12–15 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.[26]
- A study conducted among 14-year-olds 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.[27]
- 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.[28]
- 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.[29]

---

[26] 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

[27] 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

[28] 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

[29] 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

More recent research continues to validate the proposition that social media is causing strong adverse mental health outcomes amongst adolescents:

- Longitudinal research shows that both low and high increases in social media use during early adolescents were significantly associated with lower (worse) cognitive functioning, including memory and reading.[30]
- A 2024 meta-analysis found that social media use was a significant risk factor for self-harm and suicidal ideation.[31]
- In our research, in partnership with UCLA's School of Education, we have found a significant, negative correlation between average daily hours spent on social media and ratings of life satisfaction amongst 5th through 12th grade students.[32]

The Social Media Industry Concedes the Significant Harms Caused by Their Platforms

Even social media executives themselves have readily acknowledged the vast safety concerns here in Congress:

---

[30] Nagata, J.M., Wong, J.H., Kim, K.E., Richardson, R.A., Nayak, S., Potes, C., Rauschecker, A.M., Scheffler, A., Sugrue, L.P., Baker, F.C. and Testa, A. (2025). Social media uses trajectories and cognitive performance in adolescents. *JAMA*. doi: 10.1001/jama.2025.16613

[31] Chen, Z., Liao, X., Yang, J., Tian, Y., Peng, K., Liu, X., & Li, Y. (2024). Association of screen-based activities and risk of self-harm and suicidal behaviors among young people: A systematic review and meta-analysis of longitudinal studies. *Psychiatry research, 338*, 115991. doi: 10.1016/j.psychres.2024.115991

[32] Ding, Z., Hansen, M. & Ong, C. (2025, April 23-27). Adolescents' exposure to cyberaggression and desensitization to cyberhate on social media [Poster session]. American Educational Research Association 2025 Conference, Denver, CO, United States. https://doi.org/10.3102/IP.25.2197337

- Mark Zuckerberg of Meta, conceded among other lapses that Meta, then Facebook, *"didn't do enough to prevent these tools from being used for harm."*[33]
- Shou Zi Chew of TikTok, stated that the "security, privacy, and content manipulation concerns raised about TikTok are really not unique to us. The same issues apply to the other companies."[34]
- And under questioning from Senator Durbin about ongoing issues with grooming, child sexual abuse material, and sextortion, Discord CEO Jason Citron said, "This is an ongoing challenge for all of us."[35]

Given the evidence, including statements by the social media platforms' own leadership, no ambiguity should remain concerning the extent of the harms caused or exacerbated by social media use.

Compelling Evidence of a Durable Conflict of Interest Between Profits and Safety

The social media industry's ethical responsibility to protect children from these harms is unmistakable. Yet, thanks to courageous whistleblowers and the diligent work of state attorneys general across the country, we now have overwhelming evidence that the industry has repeatedly chosen to prioritize profits over children's safety.

---

[33] Zuckerberg, M. (2018, April 11). *Testimony of Mark Zuckerberg, Chairman and Chief Executive Officer, Facebook.* Hearing before the United States House of Representatives Committee on Energy and Commerce.
[34] Chew, S. (2023, March 23). *Testimony of Shou Chew, Chief Executive Officer, TikTok Inc.* Testimony before the U.S. House Committee on Energy and Commerce.
[35] Citron, J. (2024, January 31). *Testimony before the United States Senate Committee on the Judiciary: Big Tech and the Online Child Sexual Exploitation Crisis.* U.S. Senate Committee on the Judiciary.

Again, even just a few of the highlights from the whistleblowers and various court filings makes a most compelling argument for a prevailing culture of willful disregard for the health and well-being of teen and child users:

- New Mexico's unredacted complaint against Snap Inc. asserts that "Snap also complained internally that identifying and protecting minors from sexually explicit content and predatory users would overburden its moderators, "create disproportionate admin costs," and should not be its responsibility. Snap employees pointed to a "case where an account had 75 different reports against it since Oct. '21, mentioning nudes, minors, and extortion, yet the account was still active."[36]
- In North Carolina's case against TikTok, video evidence as released with a TikTok executive making the statement: "We obviously wanted people to spend as much time as possible on TikTok, which can be in contrast to what is best for your mental health."[37]
- Utah's case against TikTok alleges that: TikTok coupled its livestream feature with monetization to create an environment built on exchanging TikTok's virtual currency for sexual and illegal acts. TikTok's internal "Project Meramec" investigation and the admissions of its employees document how TikTok LIVE allows adults to pay young users to strip, pose, and dance provocatively for "diamonds," which can be cashed out for real money.[38]

---

[36] State of New Mexico, Office of the Attorney General. (2024). *Amended complaint, State of New Mexico v. Snap, Inc.* (First Judicial District Court, County of Santa Fe, Sept. 30, 2024). https://www nationalreview.com/wp-content/uploads/2024/10/2024-09-30-SNAP-NM-Amended-Complaint_Redacted.pdf

[37] Cunningham, M. (2025, August 21). *TikTok employees raised concerns that app could be addictive, unsealed edited video shows*. CBS News. https://www.cbsnews.com/news/tiktok-employees-apps-mental-health-court-video-north-carolina-lawsuit/

[38] Utah Department of Commerce, Division of Consumer Protection. (2025, January 3). *News release: Utah Division of Consumer Protections announces release of previously redacted information in TikTok Inc. complaint filing*. https://blog.commerce.utah.gov/2025/01/03/news-release-utah-division-of-consumer-protections-announces-release-of-previously-redacted-information-in-tiktok-inc-complaint-filing/

- Frances Haugen, in her testimony before the Senate Commerce Committee said, "I saw that Facebook repeatedly encountered conflicts between its own profits and our safety. Facebook consistently resolved those conflicts in favor of its own profits."[39]
- Sarah Wynn-Williams, said in her testimony before the Senate Commerce Committee, "During my time at Facebook, now Meta, Executive Officers, including the CEO and COO, frequently minimized, dismissed, or even outright denied the many harms that resulted from their platforms. As far as I could tell, they did this to justify their continued focus on growth, even when it seemed obvious to me and my peers on the Policy and Communications team that the company's growth strategies would worsen the harm caused by Meta's products."[40]
- Brian Boland, Meta's former vice president of partnerships who worked at the company for 11 years and resigned in 2020. "My feeling then and my feeling now is that they don't meaningfully care about user safety," he allegedly said. "It's not something that they spend a lot of time on. It's not something they think about. And I really think they don't care."[41]
- Instagram's former head of safety and well-being Vaishnavi Jayakumar testified that when she joined Meta in 2020 she was shocked to learn that the company had a "17x"

---

[39] Haugen, F. (2021, October 4). *Statement of Frances Haugen* [Written testimony before the U.S. Senate Committee on Commerce, Science, and Transportation, Subcommittee on Consumer Protection, Product Safety, and Data Security]. U.S. Senate Committee on Commerce, Science, and Transportation. https://www.commerce.senate.gov/services/files/FC8A558E-824E-4914-BEDB-3A7B1190BD49

[40] Wynn-Williams, S. (2025, April 9). *Responses to questions for the record* [Written responses submitted to the U.S. Senate Committee on the Judiciary]. U.S. Senate Committee on the Judiciary. https://www.judiciary.senate.gov/imo/media/doc/2025-04-09_qfr_responses_wynn-williams.pdf

[41] Spinks, R. (2025, November 22). *Court filings allege Meta downplayed risks to children and misled the public*. TIME. https://time.com/7336204/meta-lawsuit-files-child-safety/

strike policy for accounts that reportedly engaged in the "trafficking of humans for sex."[42]

Urgently Needed Federal Response

The clear record of both pervasive, severe harm suffered pursuant to adolescent social media use and the demonstrated conflict of interest between profit and safety inherent in today's social media industry justifies a significant federal public policy response. Every day without social media safety reform means more harmed children. That is why we are grateful that the Committee recognizes on a bipartisan basis that a broad approach with multiple tactics is needed: resources for education, accountability and rules for platforms, research, privacy reforms, and safety technology. America's families have waited years for effective social media safety reform; we need to get effective legislation passed and signed into law this Congress.

Sammy's Law (HR 2657)

The Organization for Social Media Safety has been closely involved in the development of Sammy's Law, as we believe it to enable a proven effective, durable solution in protecting adolescents from harms related to social media use. I thank the Committee for considering this bipartisan legislation and would like to detail why we support it.

---

[42] Spinks, R. (2025, November 22). *Court filings allege Meta downplayed risks to children and misled the public*. TIME. https://time.com/7336204/meta-lawsuit-files-child-safety/

Third Party Safety Software. Third-party safety software is an external tool, independent of the social media platforms themselves, that empowers parents to protect their children by, among other features, providing alerts when dangerous content is shared through a child's social media account. These alerts enable caregivers to intervene with life-saving support at the most critical moments. For example, if a child is targeted for severe cyberbullying through a social media post or message, safety software can detect that content and alert the parent, who can then immediately seek mental health assistance.

Because millions of families already employ third-party safety software for the social media platforms and operating systems that permit access, its effectiveness in protecting children is both well-documented and significant. Over the last several years, leading safety software companies have delivered hundreds of millions of alerts to parents, helping protect millions of children from serious harm, including sexual predation, suicides, severe cyberbullying, and trafficking.[43] Third-party safety software has averted a documented 16 school shootings.[44]

Sammy's Law will provide families full access to safety software. For third-party safety software to function, social media platforms must grant the safety software provider access to a child's social media account, via an Application Programming Interface (API), when authorized by a parent or guardian. An API is a set of technical instructions that, in this case, allows a parent-authorized safety software provider to securely access specific data from a child's social media account.

---

[43] Bark Technologies. (2024). *Bark's 2024 Annual Report on Children and Technology*. Bark. https://www.bark.us/annual-report-2024/?srsltid=AfmBOor-hzZQmrVMuIAoecP35eP4pY1_5CZZE_dmOBoxDq2MglMiSKCs

[44] Baig, E. (2019, February 19). Can artificial intelligence prevent the next Parkland shooting? USA Today (Online). https://www.usatoday.com/story/tech/2019/02/13/preventing-next-parkland-artificial-intelligence-may-help/2801369002/

While many social media platforms, like YouTube, Tumblr, X, and Reddit, do provide access, unfortunately, others used significantly by children, like Snapchat and TikTok, do not. This hesitation likely stems from business concerns that child users would avoid social media platforms that support safety software in favor of other less secure platforms. To protect children, parents and guardians must be empowered to choose whether third-party safety software is the best option for their children.

Third-party safety software fills critical safety gaps left by the parental safety tools already available directly on social media platforms. In-platform tools simply do not show efficacy in protecting children from the severe and pervasive range of social media-related harms.

- **Rudimentary Options:** While most major platforms offer some form of parental controls, these tools are often limited to basic time restrictions or crude content filters and frequently overlook the very places where children face the greatest dangers, like private messaging, group chats, and disappearing content. This leaves children vulnerable to a range of harms including human and drug trafficking, severe cyberbullying, and sexual predation.

- **Do Not Adapt to Evolving Threats:** Moreover, the platforms have little incentive to evolve their controls to keep pace with the ever-changing nature of social media-related threats. For example, in recent years, drug traffickers have used emoji-coded language to sell narcotics to teens. Third-party safety software companies responded

quickly updating algorithms to detect this new threat and alert parents in real time. Meanwhile, platforms like Snapchat took years to publicly acknowledge the problem, let alone act. And when they did, they said in an October 26, 2021, Senate Commerce Committee hearing, "We have employed proactive detection measures to get ahead of what the drug dealers are doing. They are constantly evading our tactics, not just on Snapchat but on every platform." (emphasis added)[45]

- **Children Can Bypass:** Most built-in tools can be turned off or bypassed by the child, undermining their effectiveness entirely.

- **Work Only on the Individual Platform:** The tools on each social media platform only work on *that particular* platform. Unfortunately, many severe social media-related threats today are *cross-platform.* For example, illicit drugs can be marketed on a platform like Instagram and then the transaction conducted on a platform like Snapchat. Or a child can encounter a predator on a platform like Roblox and then continue interacting with the predator more extensively on a platform like Discord. Siloed safety tools are substantially less effective at protecting children.

The evidence for the ineffectiveness of in-platform tools is clear in that parents do not utilize them despite an overwhelming parental desire for more effective safety options. According to Snapchat founder and CEO Evan Spiegel, there are 20 million teen users of Snapchat, but only

[45] U.S. Senate Committee on Commerce, Science, and Transportation. (2021, October). *Protecting Kids Online: Snapchat, TikTok, and YouTube*. https://www.commerce.senate.gov/2021/10/protecting-kids-online-snapchat-tiktok-and-youtube

200,000 parents have activated the platform's Family Center.[46] That's just 1% of families making use of Snapchat's safety features, underscoring how poorly suited and poorly adopted these measures are.

By contrast, third-party safety software providers are entirely mission-driven and accountable to parents, not advertisers. Their tools are designed to work across platforms, adapt rapidly to emerging harms, and empower parents to act before severe harm occurs. Most importantly, the protection provided is comprehensive, protecting a child from a full range of social media-related harms throughout the features, spaces, and nooks of the social media platform.

Sammy's Law would not only improve protection for children, it also would meaningfully increase children's privacy. Today, parents are becoming increasingly aware of the significant risk that social media poses to their children and seek to follow the recommendations of trusted professional experts, like the American Psychological Association, and provide responsible supervision of children's social media use.[47] Without comprehensive third-party safety software access, many parents must resort to manually reviewing children's devices, duplicating accounts, or relying on expansive surveillance tools. According to a November 2022 nationally representative Morning Consult survey ,79% of parents conduct manual reviews of their children's devices and social media accounts.[48] Unfortunately, not only are these methods far

---

[46] Malik, A. (2024, January 31). Snap CEO says 20 million US teens use Snapchat, but only 200,000 parents use its Family Center controls. TechCrunch. https://techcrunch.com/2024/01/31/snap-ceo-says-20-million-u-s-teens-use-snapchat-but-only-200000-parents-use-its-family-center-controls/

[47] American Psychological Association. (2023, May). *Health advisory on social media use in adolescence*. https://www.apa.org/topics/social-media-internet/health-advisory-adolescent-social-media-use

[48] Morning Consult. (2022, November). *Nationally representative survey of U.S. parents on social media safety* [Unpublished survey].

less effective than safety software at protecting children, but they are also incredibly invasive revealing private conversations and content not connected to any harm or risk. found that 84% of parents agree current methods are more intrusive than safety software and less effective.[49] By empowering parents with access to third-party safety software on the platforms their children use most, Sammy's Law offers a better solution: more targeted, less invasive, and proven to work.

Furthermore, Sammy's Law also strictly limits what safety software may share with parents. Under the bill, data may only be disclosed if it relates to a current or imminent risk of harm, including only listed harms, including suicide, cyberbullying, violence, sexual predation, and eating disorders. This protection, among other stringent safeguards in the bill, ensure children's privacy is strengthened while enabling parents to act against real threats.

The Committee Should Pass Sammy's Law Without Delay. Sammy's Law is uniquely positioned for near-term implementation: it protects children immediately, complements other proposals under consideration, and avoids many of the constitutional challenges that have delayed broader state-level reforms. Third-party safety software is an existing, proven solution to increase safety for young adult social media users; expanding its reach to all major social media platforms will provide immediate and substantial protection for millions of children, undoubtedly saving many lives. The status quo is simply unacceptable; parents and guardians need these tools immediately.

Conclusion

---

[49] Morning Consult. (2022, November). *Nationally representative survey of U.S. parents on social media safety* [Unpublished survey].

The Organization for Social Media Safety again thanks the Committee for holding this hearing and signaling its intent to pass critical social media safety legislation. We remain available to provide our insights and assistance in this generationally urgent effort to pass legislation that will protect America's children.

I look forward to answering your questions today.

Mr. BILIRAKIS. Thank you so very much.
Now I will recognize Mr. Lekas for his 5 minutes.
You are recognized, sir.

STATEMENT OF PAUL LEKAS

Mr. LEKAS. Chairman Bilirakis, Ranking Member Schakowsky, and members of the subcommittee, thank you for the opportunity to appear before you today.

My name is Paul Lekas, and I serve as executive vice president for the Software & Information Industry Association. SIIA represents nearly 400 organizations at the forefront of innovation, from startups to global leaders in AI, cloud computing, education, technology, and more.

Our mission is to support policies that foster a healthy information ecosystem. That cannot occur without responsible data use. We share the subcommittee's goal: making the internet a safer place for all. We appreciate that the subcommittee has taken a fresh look at how to achieve this. We are here to urge passage of bipartisan legislation that protects online youth privacy and safety.

It is exactly for this reason that we worked closely with industry and policymakers to develop our Child and Teen Privacy and Safety Principles in 2024. Many of the themes in the principles are reflected in provisions of the bills under consideration today. I would like to highlight a few of these.

First is data minimization. Companies must be required to minimize the collection of personal data from youth and restrict how that data is used. This is widely recognized as a best practice by privacy experts and is even more important in the youth context.

Second, we believe companies should not advertise to youth based on their online behavior, nor should they create profiles of youth for targeted advertising. Contextual advertising should remain permitted to ensure that youth receive age-appropriate content.

Third is empowerment and transparency. Legislation should incentivize companies to provide easy-to-use tools that allow families control over their settings and data. Transparency is key to building trust and helping families make informed decisions.

Finally, we need national consistency. The internet is not partitioned by State lines. The current patchwork of State regulations creates confusion for both platforms and consumers. A Federal law must be strong and preemptive to ensure all American children have the same high level of protection.

As Congress considers new legislation, a threshold is to strike the right balance between the Constitution's protection of free expression and the governmental interest in youth safety. Thus far, many online safety laws have failed to strike that balance.

Several States have proposed inherently content-based regulations, requiring platforms to judge speech as harmful or detrimental. These regulations trigger strict scrutiny, and courts have historically struck them down for being overbroad and infringing on the free expression of adults and minors, including content reflective of their own religious or political speech.

Recent case law provides a roadmap. The Supreme Court in 2025 confirmed that age verification is constitutional when targeting

sites with unprotected sexually explicit material. On the other hand, the Ninth Circuit in 2024 warned that broadly requiring platforms to assess the risk of harm can transform a design regulation into an unconstitutional content regulation.

Legislating in this area is possible but requires precision. There is much that is permissible: securing data, restricting certain features, leveraging nontechnical tools like digital literacy.

Vague duty-of-care models, like the Senate version of KOSA, that require filtering content based on subjective harm will invite and fail constitutional scrutiny. The version of KOSA before this subcommittee reflects a serious attempt to grapple with this challenge.

In addition to creating new tools, we support modernizing older ones, like COPPA. We support codifying recent FTC regulations and, crucially, strengthening the privacy protections at the intersection of COPPA and FERPA. We must ensure that when schools contract with vendors, student data is used solely for educational purposes and we are not overburdening our families.

We also urge Congress to avoid unintended consequences in two important but very different areas.

The first is age assurance. Mandating age verification requires collecting sensitive data, often government IDs, from all users, not just kids. We should instead incentivize age estimation and parental controls which protect youth without creating high-value data repositories for cyber criminals. We must also recognize that everyone in the ecosystem has a role to play.

The second involves the collection and use of third-party data. Many institutions rely on data about minors for essential services, like extending auto insurance to teen drivers,; helping youth to develop credit history; protecting minors from identify theft; college scholarships; financial aid; countering human trafficking—the list goes on. We should prevent actors from misusing youth data without disrupting vital, societally necessary practices.

Online safety and privacy for children and teens requires a holistic approach. There is no silver bullet. There is room for legislation, and we are pleased the subcommittee is considering an array of bills to identify the right mix.

I welcome your questions and look forward to continuing to work with you to advance legislation to keep youths safe while preserving the internet as a resource for learning and connection.

Thank you.

[The prepared statement of Mr. Lekas follows:]

Testimony before the Subcommittee on Commerce, Manufacturing, and Trade of the Committee on Energy and Commerce, U.S. House of Representatives

"Legislative Solutions to Protect Children and Teens Online"

December 2, 2025

Paul Lekas
Executive Vice President, Global Public Policy & Government Affairs
Software & Information Industry Association

I. Introduction

Thank you, Chairman Bilirakis, Ranking Member Schakowsky, and members of the Subcommittee, for the opportunity to appear before you today. My name is Paul Lekas, and I serve as Executive Vice President of Global Public Policy and Government Affairs for the Software & Information Industry Association (SIIA). SIIA shares the goals of this Subcommittee in making the internet a safer place for all. It is a privilege to join with you to urge Congress to pass bipartisan legislation to protect the privacy and safety of children and teens online.

SIIA represents nearly 400 organizations at the forefront of innovation in the United States around the world. For over forty years, we have advocated for the health of the information lifecycle, advancing favorable conditions for its creation, dissemination, and productive use. Our members range from start-up firms to some of the largest and most recognizable corporations in the world. They include the nation's leading publishers and innovative developers of digital products and services for K-20 education, global leaders in AI models and applications and in cloud computing, companies specializing in data analytics and information services, academic and scientific publishers, creators of legal research and financial databases, and the global financial information and market data community.

Whether in the workplace or the classroom, our members are dedicated to responsible data use. SIIA has made it a priority to work with industry to raise the bar on responsible practices. In addition to our *Child and Teen Privacy and Safety Principles*, discussed below, in the past two years we have collaborated with industry and policymakers to launch the *Principles for the Future of AI in Education*[1] and the *Data Stewardship Best Practices for Data and Analytics*

[1] SIIA, *Principles for the Future of AI in Education* (2023), available at https://edtechprinciples.com/wp-content/uploads/2023/11/Education-Technology-Industrys-Principles-for-the-Future-of-AI-in-Education-3.pdf; *see also* https://edtechprinciples.com/.

Companies.[2] These initiatives reflect industry's interest in promoting practices that advance the interests of those who rely on their services – students and educators, the financial markets and consumers – while taking care to protect individuals' privacy and data security and mitigate the risk of data and software misuse.

The pace of technological change surrounding the internet, and in particular the way that our kids and teens interact with that technology, has created new risks. The same technology that enables close contact with friends, for example, can exacerbate bullying. Thanks to the pressure from employees, families, children, advocates, and policymakers, companies are working to build guardrails and features into their products to address those risks and build a more robust and safe space for youth online.[3]

II. The Industry's Commitment: The SIIA Child and Teen Privacy and Safety Principles

In 2024, SIIA released our *Child and Teen Privacy and Safety Principles* calling on federal policymakers to pass legislation to keep kids safe and connected while holding technology companies accountable for doing just that.[4] Many of the themes in the principles are reflected in provisions of the bills under consideration today. Our principles seek to advance youth online privacy and safety through legislation that requires companies and other stakeholders to do the following:

Minimize collection and use of youth data. Companies must minimize the collection of personal data from children and teens and restrict the ways that data is used. Data minimization is widely recognized and required by many state privacy laws for processing data of children and teens. It is especially important for those populations because children and teens are generally more trusting and less aware of the risks related to sharing personal information.

Adopt tools that empower children, teens, and families. Companies should implement easy-to-use and easy-to-access tools that empower youth and families to maintain control of their data and mitigate potential online harms. Legislation can incentivize companies to provide these sorts of tools without engaging in content-based regulation.

Foster transparency. Families and youth should have access to clear information about how data is being used and the ability to control settings. The internet is a tool that families and youth can use to support learning and connection. Companies should provide information about privacy and safety provided to children, teens, and families in a manner that is concise, prominent, accessible, and use clear and plain language. Transparency is an essential mechanism to build trust and

---

[2] SIIA, *Data Stewardship Best Practices for Data and Analytics Companies* (2025), available at https://www.siia.net/wp-content/uploads/2025/06/Best-Practices-in-Data-Stewardship-for-Data-and-Analytics-Companies.pdf; *see also* https://www.siia.net/data-stewardship-best-practices/.

[3] This testimony uses the term "youth" to cover both children (under 13 years of age) and teens (under 18 years of age).

[4] SIIA, *Child and Teen Privacy and Safety Principles* (2024), available at https://www.siia.net/wp-content/uploads/2024/03/SIIA-Child-Privacy-and-Safety-Principles-.pdf.

demystify what can seem a complicated online landscape. Many state laws require transparency for online services. The goal is to ensure parents and youth can make informed decisions about their activities online.

Restrict advertising. Companies should not advertise to youth based on their online behavior or activity and should not create profiles of youth for the purpose of targeted advertising. Companies should be permitted to serve contextual ads; this is important to ensure that children are being served age-appropriate and location-appropriate content.

Protect personal information. Protecting user data, especially the data of children and teens, is a central tenet of the principles. Companies should implement strong security safeguards appropriate to the level of personal information that may be collected, used, or shared.

Enable access to educational material. The internet is a part of children's lives. News, educational materials, information about sports and hobbies as well as other entertainment can be online. Youth should be afforded access to information online without the threat that companies will over-moderate and prevent access to useful, legal content.

Support K-12 media and digital literacy. Legislation and new policies must be accompanied by support for resources in K-12 schools to implement programs for media and digital literacy. Children and teens are growing up in a digital world, and it is critical that we prepare them to be responsible digital citizens. Platforms should also support those digital literacy efforts.

Require risk assessments. Written risk-based impact assessments keep companies accountable for their practices. Several existing legal regimes already require these assessments, and a federal requirement should align with existing regimes and encourage adoption of best practices in risk-based evaluation and assessment preparation.

Empower enforcement. Effective enforcement requires clarity about which government agencies at the federal or state level have enforcement authority and should be designed to improve privacy and safety practices. Enforcement should not be watered down with private rights of action that can lead to frivolous, excessive lawsuits based on mere statutory violations. For example, enforcement under Unfair and Deceptive Acts and Practices laws provide clear paths for enforcement action without providing private rights of action that create cottage industries of litigation.

Provide consistent rules across the U.S. Federal law should be strong, preemptive, and provide the same protections to all children and teens across the U.S. The emerging patchwork regulations create confusion among both platforms and consumers. They also create gaps, because the internet is not cleanly partitioned along state lines. A national framework would allow companies to put consistent programs in place.

III. Specific Legislative Issues

SIIA appreciates the thoughtful approach that the Subcommittee has taken for today's hearing, recognizing that there is no single solution to the concerns that have been raised involving youth privacy and safety. Our goal is to ensure kids remain safe online and retain access to information and the virtual tools critical in keeping them connected in their communities. Families must also be empowered to decide what is best for their own family online and to teach kids and teens best practices for protecting themselves while navigating the internet. And companies should be encouraged to be proactive in addressing challenges faced on their platforms, apps, or websites in a manner that recognizes the need for context-specific solutions and the varying risk profiles that each corner of the internet presents.

In short, we support efforts to pass laws that improve youth privacy and safety. Many provisions in today's legislative package achieve that. As the Subcommittee considers these bills in greater detail, we urge members to take care to avoid unintended consequences and to advance legislation that meaningfully addresses the challenge at hand.

We are providing preliminary input to key issues raised by the legislation under consideration in this hearing. As the Subcommittee refines these bills, we look forward to continuing to work with all members.

First Amendment and Free Expression

SIIA recognizes youth safety as one of the most important of government interests. At the same time, there are other values that must be balanced against the desire to protect kids online: most notably those involving free speech. The First Amendment requires that Congress calibrate its desire to legislate comprehensive youth online safety measures against the need to foster protected speech.

That is a difficult, but not impossible balance. Most online safety laws are inherently content-based regulations—they require private businesses to make decisions about speech based on its subject matter (e.g., whether it is "harmful" or "detrimental" to minors), thus triggering strict scrutiny from the courts. While the government's interest in protecting children is compelling, courts have historically struck down federal efforts, like the Child Online Protection Act (COPA), because they were overbroad, restricting a substantial amount of constitutionally protected adult speech to shield minors.[5] This scrutiny forces Congress toward less restrictive means, such as regulating design or privacy conduct, rather than content.

This already challenging landscape has been both clarified and complicated by recent judicial decisions. The Supreme Court's 2025 decision in *Free Speech Coalition v. Paxton*[6] provides a

[5] *See Ashcroft v. Am. Civil Liberties Union*, 542 U.S. 656 (2004) (holding COPA unconstitutional); *Reno v. Am. Civil Liberties Union*, 521 U.S. 844 (1997) (holding portions of the Communications Decency Act unconstitutional).

[6] *Free Speech Coalition, Inc. v. Paxton,* 606 U.S. ___ (2025), available at https://www.supremecourt.gov/opinions/24pdf/23-1122_3e04.pdf.

narrow pathway for federal regulation by upholding Texas's age-verification requirement for commercial sites hosting unprotected, sexually explicit material, essentially confirming that regulation targeting content *unprotected as to minors* may withstand intermediate scrutiny. However, the logic of this decision is unlikely to extend to general-purpose social media platforms containing vast amounts of protected, non-sexual speech.

Conversely, the Ninth Circuit's 2024 decision in *NetChoice v. Bonta*[7] (regarding the California AADC) is a major constraint on federal legislation aimed at platform design. The court found that requiring platforms to assess and mitigate the risk of "harm" to children transforms a design regulation into a content regulation, subject to strict scrutiny and thus likely unconstitutional. It found that California had less restrictive means to achieve its goals – for example, incentivizing companies to offer content filters, educating children and families, and enforcing existing criminal laws. The Ninth Circuit also highlighted concerns raised by the ACLU that vague and expansive language would likely prevent youth from accessing content such as mental health resources, information about school shootings, and content reflective of minors' own religious or political speech.

A divided three-judge panel of the Eleventh Circuit recently issued an opinion that *may* provide additional guidance to lawmakers but is still the subject of active litigation.[8] In a 2-1 decision, the panel stayed a preliminary injunction that prevented Florida from enforcing a law that would prohibit users under the age of 14 maintaining or creating accounts on social media platforms and permit users aged 14 or 15 to maintain accounts only with parental consent. The majority held that by targeting platforms with "addictive features," the law was content neutral and subject to intermediate scrutiny.

In a vigorous dissent, Judge Rosenbaum argued that the Florida law "is not just 'likely' unconstitutional; it's plainly unconstitutional on its face." He described how the law "directly regulates both expressive activity itself and conduct with an expressive element," and noted–with some force–that the prohibitions not only impermissibly allow the state to control the ideas that minors can access but prohibit parents from exposing them to those ideas. In that circumstance, he found the burden on the speech rights of both minors and adults to far outweigh the government's interest under either strict or intermediate scrutiny. We think the dissent has the better of this argument, as this case remains a minority position and would caution the Subcommittee against putting too much weight on it. That said, if the panel majority's position holds, it will support the view that legislation addressing content-neutral design features rather than content itself stands on stronger constitutional footing.[9]

These decisions provide important guidance to Congress as it develops legislation to address a range of issues involving youth online privacy and safety. Legislation such as the Senate version of the Kids Online Safety Act (KOSA), which would impose a vague, expansive "duty of care"

---

[7] *NetChoice, LLC v. Bonta*, No. 23-2969 (9th Cir. Aug 16, 2024), available at https://netchoice.org/wp-content/uploads/2024/08/Ninth-Circuit-Ruling_NetChoice-v.-Bonta.pdf.

[8] *Comp. & Comm. Indus. Assoc. v. Uthmeier*, No. 25-11881 (11th Cir. Nov. 25, 2025).

[9] SIIA filed an amicus brief with the Ninth Circuit supporting the appellee in this matter.

that requires platforms to filter content based on subjective harm, would be likely to run afoul of the First Amendment.

We are encouraged that several bills the Subcommittee is considering have taken to heart the fundamental tension between free expression and the interests of youth online privacy and safety. We encourage the Subcommittee to see the evolving case law in this area not as an impediment but as a roadmap to identify legislative solutions that address legitimate concerns about online safety and privacy while also adhering to core American values. Legislation should avoid broad measures that amount to content filtering while focusing on ways to regulate non-expressive conduct, narrowly target explicit sexual content, incentivize companies to address gaps in their privacy and safety protocol, and leverage non-technical tools such as consumer education and criminal laws.

Modernizing COPPA

The Children's Online Privacy Protection Act of 1998 (COPPA) has served as a critical baseline for protecting the personal information of children, defined in COPPA as people under the age of 13. Most important is COPPA's requirement that operators obtain verifiable parental consent prior to collecting information from a child unless the information is used for internal operations. The FTC administers COPPA and earlier this year issued long-awaited amendments to regulations.

The new FTC regulations,[10] approved by the Commission on a bipartisan basis, represent the latest iteration of an ongoing effort to modernize COPPA. Among other things, the new regulations recognize the need to make verifiable parental consent reflective of modern technologies. Whereas a signed consent form sent in via fax was appropriate two decades ago, the FTC approved newer methods like a knowledge-based authentication process or the use of facial recognition technologies. The FTC has also updated the definition of personal information to include biometric identifiers and government-issued identifiers, reflecting the variety of information on children that could be collected online.

In recent years, the FTC has focused on COPPA enforcement. This year alone, the FTC has settled a number of matters involving alleged COPPA violations based on enabling a third party in China to collect geolocation information about American children without parental consent,[11]

[10] 16 CFR Part 312, available at https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312.

[11] FTC, Online docket for *United States v. Apitor Tech. Co., Ltd.* (Oct. 1, 2025), available at https://www.ftc.gov/legal-library/browse/cases-proceedings/apitor.

unlawfully collecting information from children,[12] and deceiving children about the real costs of in-game transactions.[13]

We believe there are further updates that can be made to bring COPPA into the 21st century, including codifying recent updates into statute. Such updates include aligning to the regulatory requirements and industry best practices of data minimization and ensuring that platforms only gather data essential to preserving child safety. Under the current law, companies may engage in targeted advertising, among other things, with parental consent. As reflected in the SIIA Principles, we believe targeted advertising – as opposed to contextual advertising – should not be allowed for youth.

Perhaps most important, given our longstanding work with the educational community, we believe COPPA needs to be updated to reflect a conflict with the Family Educational Rights and Privacy Act (FERPA). There has long been a lack of clear line between FERPA and COPPA despite overlapping requirements. When a school contracts with an operator, the operator should not be able to use student information for any purpose other than for the educational purpose for which it was disclosed. This educational purpose limitation is required by FERPA but not COPPA. Clarifying this by statute would strictly limit operators' use of personal information. The updates in COPPA 2.0 clarify that educational data may only be used for educational purposes when technology is used at the direction of the school.

Age Assurance Methods

Age assurance covers a variety of methods used to determine a user's age or age range online, encompassing age verification, age estimation, and age declaration. Across the spectrum there are additional approaches that can be adopted – for example, requiring parental consent, estimating age with facial recognition technology or machine-learning models, or using government-issued identification. The choice of method depends on the required level of confidence, privacy concerns, cybersecurity risk, the risk associated with the content or service, technological availability, and other factors such as access and accessibility. Each method inevitably involves tradeoffs of important policy goals.

A principal challenge associated with more precise age assurance methods, such as age verification, is that they require gathering data from *all* users – not just those who fall within an age range or below an age threshold.[14] That collection creates outsized security risks and works

[12] FTC, Online docket for *United States v. Iconic Hearts Holdings, Inc.* (Sept. 29, 2025), available at https://www.ftc.gov/legal-library/browse/cases-proceedings/232-3029-iconic-hearts-holdings-inc-us-v; FTC, Online docket for *United States v. Disney Worldwide Servcs., Inc.* (Sept. 2, 2025), available at https://www.ftc.gov/legal-library/browse/cases-proceedings/disney.

[13] FTC, Online docket for *United States v. Cognosphere, LLC* (Jan. 17, 2025), available at https://www.ftc.gov/legal-library/browse/cases-proceedings/222-3152-cognosphere-llc-us-v.

[14] A recent study by the Center for Democracy and Technology (CDT) found that while "[t]he majority of participants were not against the concept of online age verification…when discussed in more detail and in practical terms, most conversations pertaining to the widespread implementation of age verification raised concerns - including concerns about privacy, security of collected and stored data, their limited trust in

against privacy best practices around data minimization. Age verification requires robust data collection, making it exceedingly difficult to minimize the sensitive data collected from youth users. Websites or platforms holding a rich array of sensitive data are more attractive targets for malicious actors, dramatically increasing the likelihood that a data breach will harm young people. Requiring technology companies to gather and store that information creates the opportunity for bad actors to attack and access that information. This vulnerability is more pronounced for small- and medium-sized companies that may have less robust tools and resources than larger firms.

The most significant privacy and cybersecurity risk associated with robust age verification methods—particularly those requiring the submission of government-issued identification or biometric scans—is the potential for mass data breaches and the creation of centralized identity dossiers. When platforms or their third-party vendors collect and store highly sensitive PII to prove age, this data becomes a high-value target for cybercriminals, raising the risk of identity theft, phishing, and blackmail for all users who comply. Recently, for example, a breach of a third-party service provider used by Discord to perform age verification led to the exposure of 70,000 government-issued IDs.[15]

Furthermore, as discussed by the dissent in the *Uthmeier* case, mandating verification systems fundamentally undermines anonymity and can lead to surveillance creep, as the act of linking a verified identity to online activity transforms the internet experience into a less private space, potentially chilling the protected speech of both adults and minors who value their right to anonymous expression.[16]

Several other age assurance technologies exist that significantly minimize these privacy and cybersecurity risks. For example, age estimation, which uses machine learning to predict a user's age range based on non-identifiable facial characteristics or aggregated behavioral data, is a far less invasive method. While less certain than verification and prone to bias (especially for certain demographics), it could be suitable for low-risk contexts and for triggering a higher level of

---

platforms, and the lack of user agency - all of which left participants uneasy." Michal Luria and Aliya Bhatia, "What Parents Want: Policy Insights for Social Media Safety Features," CDT (Nov. 2025), at 11, available at https://cdt.org/wp-content/uploads/2025/11/2025-11-24-CDT-Research-Social-Media-Report-final-1.pdf.

[15] Discord, "Update on a Security Incident Involving Third-Party Customer Service" (Oct. 9, 2025), available at https://discord.com/press-releases/update-on-security-incident-involving-third-party-customer-service.

[16] *See, e.g.*, Alice Marwick, et al., *Child Online Safety Legislation: A Primer*, Princeton Center for Information Technology Policy, Duke Sanford School of Public Policy, UNC Center for Information Technology, and Public Life (2024), available at https://assets.pubpub.org/bujb2qf1/COSL-06.04-11717506843758.pdf; Shoshanna Weissman, "Current age-verification methods threaten our First Amendment rights beyond anonymity," R Street Institute (June 22, 2023), available at https://www.rstreet.org/commentary/current-age-verification-methods-threaten-our-first-amendment-rights-beyond-anonymity/; Sara Forland, et al., "Age Verification: The Complicated Effort to Protect Youth Online, New America Open Technology Institute" (Apr. 23, 2024), available at https://www.newamerica.org/oti/reports/age-verification-the-complicated-effort-to-protect-youth-online/.

scrutiny only when a user's age is uncertain. At the same time, it does not create the same privacy risks as using hard identity documents.

Following the Supreme Court's opinion in *Paxton*, age verification requirements are appropriate for websites with a significant amount of sexually explicit material. Half the states have laws that require verification to access sites with one-third sexually explicit material. Outside of that context, however, legislation that requires age verification is likely to raise First Amendment challenges on behalf of adult users who believe such requirements limit their ability to access legal content. Congress would need to establish that the age assurance method required serves a compelling government interest and is the least restrictive means of advancing that interest.

Congress should look to different methods to incentivize the creation of more age-appropriate experiences and protect young people online. Creating tools that empower parents and youth with control over their data and their online experience, using signals to estimate ages and trigger additional guardrails based on company policies, and creating parental monitoring tools can help to limit young people's exposure to harmful content and interactions.[17]

Parental Controls

Parental controls are an essential part of youth online safety and privacy. We believe it is important to empower families as well as youth to manage their online safety and privacy. Every family is different, as are families' views on what content and experiences are appropriate for youth in the online world.

While we support strong privacy standards and giving families tools to exercise appropriate oversight over their children, there are inevitable challenges. One challenge is age-old: children and teens are smart and resourceful, and the ability to implement controls requires being aware of how they can circumvent these controls. This is a challenge that is hard to address through legislation as opposed to education and improving communication within a family.

Making tools for controlling security and safety features easier for parents to access, understand, and use, as well as fostering digital literacy among parents and youth is also important. Creating effective tools and enabling by default is a good start, and ensures that the environment is set up as best it can be from the start, but we also want parents to be able to exercise their own agency based on their own judgment about what's best for their children, and making sure they understand and can use the tools is essential to that work.

[17] *See, e.g.*, Shane Tews, "Age Verification Laws vs. Parental Controls: Why the Legislatures, Courts, and Tech Aren't on the Same Page," American Enterprise Inst. (Feb. 5, 2025), available at https://www.aei.org/technology-and-innovation/age-verification-laws-vs-parental-controls-why-the-legislatures-courts-and-tech-arent-on-the-same-page/; Amanda Reid, et al., "Nerd Harder: A Typology of Techno-Legal Solutionist Logics in Child Online Safety Laws," *Policy & Internet* (Sept. 2025), available at https://onlinelibrary.wiley.com/doi/epdf/10.1002/poi3.70012.

Legislation can set and enforce standards, both for the tools themselves and for the information made available by platforms to parents. It can also leverage social resources to ensure that parents are provided with information in their communities.

Emerging Trends and AI Chatbots

As lawmakers consider risks associated with emerging technologies such as AI chatbots, we recommend a focus on clear, evidence-based, and risk-proportionate requirements rather than broad restrictions that could unintentionally limit access to beneficial technologies including educational tools, accessibility features, or other creative learning and age-appropriate content.

Building on the SIIA's existing principles on children and teen privacy and safety, we have been working closely with our members to develop a comprehensive set of AI chatbot principles, the *SIIA CHAT SAFE Principles*, that simultaneously encourages the development of emerging AI tools while protecting the privacy, safety and security of all Americans. These principles outline guidance for clear disclosures, harm mitigation, accountability, trust and reliability, security and privacy, and adaptability.

Extensive legal frameworks exist in regulated spaces. Developers building tools for use in these spaces and deployers implementing tools in these spaces should ensure that tools align with the goals of CHAT SAFE as well as other privacy, safety, security, and civil rights requirements.

As Congress considers legislation in this space, we encourage policymakers to align with this balanced framework that supports innovation and encourages meaningful protections for children and teens.

Third Party Data Collection and Use

The use of data by third parties has also raised attention. As the Subcommittee considers potential restrictions on third-party data collection and use, we would urge members to consider the possibility for unintended consequences. Data providers come in many stripes and in addition to those data brokers who may engage in practices that undermine youth privacy and safety, many providers engage in responsible practices that both maintain data security and further the interests of youth and are in fact essential to their wellbeing.

SIIA has adopted principles for responsible data use earlier this year: *Data Stewardship Best Practices for Data and Analytics Companies*.[18] Currently, some SIIA members enable the limited, but mission-critical use of minors' data by a range of institutions – colleges and universities, insurance companies, financial institutions, government agencies, foundations, and non-governmental organizations (NGOs) – that rely on that data to provide services that minors and their families rely on. Those include:

[18] SIIA, *Data Stewardship Best Practices for Data and Analytics Companies* (2025), available at https://www.siia.net/wp-content/uploads/2025/06/Best-Practices-in-Data-Stewardship-for-Data-and-Analytics-Companies.pdf; *see also* https://www.siia.net/data-stewardship-best-practices/.

- Extending auto insurance for teen drivers;
- Building minors' credit history;
- Targeting colleges' recruitment efforts to underserved student communities;
- Protecting minors against identity theft and fraud;
- Identifying candidates for scholarships
- Providing financial aid for college;
- Assisting in military recruitment;
- Suppressing the data of minors who are children of judges and law enforcement officials protected by *Daniel's Law*-style legislation;
- Maintaining data and whitelists to enable age verification where required; and
- Tracking exploitation of minors in connection with human trafficking efforts by NGOs and financial institutions.

We do not believe that it is the intent of the Subcommittee to disrupt these kinds of everyday activities. This list demonstrates, however, that too broad of a legislative brush will prevent valuable uses of this data that many people rely on and take for granted. Successful legislation in this sphere will both target "black hat" data brokers and preserve the essential uses that society relies on. We encourage the Subcommittee to use the best practices we developed as a tool to guide policymaking: raising the bar for industry by identifying the characteristics of responsible data providers, and enabling the pro-social data uses described above.

IV. Conclusion

Building a safer, healthier, and more useful internet for youth and families requires everybody's input and all of us to work together. Our members have taken important steps to provide better resources and tools for parents and improve protections for youth safety and privacy. We support legislation that will help to make the internet safer while avoiding unintended consequences by erecting barriers that expose sensitive data, restricting access to content that ignores children's curiosity and ability to work around safeguards, and encouraging youth to seek out darker, harder-to-regulate spaces.

We hear those who have concerns about the impact of technology on today's youth. But we believe the approach must be holistic. Child abuse, CSAM, bullying, and eating disorders existed long before social media. These are old problems with complicated causes. We believe there is a role for government to play and there is more that industry can be doing. There is also a need to focus on non-technical solutions. Education, community building, and support for families are part of that equation. Our kids should be safe. They should be safe in schools and at home. They should be safe in youth sports and in their houses of worship. And they should be safe on the

internet. Developing these environments requires all of us to work together on solutions that acknowledge the constant changes in these problems. There are no silver bullets.

The SIIA *Child and Teen Privacy and Safety Principles* demonstrate industry's readiness to act, and eagerness for Congress to pass legislation designed to advance these goals. We stand ready to work with the Subcommittee to turn these principles into law and provide our best counsel as the Subcommittee considers the legislation assembled today.

Mr. BILIRAKIS. Thank you, Mr. Lekas.

Now I recognize Ms. Ruane for your 5 minutes. You are recognized.

STATEMENT OF KATE RUANE

Ms. RUANE. Thank you so much.

Thank you, Chair Bilirakis, Ranking Member Schakowsky, Chair Guthrie, and Ranking Member Pallone, for the opportunity to testify today.

I am Kate Ruane, director of the Free Expression Project at the Center for Democracy & Technology.

Children will use online services for their entire lives. The subcommittee is right to focus on their future.

I would like to raise five points essential to protecting children online.

First, Congress should address root causes of online harms, including privacy. Comprehensive consumer data privacy legislation is the best way to protect everyone online.

Currently, many online services' business models are based on advertising sales powered by platforms' collection, use, and sale of personal information. This is harmful because it is privacy invasive, increasing the risks of data breaches. It is also deficient because it ignores better signals of what users value about online services by conflating engagement with user preference.

Congress could realign this business model to benefit everyone through comprehensive privacy legislation.

Enhancing children's privacy protections is also a laudable goal. Measures like COPPA 2.0 and Don't Sell Kids' Data Act, crafted properly, would address some of the root causes of harm to kids online.

But the bills under consideration today put the FTC in charge of enforcement. At the same time, the current administration is undermining its independence and ability to enforce the law fairly.

As the committee considers how to protect kids, it must also ensure that the FTC executes its policies to protect all children and support the rule of law.

Second, protecting children includes protecting their right to express themselves online. Minors use social media for everything, including to access news, communicate with family and friends, do their schoolwork, and create art.

Children have First Amendment rights, and as Justice Scalia wrote, "Only in relatively narrow and well-defined circumstances may the government bar public dissemination of protected materials to them."

We are encouraged that today's Kids Online Safety Act narrows the overly broad duty of care in an attempt to grapple with the tension between ensuring safety and protecting free expression. This is a difficult balance to strike, but it is preferable to flatly banning minors from accessing critical speech services like social media. We hope to work with the committee as the bill moves forward.

Third, age assurance creates significant privacy risks that should be mitigated in legislation. Age verification and assurance raise significant concerns for all users' rights. To name just two, age-assurance techniques mean either more collection or more processing

of sensitive data, leading to increased risks of data breaches which could include people's IDs or biometric information. Age assurance also chills online engagement with sensitive topics that people want to keep private.

These concerns are not theoretical. Researchers at Georgia Tech have a forthcoming study demonstrating that the privacy and security concerns related to the use of age-assurance techniques are playing out in realtime, with increased risks for end users.

If Congress nevertheless feels obligated to impose age-assurance requirements, it should mitigate the risks by requiring the highest levels of privacy guardrails, including data minimization, deletion, reliance on high-quality data transparency and accountability.

Fourth, creating good policy requires taking into account the perspectives of minors and their caregivers. CDT has conducted research asking a sample of teens and their parents about features of current child safety proposals.

To give just two salient examples of their views: First, parents and teens expressed safety and privacy concerns with subjecting minors to age-assurance methods, preferring parent-centered approaches that enable parents to declare their children's age.

Second, we found that teens preferred algorithmic recommendations. Teens trust these feeds precisely because they feel that they are in control of that content.

Knowing what parents and minors want and how they currently navigate their online lives will improve policymaking at both companies and in legislatures.

Finally, Congress must not unduly restrict States' ability to act. Many of the bills at issue today would preempt State laws and regulations that simply relate to the provisions in the bills. We are concerned that the "relates to" standard will broadly preempt many existing State laws and emerging legislation that provide significant protections to children online, even if State law would provide better protections for kids.

To make matters worse, public reporting indicates that Congress may be negotiating a deal to pair a kids' safety package with the controversial provision preempting State laws on artificial intelligence. It would be ill-advised to broadly preempt States' ability to enact laws related to AI's impact without putting in place strong Federal protections at least equal in scope to any such preemption.

Thank you for the opportunity to testify, and I look forward to your questions.1A[1]

Mr. BILIRAKIS. Thank you very much. We appreciate that.

Now I will recognize Mr. Thayer for your 5 minutes.

STATEMENT OF JOEL THAYER

Mr. THAYER. Chairman Bilirakis, Ranking Member Schakowsky, and members of this esteemed committee, thank you for holding this incredibly important hearing to advance legislative solutions that ensures the health and safety of kids online.

[1] Ms. Ruane's prepared statement has been retained in committee files and is available at https://docs.house.gov/meetings/IF/IF17/20251202/118714/HHRG-119-IF17-Wstate-RuaneK-20251202.pdf.

I am Joel Thayer. I am a practicing attorney, and I sit as president of the Digital Progress Institute, a think tank dedicated to finding bipartisan solutions in the tech and telecom policy spaces.

Finding political consensus on incremental solutions to today's acute concerns in tech policy is at the core of our advocacy. Indeed, some of the bills before you today are based off of frameworks we helped develop.

This hearing, coupled with its bevy of bills, makes a few things abundantly clear.

First, we care about our children and their wellbeing, on and off their devices.

Second, we are no longer satisfied with the status quo.

In so many ways, today's youth are robbed of their innocence far more easily than ever before. This is thanks to the ubiquity of mobile devices and the services they host. Large tech platforms are inundating kids with lewd and lascivious exhibitions and even connecting them to child predators. This is well-documented. Senator Marsha Blackburn even went as far as describing Instagram as the "premier sex-trafficking site in this country."

Despite what the tech companies trumpet in their press releases, parents are left with almost no resources to combat their encroachments.

Worse, tech companies are, in fact, perpetuating the problem. Herein lies the rub. Big Tech's form of child exploitation pays very well. Our children are not only Big Tech's users but are also their product. Meta specifically targets young users and even places a monetary value of $270 on each child's head.

But the issue is worse still. Children are not only feeding Big Tech algorithms to sell to advertisers but are also used to inform their respective AI programs—AI programs like chatbots that have already resulted in some child deaths by encouraging kids to commit suicide.

At DPI, we are all for winning the AI war, but we do not believe children should serve as its casualties. It is why measures you are considering today are so essential to both ensuring that we remain dominant in the AI race and we protect our most vulnerable: our children.

However, we cannot ignore the long road ahead to get these passed. Big Tech's lobby is not only fierce but also unrelenting. They mire the validities of these solutions by instilling fears of consumers forfeiting privacy and the stifling of speech. But this is all a farce.

As to privacy, I say consider the source. Courts, regulators, and consumers have found every one of these companies to have violated their users' personal privacy.

Take Apple, for instance, that proclaims your privacy is a "fundamental human right." Discovery from a class action lawsuit, however, reveals that since October 2011 Apple had routinely recorded users' private conversations without their consent and disclosed those conversations to third parties, such as advertisers. Some of these disclosures included private conversations with their doctors. So much for privacy being a human right.

One of Google's privacy violations was so egregious that the Federal Trade Commission created a first-of-its-kind settlement requir-

ing Google to implement a comprehensive privacy program that it unbelievably didn't already have.

Social media companies do not fare much better. Again, an FTC report found that social media companies like Snap, Meta, and TikTok have all engaged in vast surveillance of users, with lax privacy controls and inadequate safeguards for kids and teens. Point being, these companies are hardly an authority on proper privacy hygienics.

As to free speech, I stand on the shoulders of Third Circuit Judge Paul Matey, who poignantly stated that Big Tech "smuggles constitutional conceptions of a 'free trade in ideas' into a digital cauldron of illicit loves that leap and boil with no oversight, no accountability, and no remedy."

And it is true. Big Tech has leveraged the admittedly messy First Amendment jurisprudence to turn our bulwark for free expression into a sword to cut down laws they frankly don't like.

But here is the good news. The Supreme Court has created a clear pathway for these measures. To start, in *TikTok* v. *Garland*, the Supreme Court categorically rejected TikTok's argument that the mere regulation of an algorithm raises First Amendment scrutiny. Even better, the Court clarified that a law regulating a tech platform doesn't invite First Amendment review if the law's primary justification is not content-based, even if its ancillary justifications are.

In sum, the bills before us today, particularly the App Store Accountability Act, the SCREEN Act, and the Kids Online Safety Act, have taken these considerations into account and are poised to resolve many of the challenges parents are facing in today's digital age with respect to child safety.

With that, I appreciate the committee's time for inviting me to testify, and I look forward to all of your questions and working with you further.

[The prepared statement of Mr. Thayer follows:]

Testimony of
Joel Thayer
President
The Digital Progress Institute

Before the

Subcommittee on Commerce, Manufacturing, and Trade
Energy and Commerce Committee
United States House of Representatives

Hearing titled

"Legislative Solutions to Protect Children and Teens Online"

December 2, 2025

Chairman Bilirakis, Ranking Member Schakowsky, Chairman Guthrie, Ranking Member Pallone, and members of this esteemed committee, thank you for holding this incredibly important hearing to advance legislative solutions that ensures the health and safety of kids online. I am Joel Thayer. I am a practicing attorney and sit as President of the Digital Progress Institute—a think tank dedicated to finding bipartisan solutions in the tech and telecom policy spaces. Finding political consensus on incremental solutions to today's acute concerns in tech policy is at the core of our advocacy. Indeed, some of the bills before you today are based off frameworks we helped develop.

This hearing coupled with its bevy of bills makes a few things abundantly clear. First, we care about our children and their well-being on and off their devices. Second, we are no longer satisfied with the status quo. In so many ways, today's youth are robbed of their innocence far more easily than ever before. This is thanks to the ubiquity of mobile devices and the services

they host. Large tech platforms are inundating kids with lude and lascivious exhibitions and even connecting them to child predators. This is well documented. Senator Marsha Blackburn even went as far as describing Instagram as the "premier sex trafficking site in this country."[1]

Despite what the tech companies trumpet in their press releases, parents are left with almost no resources to combat their encroachments. Worse, tech companies are, indeed, perpetuating the problem.

Herein lies the rub.

Quite frankly, Big Tech's form of child exploitation pays well. As we all know, our children are not only Big Tech's users but are also their product. Meta specifically targets young users and even places a monetary value of $270 on each child's life.[2] But the issue is worse still; children are not only feeding Big Tech's algorithms to sell to advertisers but are also used to inform their respective AI programs. Programs, like chatbots, have already resulted in some child deaths by encouraging kids to commit suicide.[3] At DPI, we are all for winning the AI war, but we do not believe children should serve as its casualties.

It is why the measures you are considering today are so essential to both ensuring that we remain dominant in the AI race and we protect our most vulnerable populations—children and teens.

---

[1] NBC News, *'That's Ridiculous': Zuckerberg Pushes Back on Meta Sex Trafficking Accusation*, Website (Jan 31, 2024), https://www.nbcnews.com/video/-that-s-ridiculous-zuckerberg-pushes-back-on-meta-sex-trafficking-accusation-203337797724.

[2] Heritage Foundation, X @Heritage (Jan 31, 2024), https://x.com/Heritage/status/1752767189663240548.

[3] Angela Yang, Laura Jarrett, & Fallon Gallagher, *The Family of Teenager Who Died By Suicide Alleges OpenAI's ChatGPT is to Blame*, NBC News (Aug. 26, 2025), https://www.nbcnews.com/tech/tech-news/family-teenager-died-suicide-alleges-openais-chatgpt-blame-rcna226147.

However, we cannot ignore the long road ahead to get these passed. Big Tech's lobby is not only fierce but also unrelenting. They mire the validities of these solutions by instilling fears of consumers forfeiting privacy and the stifling of speech. But this is all a farse.

As to privacy, I say consider the source. Indeed, courts, regulators, and consumers have found every one of these companies to have violated their users' personal privacy. Take Apple, for instance, that proclaims your privacy is "a fundamental human right."[4] Discovery from a class-action lawsuit reveals that, since October 2011, Apple had "routinely recorded their private conversations after consumers activated its Siri unintentionally, and disclosed these conversations to third parties such as advertisers."[5] Some of these disclosures included private conversations with their doctors.[6] So much for privacy being a "human right."

Google is even worse. In fact, one of Google's privacy violations was so egregious that the Federal Trade Commission (FTC) created a first-of-its-kind settlement, requiring Google "to implement a comprehensive privacy program" that it unbelievably didn't already have.[7]

Social media companies do not fare much better. An FTC report found that social media companies, like Snap, Meta, and TikTok, have "engaged in vast surveillance of users with lax privacy controls and inadequate safeguards for kids and teens."[8]

---

[4] Apple, *Privacy*, Website (last visited Dec. 2, 2025), https://www.apple.com/privacy/#:~:text=Privacy%20is%20a%20fundamental%20human,and%20services%20to%20protect%20it.

[5] Jonathan Stempel, *Apple Must Face Siri Voice Assistant Privacy Lawsuit -U.S. Judge*, Reuters (Sep. 2, 2021), https://www reuters.com/technology/apple-must-face-siri-voice-assistant-privacy-lawsuit-us-judge-2021-09-02/.

[6] *Id.*

[7] Rachel Courtland, *Google Agrees to 20 Years of Privacy Audits*, IEEE Spectrum (Mar. 20, 2011), https://spectrum.ieee.org/google-agrees-to-20-years-of-privacy-audits#:~:text=The%20FTC%20says%20this%20is,privacy%20of%20consumers'%20information%22..

[8] F.T.C., *A Look Behind the Screens: Examining the Data Practices of Social Media and Video Streaming Services*, Staff Report (2024), https://www ftc.gov/reports/look-behind-screens-examining-data-practices-social-media-video-streaming-services.

Point being, these companies are hardly an authority on proper privacy hygienics.

As to free speech, I stand on the shoulders of Third Circuit Judge Paul Matey who poignantly stated that Big Tech "[s]muggles constitutional conceptions of a 'free trade in ideas' into a digital cauldron of illicit loves' that leap and boil with no oversight, no accountability, no remedy."[9] And it's true. Big Tech has leveraged the (admittedly) messy First Amendment jurisprudence to turn our bulwark for free expression into a sword to cut down laws they don't like.

But there's good news. The Supreme Court is creating a clearer pathway for these measures. To start, in *TikTok v. Garland*, the Supreme Court categorically rejected TikTok's argument that the mere regulation of an algorithm raises First Amendment scrutiny.[10] Even better, the Court clarified that a law regulating a tech platform doesn't invite First Amendment review if the law's primary justification is not content based, even if its ancillary justifications are.[11]

In sum, it's clear from my review, that the bills before us today, particularly the App Store Accountability Act, the SCREEN Act, and the Kids Online Safety Act, have taken these considerations into account and are poised to resolve many of the challenges parents are facing in today's digital age with respect to child safety.

I appreciate the committee for inviting me to testify and look forward to your questions.

---

[9] *Anderson v. TikTok*, 116 F.4th 180, 185 (3rd Cir. 2024) (Matey, J. concurring).

[10] 145 S.Ct. 57 (2024).

[11] *Id.* at 72.

Mr. BILIRAKIS. Thank you so much.

Now I will begin the questioning and recognize myself for 5 minutes.

Mr. Berkman, for too long the narrative has been that online safety is solely parents' responsibility. But, as you know, 80 percent of parents say that harms now outweigh the benefits and they feel completely outmatched by these highly complex platforms designed to keep their kids hooked.

My bill, the Kids Online Safety Act—again, it is a discussion draft—fundamentally flips this dynamic. We require platforms to enable the strongest safeguards by default, rather than forcing parents to dig through multilayered menus to find these critical tools.

Can you explain why shifting the burden of safety from the parent to the platform can change the trajectory of this dire safety crisis?

Mr. BERKMAN. Thank you for the question, Chairman, and I think it is a very apt one. You are correct that parents across the country are frustrated, they are saddened, and they feel defeated.

We work with hundreds of thousands of families, partnering with K-through-12 schools, teaching essential social media safety skills. And so we can hear from families on the ground nationwide.

Children are using multiple platforms many hours a day with many different features, and they are not set to be safe, by design. And so we do believe that the provisions you have put forward in your legislation would materially move safety forward and ensure that parents are not battling for their children's safety alone.

And I would note Sammy's Law, as well, would give parents one unified tool to help maximize safety. And so that is why we support that bill.

Mr. BILIRAKIS. Thank you very much.

Mr. Thayer, in your testimony you state that KOSA, along with many of the other bills considered today, will resolve many of the challenges parents are facing in today's digital age with respect to child safety.

KOSA includes numerous other protections such as parental controls, default settings, policies to address design features, and mandatory audits.

Can you explain how KOSA will empower parents to protect their kids online and will hold Big Tech accountable?

Mr. THAYER. Well, you took the word right out of my mouth. The keyword there is "accountability." And right now there is absolutely none.

At this point, we have to rely basically on their musings via press releases and other terms of service that we hope they will adhere to. And we have actual data to support that. At this time, TikTok, Meta, and the like all have so-called parental protections, and they all have failed miserably.

The problem is that there are, frankly, no laws that actually articulate what their goals are and what they are responsible for. Things like KOSA, which I prefer over more general statutes, articulate clearly what these companies are responsible for doing and when they run afoul of those responsibilities and when we can enforce.

At this point, they have no Sword of Damocles over their head, and even if they did, we wouldn't be able to cut it down to get the results that we need to protect kids and protect parents.

So KOSA would go a long way in ensuring that the status quo is not going to be the status quo forever.

Mr. BILIRAKIS. Thank you very much.

Mr. Lekas, in your testimony you call for online tools that empower children, teens, and families. In your view, are KOSA's requirements for platforms to implement new safeguards and parental controls workable?

Mr. LEKAS. Thank you for that question.

In our sense—and we are still reviewing this with our members, but—the tools that would be required under KOSA are definitely workable. There's a number of companies that have implemented some of these tools already, but we need them to be implemented across the board. We need to protect all children on all platforms.

The other thing I would say about KOSA is the requirements to establish procedures and processes and so forth seem really well designed to address the constitutional concerns that have come up with respect to earlier drafts of this legislation.

Mr. BILIRAKIS. Very good. Thank you very much.

I will yield back.

And I will recognize now the ranking member of the subcommittee, Ms. Schakowsky, for her 5 minutes of questioning.

Ms. SCHAKOWSKY. OK.

Ms. Ruane, I wanted to ask you, what is the biggest gap that you see right now, that if we were to begin right now to fix it, what do you think is the biggest gap that we are encountering?

Ms. RUANE. Thank you, Representative Schakowsky, for the question.

I see a number of gaps that would be left by the legislation. Even with the 19 bills, I see a number of gaps that would be left.

The biggest one that I see is the preemption standard that is within all of the bills that are currently before the committee. We are concerned that the "relates to" preemption standard will preempt State laws that specifically protect kids and also State laws that have general protections that also apply to children, so State UDAP laws, State tort laws, and also State comprehensive privacy laws that have specific protections for children, including enhanced protections for children's data as sensitive data.

Texas, for example, protects all children's data as sensitive data at a higher standard than the current COPPA does. The current preemption standard under the bills that we are considering today would likely preempt that law as applied to kids.

If we finish this process with the "relates to" standard in place, you will likely wind up with children having less protections at the State level than they do today, and we will have failed to do our jobs.

So I think that is one of the biggest gaps that I see.

I also see that there is not enough—in any of the bills that require age verification, we do not see sufficient guardrails to protect and require privacy and security practices within the age-assurance requirements and to ensure that any age-assurance tech-

niques that are used are fairly and equitably accessible to everyone that has to go through the age-assurance process.

Ms. SCHAKOWSKY. You know, when I listen to you, I think there are so many things that need to be changed as soon as possible, and the idea that the States cannot do anything in the legislation is quite shocking to me. And so I just really think that we have to go back to the drawing board and make sure that we know.

The other thing I wanted to ask you is about LGBTQ kids and making sure that they have some authority to be there, to be heard. And I wonder if you could comment on that.

Ms. RUANE. Absolutely. Thank you for the question, Ranking Member.

We are significantly concerned that any censorship incentives within some of the bills that are before us today and within the Senate's version of KOSA could lead to the censorship of LGBTQ speech—access to that content by LGBTQ kids and speech by LGBTQ kids, because oftentimes that speech can be miscategorized as sexual speech or as speech that falls into categories that platforms look to take down because they are concerned about enforcement and about harms to children related to accessing sexualized content.

Our second concern with respect to that is that the bills at issue today delegate authority, enforcement authority, to this current FTC, which has demonstrated its willingness to target groups that it disfavors, including transgender families—including transgender people, their families, and their caregivers.

If we do not have an independent FTC that is enforcing the law fairly as it applies to all children and protects all children, we have significant concerns about how these bills would operate in practice, even if the way that they are currently constituted is neutral and would protect everyone.

Ms. SCHAKOWSKY. So appreciated.

And, with that, I yield back. Thank you.

Mr. BILIRAKIS. The gentlelady yields back.

I now recognize the chairman of the full committee, Mr. Guthrie, for his 5 minutes of questioning.

Mr. GUTHRIE. Thank you. I appreciate that.

And thank you all for being here.

So, Mr. Berkman, there is no single solution for protecting kids online, and that is why we are advancing a comprehensive strategy of nearly two dozen bills that build in layers of protection, from age verification in COPPA 2.0 privacy protections to parental tools and default by design.

Can you speak to the urgency of this moment and the need for Congress to protect kids and children and teens online?

Mr. BERKMAN. Yes. I appreciate the question.

We are seeing, still, an alarming disconnect in terms of awareness of how severe and pervasive the harms of social media are. We are seeing millions of children across the country harmed. We are on the ground, working with families, and the actual data is absolutely stunning and the stories are heartbreaking.

And so I appreciate the approach taken by the committee. We need to find consensus and pass meaningful social media safety legislation this year to protect our children.

Mr. GUTHRIE. Thank you.

And to add to that, Mr. Lekas and Mr. Thayer, can you explain why we need a layered, comprehensive strategy rather than just one single bill?

Mr. THAYER. I thank you for the question. And I think the question sort of beckons the answer, is that individual layers require different policy solutions. The same thing that would apply to a social media company may not be apropos to maybe something on the app store layer, even the operating system layer or device layer. Each one of these folks have a role to play—or, each actor has a role to play, and every policy solution should be attuned to what those particular roles are.

So a comprehensive approach, whether it is privacy, competition, or even child safety, has to be administratively thought through. So, again, in full agreement with what I have heard today. And it seems to be the case that each individual layer requires a special sensitivity to what those particular areas do and needs a policy solution that meets them where they are.

Mr. GUTHRIE. Good. Thank you.

Mr. Lekas?

Mr. LEKAS. Thank you for that question.

I think the overall goal that seems to be the consensus of everyone in this room is, we need to protect youth online. We need to improve the privacy protections and the safety protections for youth.

And I think stepping back and looking at all the different components here and trying to identify what is the best way to do each of these components is a really smart way to proceed. Congress has been debating legislation in this space for years, and it is urgent to move forward now. So we appreciate the approach taken by the committee.

Mr. GUTHRIE. Thank you.

And, also, Mr. Thayer, in my opening statement I emphasized that a law that gets struck down by courts won't protect a single child.

From a legal and constitutional perspective, why is it so critical that Congress can step in to establish a single, uniform national standard? And how does this package of bills learn from the defects of laws that have failed judicial review?

Mr. THAYER. Well, as someone that really does appreciate the structure of our Constitution and especially the Federal structure that they have created and, again, leveraging the insights from different Justices, much smarter legal minds than my own—Justice Brandeis, for instance, said that the States are the laboratories of our democracy. But, at the same time, those laboratories yield results.

And I think what we have seen in the past 10 years, absent Federal insight as to what Congress actually wants or what the national standard is, has allowed for a lot of these experiments to go all the way through the courts. The courts have evaluated each one of these standards and have given, as I said in my opening testimony, a pathway for Congress to actually set those standards.

Because part of that experiment is not just only seeing where Congress can step in, it is seeing the limitations that States have

in fully protecting children. A child in Texas should be equally protected as a child in California or in Iowa and everywhere else. And that is where I think the Federal standard is probably preferable in many cases. But, again, that comes from a lot of the insights that we are getting from States.

Mr. GUTHRIE. OK. Thank you.

And that concludes my questions. I yield back.

Mr. BILIRAKIS. The gentleman yields back.

I now recognize the ranking member of the full committee, Mr. Pallone, for his 5 minutes of questioning.

Mr. PALLONE. Thank you, Chairman Bilirakis.

Data brokers collect and sell billions of data points on nearly every consumer in the United States, including children. And while I believe that comprehensive privacy is the preferred path to addressing the risk of data brokers, I also believe it is imperative to do what we can now to prevent data brokers from exploiting the personal data of our kids.

So I have a series of questions for Ms. Ruane. If you could just answer them quickly, because otherwise I won't get through them.

First is, why is it so important that kids and teens are able to enter adulthood without an extensive profile already built of their online activities and inferences about who they are?

Ms. RUANE. Thank you, Ranking Member.

Well, kids are growing up online, right? They are sharing all of their information all of the time. They are engaging constantly. And their data is also being collected constantly, in ways that they might not understand or even be aware of or be developmentally capable of making decisions about. They don't know they are making a trail that is going to follow them forever.

But what is most important is that children are not commodities, and their lives and privacy have to be respected. Ensuring that their information cannot be bought and sold by shady data brokers will meaningfully protect their privacy in general and their ability to enter adulthood without a profile that will follow them for the rest of time.

Mr. PALLONE. Well, thank you.

Now, many of the bills being considered for this hearing today contain broad preemption clauses, and in many cases preempting any State laws that relate to the legislation.

So the next question is, What are some unintended consequences of such broad preemption? Could common law and product liability claims currently being used to hold tech companies accountable be impacted by that?

Ms. RUANE. Yes, absolutely. We are concerned that currently extant State protections that protect everyone will no longer be able to protect children across all 50 States.

One other thing to note is, a lot of the bills today focus on legacy platforms and services that have existed for a while, and they do not focus on emerging technologies like generative AI. If we institute a broad "relates to" preemption standard across all of these bills, we run the risk of preempting States' ability to act on emerging technologies quickly.

Mr. PALLONE. OK.

Many of the bills being discussed today also have provisions that expand access to the data of teens, both to third parties and to parents, in the name of increased safety. And while I encourage parents and teens to have conversation about teens' online activity, that also needs to be balanced against teens' rights to privacy.

So, as we consider the bills before us, how do we best balance privacy and safety? Are there any specific provisions in these bills that pose a threat to kids' privacy?

Ms. RUANE. Absolutely. Parents and kids, families, need tools to help them navigate their online lives, and CDT fully supports giving parents those tools and children those tools, but we are concerned about any provisions that give parents access to and control over the content of kids' communications.

One thing that the current version of KOSA does well is it ensures that platforms do not have to disclose the contents of kids' communication. But today's new version of COPPA 2.0, for example, contains language that might allow parents to delete their kids' data and to delete content that they may have created.

When we talk to parents and kids about whether they wanted to have those sorts of tools, parents told us that that seemed overly burdensome for parents, and kids told us that seemed overly invasive to them.

Moreover, as you noted in your opening statement, not all kids are growing up in families that are perfectly supportive, and some kids are growing up in situations where they don't have families at all.

Mr. PALLONE. Well, that is sort of my last question——

Ms. RUANE. Yes.

Mr. PALLONE [continuing]. Because I know we're going to run out of time. But the unfortunate reality is that there are parents who abuse and neglect their children. For these kids, access to safe spaces online can be critical.

So the last question is, how do we foster healthy connections online while ensuring that kids and teens are protected? Are there potential risks to children and teens in dangerous or hostile family environments caused by the measures in these bills?

Ms. RUANE. Well, when we talked to teenagers about how they use, for example, direct messaging services, they told us that what they really want are more controls over who gets to message them—so the ability to reduce their own visibility online. Congress could also incentivize more friction or speed bumps in interaction with, kind of, unknown profiles or unknown adults.

We also took note that one of the bills today would restrict access to ephemeral messaging. Now, while it is understandable that in some circumstances ephemeral messaging could be linked to harm, we also want to note that it could also be used to protect kids' privacy.

So, for example, children might communicate with each other, teens might communicate with each other through racy text messages. Ephemeral messaging could reduce the likelihood that those messages be used for abusive purposes like nonconsensual intimate image distribution at a later date.

Ephemeral messages could also be helpful for children who have relationships with domestic violence victims or who are domestic

violence victims themselves to ensure safety and to ensure their ability to communicate privately without risk to their physical selves.

Mr. PALLONE. Thank you.

Thank you, Mr. Chairman.

Mr. BILIRAKIS. Thank you very much.

And the gentleman yields back.

We will recognize the vice chairman of the subcommittee, Mr. Fulcher, for his 5 minutes of questioning.

Mr. FULCHER. Thank you, Mr. Chairman.

A question for Mr. Berkman. This has to do with recommendations you might have for young adults who are engaging with some self-harming behavior.

In your testimony, you cite some statistics having to do with self-harm, cyberbullying, with eating disorders, and—and that particular topic. And we have also learned through various court filings that social media companies have been knowing about this. They know this is going on.

Not long ago, we had some hearings with TikTok, and we learned that they had sent 13-year-olds even more content on self-harm and with eating disorders. And that came out also that Meta had pushed body-image content when teens had expressed some dissatisfaction with their bodies. So these social media companies, they know about this.

And I dealt with this in a previous life as a State legislator, with some mental health issues.

And I just want to ask you, from your perspective, what recommendations or guidelines can you offer for this body here to address this growing problem?

Mr. BERKMAN. Thank you, Congressman, for the question, and I appreciate it.

It is true and something we really need to recognize across this country that these companies have a durable inherent conflict of interest between our children's safety and their profits. And so, last decade, we have seen child harmed after child harmed. And so one of the bills that we really support here is a bill called Sammy's Law, and that would give parents, families access to what we call third-party safety software—software not connected to the social media platforms themselves—that can provide families with critical lifesaving alerts, like eating disorder-related content, content involving suicidal ideation, so that families can provide lifesaving support at the exact right critical moment, which right now they are not getting, and because of that we are seeing fatalities.

Mr. FULCHER. So engagement with the parents, and that third-party software is a help.

Mr. BERKMAN. Third-party software, and I would note, is significantly—it adds to privacy in a significant way over the status quo. This is technology that we now have that can limit alerts to parents on a list of harms that every Member of this body agrees on and that children vitally need support to protect themselves from.

Mr. FULCHER. Thank you for that. I am going to come back to you here in just a second, but I want to get a question to Mr. Thayer here.

We really need real consequences for bad actors and the enforcement that goes with it. In all the bills we consider here today, they place regulatory obligations on tech platforms and include both FTC's first fine authority and authorizes State attorneys general to engage with this.

First of all, do you see that as adequate, and can you discuss the benefits of these enforcement tools and how they will actually be used to hold some of these tech firms accountable?

Mr. THAYER. Yes, our DPS position is the more cops on the beat, the better. State attorney generals have a very special role when it comes to consumer protection, as does the FTC. I think one value of these bills is that they are specific authority statutes as opposed to general authority statutes, which means you can target the specific harms on both the Federal and the State level on exactly what they want.

And in terms of combining the two, you have the FTC, which has a giant remit already—they have a national remit—whereas State attorney generals can react almost in real time or, if not, very close to, to the local issues that have—that they can observe.

So I work very closely with State attorney generals' offices in California, Texas, and Louisiana, and I can tell you that they look at these statutes and they—they look at these statutes in a very comprehensive way, and they also look at it from the perspective of protecting their populations in particular.

So, again, in my view, you need both. You can't just have—put all the reliance on the FTC. You are going to need some State attorney generals looking at this as well.

Mr. FULCHER. Great. Thank you.

Mr. Berkman, I have got 20 seconds left. Any input on that?

Mr. BERKMAN. Yes, we agree you need a robust enforcement regime. State attorneys general kind of added to that regime. We have leadership across the country from Mississippi, Illinois, Arkansas, and California attorneys general prosecuting in an effective way violations of law by the social media industry that is impacting children. They are doing it collaboratively, which means pooled resources, that means effective enforcement, that means saved lives.

Mr. FULCHER. Great. Thank you, Mr. Berkman.

And, Mr. Chairman, I yield back.

Mr. BILIRAKIS. The gentleman yields back.

Now recognize Ms. Castor from the great State of Florida. You are recognized for 5 minutes of questioning.

Ms. CASTOR. Well, thank you, Mr. Chairman. Thank you for teeing up action to address the privacy, intrusion, surveillance, and targeting of kids online and the growing harms due to the malign design of online apps that lead to physical and mental harm to young people.

I want to thank the witnesses, but the panel is missing a parent. There are many here today who could have testified. You are missing a young person. There are other young people here who could have testified. You are missing a psychologist or a pediatrician. And one of the many whistleblowers, former tech company employees, to testify on the insidious schemes to addict and exploit children even as tech company executives knew of the harm to kids.

It was 2021 when Francis Haugen, the Facebook whistleblower, testified before Congress that Facebook Meta built a business model that prioritizes its profit over the safety of its users. She said Facebook repeatedly encountered conflicts between its own profits and safety and that Facebook consistently resolved those conflicts in favor of its own profits. She went on to testify that Facebook became a trillion-dollar company by paying for its profits with our safety, including the safety of our children. Doesn't this remind you of the tobacco company propaganda of years ago?

This committee knows too well that the big tech companies take advantage of young people online. That is why it is so disappointing that Republicans in the House are offering weak, ineffectual versions of COPPA and KOSA. These versions are a gift to the big tech companies and they are a slap in the face to the parents, the experts, and the advocates, to bipartisan Members of Congress, who have worked long and hard on strong child protection bills to protect them from what is happening online.

So despite a broad agreement among House Members and Senate Members, we really need to address these watered-down bills, and I am hoping that the rank-and-file membership and the members of this committee will chart that course. For example, we should not put a ceiling on kids' protections at the State level or stifle the good work of the States or weaken knowledge standards that are critical to holding tech companies accountable.

Ms. Ruane, you have already addressed preemption. You said a lot of the preemption language in the bills would provide less protection to kids. You have touched on weaker enforcement. That is contained here. You talked about data minimization.

How does—there is now a difference in the knowledge standards too. The Senate versions are kind of viewed as the strong bipartisan versions. How does the Senate knowledge standard further protect young people compared to what is in the House version?

Ms. RUANE. Thank you, Representative Castor. Yes, there is a difference in the knowledge standard in the bills at issue today. Particularly in COPPA 2.0, we see a tiered knowledge standard that preserves actual knowledge for the vast majority of actors, and that is, you know, basically preserving or maintaining the status quo. The Senate version of COPPA 2.0 has an updated knowledge standard, which would apply to all actors. Honestly, this is a difficult balance to strike, but the hope is to land on a standard that does not permit a company to look the other way when they know there are kids on their service, while avoiding incentivizing broad age assurance across the entire internet.

While we think there needs to be changes to House COPPA, we fully support enhancing protections for children's privacy, and we hope that we can all work together to update COPPA 2.0 in a way that would do so.

Ms. CASTOR. Thank you for that. Do you want to say anything else about enforcement as well? You already talked a little bit about the FTC, but when we are talking about kids, isn't it appropriate to have a number of tools in the toolbox to make sure they are safe and tech is held accountable?

Ms. RUANE. Absolutely. It is not just appropriate, it is also how Congress has approached protecting children historically. Congress

has generally not chosen to preempt States' ability to act and has always ensured that there are more tools in the toolbox. It was good to hear and it is good to see that the FTC would have things like first fine authority and that State attorneys general would have the ability to act, but we also need to see things like private rights of action as a force multiplier for families and kids to be able to enforce their rights under any statute that Congress passes.

Ms. CASTOR. Thank you for that.

I also want to make sure that I get into the record a number of provisions. Mr. Chairman, at the end of the hearing, we will have a number of documents to submit for the record, a lot of letters from groups: the Federal Trade Commission September 2024 report that I recommend to the committee, the—some of the whistleblower testimony from the United States Senate that is very illuminating, some of the other reports from various medical societies. I think all of this would really inform our decision making as we move forward.

Mr. BILIRAKIS. Thank you.

Ms. CASTOR. And I will ask unanimous consent at the appropriate time.

Mr. BILIRAKIS. Absolutely.

All right. Now we will recognize Dr. Dunn. He is the vice chair of the full committee. We will recognize you for 5 minutes, sir, for your questions.

Mr. DUNN. Thank you very much, Mr. Chairman.

I have been fortunate to wear a lot of hats in my life. I was a soldier. I served my community as a sergeant for 35 years. But the title that keeps me up at night, that drives me, is granddad. My sixth grandchild was born yesterday, as you know, Gus. I made it look easy.

But we are living through a crisis right now. We have handed our children devices that are more powerful than the most powerful computers, sent men to the moon, but we failed to install the digital equivalent of seatbelts and smoke detectors on these things.

As a doctor, I see—when I see a patient bleeding, I just apply a tourniquet. I don't call a committee meeting. Right now our children are bleeding. Our children and our grandchildren are being targeted, groomed, and exploited on social media platforms that are designed—intentionally designed—to hide the evidence of their exploitation.

That is why I introduced H.R. 6257, the Safe Messaging Act for Kids, call it SMK Act of 2025. This bill is a direct intervention to stop two specific mechanisms that predators use to hunt our children: ephemeral messaging and unsolicited contact. The problem is disappearing evidence.

Let's talk about ephemeral messaging. This is a fancy term for a dangerous feature that messages automatically delete themselves after they are viewed. Imagine if a drug dealer could sell fentanyl to a teenager in a school hallway, and then the moment the transaction is done, any security camera footage automatically erased itself. That is what is happening online.

Predators love ephemeral messaging. It is their best friend. It destroys any evidence of grooming, cyberbullying, illicit transactions

before a parent ever sees it and before law enforcement can build a case. My bill would put an end to this.

Under section 3 of the SMK Act, social media platforms would be strictly prohibited from offering ephemeral messaging to any user they know or willfully disregard is a minor under 17. If you are a tech company and you know your user is a 14-year-old child, you should not be handing them a tool to destroy evidence. It is that simple. The solution is, of course, parental authority.

The second part of this bill is unsolicited contact. Right now in the digital world, strangers can walk up to our children and whisper in their ear. We would never allow that on a playground. Why do we allow it in direct messages? The SMK Act mandates parental direct messaging controls. We are putting parents back in the driver's seat.

For children under 13, the bill requires the direct messaging features be disabled by default. A 10-year-old should not be fielding messages from strangers. If that feature is to be turned on, a parent must proactively give verifiable consent. For teenagers under 17, parents have to have the tools to see who is knocking on the door.

The bill requires platforms to notify parents of requests for unapproved contacts and gives the parents the power to approve or deny those requests before any messaging occurs. This isn't about hovering. This isn't helicopter parenting. It is just about parenting. It is about giving moms and dads the dashboard they need to keep kids safe.

Mr. Chairman, in medicine, you know, we take an oath: Do no harm. For too long we have allowed social media platforms to violate that oath, and they have built features that harm our children, drive engagement by our children. The Safe Messaging Act for Kids is a commonsense, you know, treatment plan for this, and it preserves the evidence of crimes, it restores parental authority that protects our kids, and I urge my colleagues to support this legislation.

I will submit questions for the panel. Sorry I have used up my time, but I wanted to make a case for this.

Thank you so much, Mr. Chairman.

Mr. FULCHER [presiding]. Thank you.

The gentleman from Florida, Mr. Soto, is recognized for 5 minutes.

Mr. SOTO. Thank you, Mr. Chairman.

Today we are here to empower parents to protect kids online, and Congress needs to do its job and make rules of the road. It has been 5 years since the Children's Online Safety Act has been filed—5 years too long to address this critical issue.

When we look at the internet and social media, we see education, entertainment, communication with friends—all great things for kids. But we also see a quagmire of issues that they could fall into, which is why we need guardrails to protect children's privacy, stop access to adult content, unbridled chatbots, even predators online.

So today we have 19 bills, including our bipartisan Promoting a Safe Internet for Minors Act with Representative Laurel Lee, my fellow Floridian. H.R. 6289 directs the Federal Trade Commission to conduct nationwide education campaigns to promote safe inter-

net use by minors, encouraging best practices for educators, parents, platforms, and minors, and sharing the latest trends about negatively impacting—that are negatively impacting minors online, and making publicly available online safety education.

The only issue is we have an FTC where President Trump fired both the Democrats, and now there are only three out of the full five strength that they need, and the courts have been taking their sweet time to address this issue. And so it is critical that we as a committee make sure we get the FTC up to strength and hold the President accountable for this unlawful action.

We also need to limit kids' access to chatbots. We saw a tragic story from Central Florida—of Sewell Setzer III's story, a ninth-grader from Orlando Christian Prep. He died by suicide last year at age 14 after being prompted by a chatbot that he was listening to. Sewell's mother, Megan Garcia, testified in the Senate Judiciary Committee in September of this year. In her testimony she described how Sewell was manipulated by the chatbot and sent sexually explicit material. She has filed a wrongful death suit—lawsuit.

This is why bills like the SAFE Bots Act that we see which would develop AI policies to prevent harm, AI disclosure prohibiting them from posing as licensed professionals, and then enforcement's key, the FTC, which we need to fully restore to its full strength, and State attorneys general.

And then back in Florida we see new laws that restrict use under 14 years of age, parental consent 14 and 15 years of age, and it was just recently upheld on appeal. And lastly, we are working with local sheriffs like the Osceola County Sheriff's Office to get the millions in funding to protect kids online with the Internet Crimes Against Children Task Force, absolutely critical for our local kids.

Ms. Ruane, we saw President Trump illegally fire two of the Democratic members of the FTC. Even with all these bills that we have filed, even if they pass, how does the decimation of the FTC affect enforcement of laws meant to protect kids online?

Ms. RUANE. Thank you, Representative Soto. So the FTC has historically had—as an independent agency, has historically had a reputation of protecting consumers regardless of the party in office. The current administration is undermining that reputation and threatening the FTC's ability to enforce the law fairly.

If—I say this in my testimony, but I will say it here again: Laws are only as good as their enforcement mechanisms. They are only as good and fair as their enforcers. Laws without good enforcement are, at best, just words on the page, but at worst they are weapons to be used by the powerful against the powerless. And the worry with the FTC becoming a politicized institution is that, rather than enforcing the laws to protect everyone and uphold the rule of law, it will instead become a partisan tool that could be used and weaponized against those that the administration, whoever occupies the office, dislikes or, on the other hand, favors.

If, for example, you know, the President has a particular relationship with a particular company or a particular CEO, we are concerned that the politicization of an FTC could lead to favorable treatment and lack of enforcement of laws against those companies

and, on the other side, targeting or retribution against those who would——

Mr. SOTO. Thank you, Ms. Ruane.

Mr. Thayer, we talked a little bit about bots being out of control. What rules really do we need to help make sure we protect our kids?

Mr. THAYER. Thank you, Congressman. Look, we are going to need a lot. I mean, the rate at which this adoption is happening is unlike anything that we have ever seen, even with respect to social media and particularly when it comes to kids. Kids are now using chatbots for everything under the sun, whether it is——

Mr. FULCHER. Mr. Thayer, time has expired. If you could wrap really quick, please.

Mr. THAYER. Sure. In general, solutions that you guys have proposed today can go a long way. Also, what Senator Hawley has introduced is another interesting avenue, along with Senator Blumenthal. So I look forward to working with you and your office on this.

Mr. FULCHER. Thank you for that. Time has expired.

The Chair recognizes the gentlelady from Florida, Mrs. Cammack, please.

Mrs. CAMMACK. Well, thank you, Mr. Chairman. Thank you to our witnesses and for everyone in the audience here today.

As a new mom, today's hearing certainly is hitting pretty close to home. Today we are reviewing 19 bills, but we are missing a critical one: the App Store Freedom Act. This bill would empower parents and consumers, foster innovation, and most importantly protect kids online and their data. This bill has broad bipartisan support on this committee and is a critical step in keeping kids safe online.

I want folks to imagine for a moment what it would look like if parents—parents—were allowed to build an online marketplace, an app marketplace, where they could vet the apps and knew for sure that their kids were safe. Today that is not possible. And only our bill, the App Store Freedom Act, can do that.

I would also like to point out for the record that last year alone, in 2024, the Apple App Store facilitated nearly $406 billion in sales. So taking that into consideration, the 30 percent tax, no matter how you slice it that Apple requires of these apps and their subscriptions, is a multibillion-dollar industry. So it would stand to reason that Apple has a couple billion reasons why they don't want to protect kids online and they don't want parents creating their own marketplace.

So I am going to jump to our questions. Panel, we are going to go rapid fire to start.

In 2024, in my home State of Florida, 13- and 14-year-old boys were using nudify apps to take pictures of their 12-year-old classmates and digitally unclothe them. The perpetrators—because that is what they are—then shared those images with their classmates and others. Another investigation into Apple showed that it allowed a nudify app in its App Store and then rated it, Apple rated that app as appropriate for 4-year-olds. Four-year-olds.

So for the panel, rapid fire. We will start with you, Mr. Berkman: Do you think that app stores should be allowed to have children accessing nudify apps, yes or no?

Mr. BERKMAN. No.

Mrs. CAMMACK. Mr. Lekas?

Mr. LEKAS. No.

Ms. RUANE. No.

Mr. THAYER. Hell no.

Mrs. CAMMACK. Excellent. I like this rapid fire.

For the panel, yes or no: Today Apple and Google profit by taking a 30 percent commission for sales of app subscriptions, apps that include the ability to nudify underage classmates.

Is that acceptable, yes or no?

Mr. BERKMAN. No.

Mr. LEKAS. I have no awareness of those facts. I can't speak to the question.

Mrs. CAMMACK. Interesting.

Yes or no?

Ms. RUANE. I am not sure, but I think no, because——

Mrs. CAMMACK. God, I would hope no.

Mr. Thayer?

Ms. RUANE. The question is whether they should profit off of nudify apps?

Mrs. CAMMACK. Should they profit—should Apple and Google be profiting off of——

Ms. RUANE. No. No, no one should profit off of nudify apps.

Mrs. CAMMACK. I appreciate the clarity in your answer. Thank you.

Mr. Thayer?

Mr. THAYER. Again, hell no.

Mrs. CAMMACK. No. I appreciate that.

Now, I think we are all aware that there have been investigations into nudify apps being used by minors against fellow minors and also adults using these apps to nudify minors. This has been covered extensively through the BBC, FOX News, CNN, CNBC, and others.

So, Mr. Thayer, Apple and Google have said that they are keeping kids safe online, but based on that track record that is well documented, do you think that Apple and Google are doing everything that they should to keep kids safe in the app store?

Mr. THAYER. Not even the bare minimum.

Mrs. CAMMACK. Perfect. Now as mentioned before, we have a bipartisan bill with many cosponsors on this committee that would stop Apple and Google from maintaining their app store monopoly, because that is, in fact, what they have. Often when we talk about monopolies, we focus on price gouging, but there are other good reasons why you would want to stop a monopoly from abusing their power, like speeding up innovation, improving quality, protecting kids, for example.

So, Mr. Thayer, you recently signed a letter in support of our bill, the App Store Freedom Act. Thank you for that.

It is not easy taking on the tech giants, is it?

Mr. THAYER. As someone who has taken them on in every State, no.

Mrs. CAMMACK. You can just keep your microphone on too.

Mr. THAYER. OK.

Mrs. CAMMACK. Now, could you——

Mr. THAYER. Just point of clarification, I think we led that letter, so——

Mrs. CAMMACK. Yes, you did. Thank you. Thank you for your leadership in that.

Could you help the committee here understand how more competition keeps kids safe?

Mr. THAYER. Well, it is pretty intuitive. So, I mean, more competition means more tools. More tools means more access for parents to use. So at the end of the day, competition is another area where we can actually increase parental controls and also incre—make privacy actually a thing that you have to fight for in the market.

Right now, as you note, there is no free market in the app store market. There is no app—there is no—and there actually is no competition in the search market either. But I would like to quote one thing from an antitrust case that involved Apple at the Supreme Court.

Mrs. CAMMACK. OK. Go fast.

Mr. THAYER. This is Justice Kavanaugh: There is no intermediary in the distribution chain between Apple and the consumer. And they need to be held accountable.

Mrs. CAMMACK. Mr. Thayer, I appreciate that. And I just want to end on this: Do you think that any monopoly, particularly those like Apple and Google, are in the best position to protect kids and their data?

Mr. FULCHER. Make that a yes or a no. Time has expired.

Mr. THAYER. Yes. But without—we need legislation to make sure they actually do what they say they are going to do, but the answer is kind of——

Mrs. CAMMACK. A bit of the fox guarding the hen house?

Mr. THAYER. Little bit.

Mrs. CAMMACK. OK.

Mr. THAYER. More than a little bit.

Mr. FULCHER. Thank you. Time has expired.

Mrs. CAMMACK. I appreciate that. I yield.

Mr. FULCHER. The Chair recognizes the gentlelady from Massachusetts, Mrs. Trahan, for 5 minutes.

Mrs. TRAHAN. Thank you, Mr. Chairman.

Well, I don't think I need to belabor the points that my colleagues have correctly made about this hearing's policy and procedural failures. The flagship proposals for today's hearing, KOSA and COPPA 2.0, have been gutted and co-opted by Big Tech. And in their process of backroom dealmaking, committee leadership has shunned parents, advocates, and bipartisanship. I sincerely hope we can move past this to get meaningful, balanced kids safety legislation across the finish line, and I am here, as I always have been, to work with my colleagues on both sides of the aisle to achieve that.

To that end, I do want to call attention to an area that is missing from this hearing's slate of kids safety measures: app store competition. App stores are the distributors of the software kids rely

on to run their digital lives. Apple and Google control access to nearly all American smartphones, and Federal courts have already found that they hold monopoly power over those markets. They wield that dominance to block third-party app stores while profiting from their own inadequate child safety practices.

As a coalition of child safety organizations recently noted in a letter to the committee, quote, "without meaningful competition, these firms have continually failed to protect children from sexual exploitation, exposure to obscenity, abuse of their data, and more," end quote. In the case of Apple, one of its engineers even said in private messages that it is, quote, "the greatest platform for distributing child porn" and called child predator grooming a, quote, "underresourced challenge."

Mr. Thayer, in your testimony, you call out some of the specious arguments offered by Big Tech against practical solutions to improve kids' safety. What is your response to Apple and Google's suggestions that the App Store Freedom Act and other measures will hurt kids' privacy and security, and are these companies' financial incentives actually aligned with the needs of our children?

Mr. THAYER. So in my testimony—I will State it again—it is all a farce. It is always the case where they play this game of if you want to regulate competition, it is a privacy issue; if you want to regulate privacy, it is a competition issue. So, frankly, it is the same story being told over and over again. And as I said in my testimony, Big Tech's lobby is unrelenting and unwavering on these points, and, frankly, it has to stop. And the fact that they have been gaslighting us for the past couple decades is a bit absurd, and I think it is now time to act on bills like how you—bills that you propose and many of the bills that we are seeing today.

Mrs. TRAHAN. Thank you. It is, I agree, exhausting.

What we need is competition in parents' and kids' interests. As my colleague from Florida posed earlier, imagine for a moment a kids-first app store, one built from the ground up to protect children, replete with a curated set of apps, tailored review practices run by experts in child safety, and feature rich parent controls. In this app store, safety ratings are vetted by experts, not self-reported. Bad actors are promptly booted and not allowed to return. Such an experience is technically feasible but made virtually impossible by Apple and Google's policies.

Mr. Thayer, do you agree that the App Store Freedom Act, a bipartisan bill that I am coleading with Representative Cammack and Soto and others, would empower parents with meaningful choice over what software is on their kids' devices?

Mr. THAYER. I think it is a huge step in the right direction, and it would absolutely go a long way in helping parents. More competition means more tools.

Mrs. TRAHAN. Thank you.

In closing, I urge this committee to internalize two important points: Apple and Google cannot be trusted to protect our kids, and parents deserve better. It is vital that Congress ensures that the open market can foster competition that, unlike Big Tech, actually takes kids' safety seriously. Thank you. I yield back.

Mr. FULCHER. The gentlelady yields.

The Chair recognizes the gentleman from California, Mr. Obernolte, please.

Mr. OBERNOLTE. Well, thank you very much, Mr. Chairman. And I would like to thank the committee for holding this hearing.

This is a critically important topic, and, frankly, Congress is far behind in enshrining some of these protections into Federal law. So we have been trying for years to get this across the finish line. I am hoping that this is the year that some of these bills will make it through a markup and get past the House.

As most of the people on the committee know, for many years I ran an app developer, and so when I read these bills, I kind of look at them through the lens of, if I was still developing, how difficult would these be for me to comply with and how would I go about complying with these requirements? And through that lens, unfortunately, the bills that we are considering today have a couple of pretty serious implementational problems.

Let's start with age verification, which, you know, is key to the protections we are trying to provide here, because if we are going to say that an application can't do things if certain things—if a user is a minor, then we have to be able to figure out whether or not the user is a minor. That is really central to the protections we are trying to provide.

The problem is—and a couple of the panelists brought it up in your testimony—when you force every single app developer to do that and the typical user might have 100 apps on their phone, you are collecting private information used to verify that age is 100 times and you are storing it 100 times, and that creates these repositories of private information that are really attractive targets for cybercriminals.

So let me just suggest that it is much more efficient and much safer to do that just once at the operating system level. And that means that in the case of an iPhone, Apple would do it; in the case of an Android phone, Google would do it. They have a lot more information than developers do about the users of those platforms. And when you do it that way, you can enforce other protections.

For example, if you have an application that is labeled "for adults only," the operating system shouldn't even launch it if a minor is the current user of the system.

A couple of the bills, you know, talk about this. When an application developer is allowed to rely on the age signal that is being generated by the operating system, and there has been kind of an assertion that there are conditions under which applications shouldn't be able to rely on that signal, and that is crazy, because the developer doesn't know as much as the operating system does.

So let me just assert that, if your application is for adults only and the operating system is telling you that there is an adult using it, you should be able to rely on that.

You know, another thing that I think is really important for us to have a discussion on is this concept of duty of care. And I think it is reasonable that we should impose a duty on the people that are developing and deploying these applications, but I also think that it is lazy legislating for us not to define what we mean when we say "duty of care."

We had a good example in a hearing in this subcommittee—I believe it was last year—when we were talking about whether or not an application should have a duty to prevent online bullying by taking down a post if it was reported as bullying. And we all could agree, you know, that is reasonable. That is a reasonable requirement.

But we are also obligated to say, you know, when we impose that requirement, well, what is the requirement? What is a reasonable amount of time? Is it 2 days? Is it a day? Is it an hour?

You know, if we don't define what we mean when we say "duty of care," then we are allowing some court in the future to be arguing about what we meant when we crafted the legislation. And let me just assert that, you know, it is our responsibility to not put our courts and our judicial system in that place and define what we mean up front.

Enforcement. There has been a couple assertions by the panelists that a private right of action is a good thing. You know, let me just say we have to be really cautious about that. There are numerous examples in States across the country where that has gone awry. I will give you an example from my home State of California.

We passed in the State legislature a few years ago something called the Private Attorney General Act that allowed private parties to enforce labor laws, and now if—anyone that has a district in California has horror stories about where abusive law firms go after not big businesses, because they can defend themselves, but small businesses. And I can point to multiple businesses in my district that have been driven out of business by frivolous lawsuits that anyone would agree is frivolous.

And then one last—and I am not going to have time for questions, because I talk too much—but talking about preemption. You know, here is the deal. Like, we are trying to craft a compromise between being permissive and being protective. I mean, if we wanted to completely protect our kids, we would say kids can't go online, right. But, you know, we don't want to do that. We want to strike a balance.

Once we have struck a balance, why would we allow different States to enact different balances? That creates a barrier to entry that favors large businesses over small businesses, and just think about how difficult it is to comply with potentially 50 different State standards if you are two people in a garage somewhere trying to start a development company.

So I am really happy we are having this conversation, and I think it is critically important we get this balance right, we get something across the finish line this year.

I appreciate the discretion, Mr. Chairman. I yield back.

Mr. BILIRAKIS [presiding], OK. The gentleman yields back.

Now I will recognize Mr. Mullin for his 5 minutes of questioning.

Mr. MULLIN. Thank you, Mr. Chair.

Turning to the SAFE Bolts Act—pardon me, SAFE Bots Act. As with some of the other bills being discussed today, I am concerned that this bill would require sensitive age verification data from users for it to be effective—data that, as pointed out by my colleagues, in recent times has not been collected or safely stored by companies.

So, Ms. Ruane, in your testimony you described the First Amendment and privacy concerns with the age verification tools. Can you briefly outline some of the tools or ways companies verify the ages of their users and some of the risks with those methods?

Ms. RUANE. Yes, absolutely. Thank you for the question.

Yes, age assurance techniques create privacy and security risks regardless of where they are deployed, and if we are going to require their usage, we need to require them under the safest, highest guardrails we can possibly implement, including ensuring data minimization and deletion of that data.

We also need to ensure that there is equitable access to services that impose age verification to access them, because some age verification techniques are disproportionately ineffective when applied to people who have differing gender identities and people of—with differing skin colors than White people, basically.

Mr. MULLIN. Thank you for that. I believe the SAFE Bots Act discusses important issues. AI chatbots should not impersonate licensed professionals, but I think this is true under all circumstances, not just for minors, especially given the difficulties around verifying the age of users.

So turning to a separate issue. In your testimony, Ms. Ruane, you outline this important role that States have historically played in protecting minors from harm. I believe this is an important point to acknowledge, particularly as lawmakers look to close gaps and loopholes that may have left some emerging technologies outside the reach of current law.

So what are the risks of widespread preemption displacing longstanding State-level protections or preventing lawmakers at all levels of government from adapting current laws to novel circumstances of chatbots?

Ms. RUANE. Absolutely. Thank you for the question.

Red States and blue States alike are currently examining the impacts of emerging technologies on children and, frankly, on everyone. We don't fully understand how these technologies work, how they gather data, how they use data, and the bills at issue today do not focus enough on chatbots to ensure that there will be comprehensive protections going forward. States are light years ahead of the Federal Government on that issue right now, and we need to preserve their ability to act—not just with respect to kids, but with respect to everyone.

Mr. MULLIN. Thank you for that. So, lastly, turning to KOSA. There is certainly no question that we need to protect kids online, but we need to also balance concerns around young people's right to access legitimate information. Kids use the internet to find community as well as to access important resources that are essential to their health, safety, personal development, that may not be available or easily accessible in offline circumstances.

As we consider proposals like KOSA, we need to ensure we are reducing real harms without creating new risks throughout intended censorship or eliminating access to critical resources.

So again, Ms. Ruane, you noted in your testimony the current version of KOSA moves in the right direction by strengthening protections for kids online while preserving access to information. Could you elaborate on that just a little bit? Why do you think this

better ensures we maintain that balance and avoid unintended restrictions on the resources kids and teens are currently relying on?

Ms. RUANE. Absolutely. Thank you.

So in the Senate version of KOSA, one of our concerns is that it gives too much authority to platforms and requires them essentially to guess what types of content will harm children, and the guessing process is going to be backed up by whatever the government in charge of it—in this case the current FTC—will determine harms children. So, for example, LGBTQ-related content or other controversial content, like climate change-related content or content related to armed conflicts going on in the world, could be censored under KOSA if platforms guess that it will harm children.

The House version of KOSA narrows the duty of care, requiring platforms to essentially address what are already illegal categories of content, hopefully narrowing and limiting the amount of guessing they will have to do about what content to deliver to kids. And we think that that is moving in the right direction in terms of preserving all kids' ability to access information and speak online.

Mr. MULLIN. Thank you for that. I yield back.

Mr. BILIRAKIS. Appreciate it. The gentleman yields back.

Now recognize Mr. Bentz for his 5 minutes of questioning.

Mr. BENTZ. Thank you, Mr. Chair, and thank the panel for sharing with us today your thoughts on this most important issue.

Back in Oregon, where I am from, legislators have contacted me and asked what we are going to do in this space. Their primary concern is preemption.

And so, Mr. Thayer, starting with you. One of the questions that has been asked is that several States—California, Utah, Arkansas, Texas, Florida—have passed and are implementing laws that require parental consent, a default time limit, secure curfews, or age verification for minors. If this bill preempts those laws but does not itself impose comparable restrictions, aren't you effectively asking Congress to shield business models from the very protection States have decided children need?

Mr. THAYER. So on the issue of preemption, obviously, it is a sticky wicket and we take heavy thought in. I actually agree a lot with Ms. Ruane's—and I apologize if I am mispronouncing your name—statements when it comes—it relates to standard. I like a more complex type of preemption and to be a little bit clearer about what it is conflicting out.

And so at Digital Progress Institute we are very interested in narrow preemptions. And so, again, happy to work with your office, and I am sure other folks as well would like to work with you as well to figure out exactly how to straddle that line.

Mr. BENTZ. Mr. Berkman, your thoughts.

Mr. BERKMAN. On the App Store Accountability Act specifically?

Mr. BENTZ. No. On the thought of if we act here as we are going to, I hope, to protect children and we include in that packet of legislation a preemption of States getting involved, how do we explain to the States that we have gone to the very top level of protection when many would say, "No, you haven't"?

In other words, how does this preemption piece fit, and how do we justify it here in Congress by saying to States, like my Oregon, saying, "Hey, we have it right, and you guys can just watch"?

Mr. BERKMAN. Yes, so we make this analysis on a bill-by-bill basis, and our calculus is very clear: We are looking for a robust national framework that improves social media safety in the totality of the circumstances. And so we will move bill-by-bill in that analysis.

Mr. BENTZ. When I was thinking this through—and I haven't given it enough thought, I will admit that right off—it seemed to me that it was a commerce issue, right. You have 51 different approaches—50, depending upon who you count as States and who aren't. The question is, why would we say we in Congress want to take this upon ourselves when we are basically establishing a ceiling as opposed to a floor? That is how the question has been put to me back by my legislature—legislators.

Mr. BERKMAN. It really is—in our view, it is a bill-by-bill analysis. In some pieces of legislation, like Sammy's Law, preemption is noncontroversial, bipartisan, and makes a lot of sense. And so we are looking at, at the end of the day, where are we going to get the most protection for children and what is the analysis per bill?

Mr. BENTZ. So your thought would be, look at each bill, measure each bill, and go from there, and then somehow you can go back to the States and say, "Well, we may not have taken care of it here, but we have over there."

That takes us nicely to the remarks made by my colleague, Mr. Obernolte, where he was talking about the difference between a general duty as opposed to specific things that you can't do. Share with me why one is better than the other, the broad, general duties undefined, although we hope we could, as opposed to calling out specific practices that are not allowed.

Mr. BERKMAN. In terms of a duty of care?

Mr. BENTZ. Yes, but tell me which one is better for the protection of the child.

Mr. BERKMAN. I mean, our focus today is on the legislation in front of us, and we are desperately trying to seek consensus on legislation that moves social media safety forward. And so right now we're not looking at a broad level duty of care in the hearing today.

Mr. BENTZ. Well, ignoring that attempt to not answer my question, which one do you think is better, or is it a combination of the two? Because as a lawyer I understand how great it is to have a specific, clear standard that you then have to prove as opposed to a broad, general thing that you are, you know, shooting at as you are bringing witnesses in. Which one do you think is better?

Mr. BERKMAN. I mean, it is really hard to answer in the hypothetical. We support language, specific language, that is going to give the most robust workable protection for children at the end of the day. We want language that can pass Congress. We want language that is going to stand, be implemented, and enforced.

Mr. BENTZ. Thank you. Thank all of you for being here.

I yield back.

Mr. BILIRAKIS. The gentleman yields back.

Now recognize my friend from the great State of Michigan, Mrs. Dingell, for her 5 minutes of questioning.

Mrs. DINGELL. Thank you, Mr. Chairman, and—for holding this important hearing, and to all of the witnesses for testifying today.

But I hope, Mr. Chairman, this is our last hearing and we move to action, because we need to be moving legislation.

I want to remind us why we are here today. In this room there are parents who lost their children because Big Tech failed to protect them. This picture sits on my desk. Sam and Laura Chapman are here for their son. Sammy was just 16 years old when a drug dealer contacted him through a private Snapchat message and delivered fentanyl-laced pills to his home. On February 7, 2021, he was found dead in his bedroom. And that is why, along with Representative Evans, we have introduced the No Fentanyl on Social Media Act.

Joann Bogard is here for her son. Mason was a 15-year-old who filmed himself attempting the choking challenge that he had seen on YouTube. That day, on May 1, 2019, his father found him unconscious. He died 3 days later. This coin sits on my desk too.

Maureen Molak is here for her 16-year-old son, David, who died by suicide on January 4, 2016, after enduring relentless cyberbullying, harassment, humiliation, and threats by his peers via text message and on social media.

Rose Bronstein is here for her son Nate, a 15-year-old who died by suicide on January 13, 2022, following nonstop cyberbullying and online harassment by his classmates in which no one stepped in to stop.

And Deb Schmill is here for her daughter, Becca, who was 18 when she bought what she thought was cocaine from a dealer she found on Facebook. It was laced with fentanyl and it killed her on September 16, 2020, the night before she was supposed to enter rehab.

These families are here today because they are fighting for what is right: to hold Big Tech accountable and protect every child online. And I know there are other parents here. I want to hear your stories. But Sammy, Mason, David, Nate, and Becca are just five of the countless young people whose lives have been stolen because Big Tech won't act, and it is time for us to act. We owe these families real bipartisan action.

So I am going to move to my bill quickly. I want to discuss the legislation that I have introduced with Congressman Evans. This bill directs Federal agencies to examine how traffickers use social media to reach minors; how platform design enables access to fentanyl, which I hope angers the President of the United States on down to all of us; and what solutions could help keep deadly drugs out of kids' hands.

Mr. Berkman, how can this research under our bill help identify platform design features that enable fentanyl access and trafficking that targets minors?

Mr. BERKMAN. Thank you, Congresswoman, for the question and for your legislation, which we do support.

There are a number of families here today. You mentioned some. You don't have time for all of them. There are a number of families here that lost children due to fentanyl trafficking and drug trafficking over social media.

This is a vital issue. We see it impacting children across the country. And so your legislation is incredibly important, because we need to understand with more specificity the features of platforms

that are enabling trafficking, and it is happening. Someone mentioned drug trafficking happening in high schools. It was an example in person. It is happening on phones in high school via social media platforms.

We have looked into this issue. We have been able to connect with a drug dealer that we obviously did not know before, and in minutes. That is how accessible this has become—drugs have become to children in the social media age. So your research is necessary so that we can have the interventions, both legislative and educational as well.

Mrs. DINGELL. Thank you.

Mr. Chairman, I am going to beg my colleagues on this committee, can we please work together to protect children and keep other children from dying? And with that, I yield back.

Mr. BILIRAKIS. Absolutely, I am with you, that is for sure.

OK. Next, I will recognize Representative Fry from the great State of South Carolina. You are recognized for your 5 minutes of questioning.

Mr. FRY. Thank you, Mr. Chairman.

I actually really have enjoyed hearing the discussion here today on the bills. I think, in preparation, my staff made this giant binder of homework that I had to go through, but I really wanted to kind of hear the discussion evolve. Because what I see on this issue generally is that you have two sides that are talking at each other or past each other, but not necessarily with each other. And I think it is really important we have got parents in the room. Typically, in an Energy and Commerce hearing, you don't see this level of engagement or people that are—that have a tremendous interest in watching what happens in these hearings, but I think it is important that we get this right. It is incredibly important.

I have got an 8-year-old, and thankfully he is not on social media, and I don't anticipate anytime in the near future where he would be on social media, but kids are, and it is important that Congress gets this right.

In the audience we have Brandon Guffey from the State of South Carolina. He is a State legislator from the Rock Hill area. Not my district. I represent the beach, which is a much better place, Brandon. But Brandon has made it his life's mission to go after sextortion. His son committed suicide as a result of a sextortion plot by a Nigerian man with 30 letters in his first name—I cannot pronounce it—messaging people on social media apps.

And so the concern is absolutely there. As a parent myself, certainly he has done incredible work in the State of South Carolina, but beyond that we have to get this right.

Again, I have a simple bill in this, the Kids Internet Safety Partnership Act, which I think encourages that dialogue, right, that it takes stakeholders—parental groups, social media companies, tech industries big, small, medium—putting together best practices, not only for the companies but for the parents too, on what to do and how to act and how to protect your children in this very connected environment.

So I am super happy with that. I am happy that it is bipartisan. No one has talked any bad things about it today, so I think we are doing something right, I think, I hope.

Paul, I want to ask you something, though. Your association published a child and teen privacy and safety principles, talking about data minimization, parental tools, transparency, and risk assessments. How well do you think that the partnership model like KISPA can do, the bill that I have, operationalize those principles, part one, and two, will your member companies commit to fully participating if Congress were to pass this and it were to be signed by the President?

Mr. LEKAS. Thank you for your question, and we appreciate your legislation as well. I think it is a really smart approach, and bringing more people together in a room to come up with solutions is always valuable and especially here. Not every solution is going to be legislative. There are things that Congress can and should do.

So I think that, you know, this is an area where a lot can be done on a voluntary basis, but it also needs some teeth from Congress. And we are supportive of turning data minimization for youth into law, prohibiting targeted advertising of youth. We think these are really important, meaningful steps that can be taken. And the challenge is we may be able to bring together a number of companies that believe in upping their game and being more responsible and recognize the real concerns out there, but we don't know that that is going to be the case across the board. And very likely there will be some of that.

Mr. FRY. Thank you for that. Real quick, I want to jump into the hot topic of the day, which is preemption. You like the House version preemption component as opposed to the Senate-passed version. Is that fair to say?

Mr. LEKAS. With respect to—well, we believe in preemption. We think that preemption is an important concept to start with because, right now—

Mr. FRY. I understand that, and I have got 46 seconds, so let me nail this down. You like the House version of the preemption better than the Senate version.

Mr. LEKAS. We are still reviewing that with our members, the specific language, but we believe there needs to be a strong national standard for everybody.

Mr. FRY. Mr. Thayer, you do not like the preemption of the House version. Is that correct? Not as much as maybe the Senate version.

Mr. THAYER. I prefer the conflict preemption over as it relates.

Mr. FRY. The Senate version.

Mr. THAYER. I believe the Senate version has something similar to what the House version has, but it should—it is unclear right now as to whether or not this is a conflict preemption standard or—but as it relates typically is a broader standard, and at DPI we typically like incremental approaches to different policies. So the closer we can get to a conflict preemption standard, I think, the better off we are.

Mr. FRY. Ma'am, and you like the conflict preemption standard over the broad preemption standard. Is that correct? Ma'am?

Ms. RUANE. Pardon me. Yes, yes, we prefer conflict preemption—

Mr. FRY. And unfortunately, Chairman, I am out of time, because I actually really wanted to dive into, like, a legal argument about the—or legal discussion about this to kind of figure out

where the components are that really drive the differences and are there ways to rectify that, right. I mean, you hear the arguments on the other side on why maybe a broad, sweeping preemption would be beneficial, but then there are compelling arguments too on the other side of allowing States the flexibility to do their thing too.

So unfortunately, Chairman, I am out of time, so I yield back, but I still want to have that discussion with you all.

Mr. BILIRAKIS. Absolutely. The gentleman yields back.

Now recognize Representative Kelly for her 5 minutes of questioning.

Ms. KELLY. Thank you, Mr. Chair, and thank you to the witnesses.

In Illinois and across the country, children and teens are becoming increasingly subject to the risk of AI chatbots, social media, and other online services. So without thorough, comprehensive privacy laws for all Americans, I worry we aren't meeting the moment to ensure the health and safety of our children, particularly concerning the mental health of children and teens. The bills we are discussing today present some opportunity for progress but also give me some concerns.

Ms. Ruane, rates of depression and suicidal ideation among teens are alarming. In Illinois, there was a law passed just this year to prohibit the use of AI for direct therapeutic purposes, such as generating treatment plans. Can you describe how overbroad Federal preemption could overrule this and other important State laws?

Ms. RUANE. Absolutely. Thank you, Representative Kelly.

Red and blue States alike are currently examining kids' interactions with chatbots and online services and emerging technologies, and they are working to design ways to address concerns related to kids' privacy and their use of these services, like Illinois—like Illinois law. Preemption—relief to preemption, in particular—would put an end to that necessary thought-and-design process that is currently happening at the State level. Ossifying incomplete Federal standards and eliminating the possibility for States to step up and fill in gaps would be a mistake.

Ms. KELLY. Thank you. Children might feel inclined to disclose sensitive data about their emotions, issues at school, mental health struggles to an AI chatbot. Alternatively, they may look to these tools to receive guidance on addressing their struggles in lieu of a friend, family member, or trusted adult. We have seen this lead to devastating situations, as Adam Raine who ended his life after seeking emotional support from ChatGPT.

With that in mind, how can we treat—prevent chatbots from attempting to diagnose, manage, or treat children?

Ms. RUANE. Absolutely. So we think that chatbots should not be allowed to present themselves as mental health professionals when they are not, when they are not licensed to do so.

Another aspect of this that is worth thinking about is that this is another good example of why broad preemption would be concerning in this circumstance. Chatbots, basically all generative AI services, are data vacuums. They are collecting and compiling information from first parties, from third parties, from data brokers,

all over the internet, and they are still in need of more and ever more data to train their services.

If we preempt States' ability to deal with that issue, along with the issue of the—with the issue of the prompts that children are giving to services that are, as you noted, very private and related to extremely sensitive information, we will be failing children if we leave that gap in Federal law and at the State level as well.

Ms. KELLY. You answered my other question. Like, how do we protect—but I did want to ask everyone really quick—this is a question that was posed to me that I am just going to ask.

Some wanted to know, why don't we just codify massive statutory damages that make it so painful to be caught that then companies would pay attention? Do you think that would work?

And just go down the line.

Mr. BERKMAN. Yes.

Ms. KELLY. Oh, you do. Oh, that was short and sweet.

Mr. LEKAS. I think there needs to be a showing of harm.

Ms. KELLY. A showing of harm.

Mr. LEKAS. Actual harm. Yes.

Ms. RUANE. We absolutely agree that damages need to be meaningful.

For example, earlier this year, the FTC issued a fine against Disney for $10 million for COPPA violations. Disney is a $200 billion company. Ten million dollars is a rounding error.

We need any damages that come as a result of violations of these privacy laws to be meaningful so that it incentivizes compliance.

Ms. KELLY. Thank you.

Mr. THAYER. Yes, with strong injunctions.

Ms. KELLY. All right. Thank you so much.

Thank you to the witnesses.

And I yield back.

Mr. FULCHER [presiding]. Thank you.

The Chair recognizes the gentlelady from Florida, Ms. Lee, for 5 minutes, please.

Ms. LEE. Thank you, Mr. Chairman and our witnesses.

I also want to thank Chairman Bilirakis and Chairman Guthrie for including two of my bills—the Promoting a Safer Internet for Minors Act, which is co-led by my friend from the great State of Florida, Mr. Soto, and the Children and Teens' Online Privacy Protection Act, also known as COPPA 2.0, which I am proud to colead with Mr. Walberg of Michigan—in today's hearing.

I have dedicated much of my career to protecting the most vulnerable in our society, including children and teens online, and I am committed to working with this committee to continue that work. I very much appreciate the discussion today about advancing policies that protect children and also empower parents as they navigate the digital landscape, while also safeguarding our First Amendment rights.

Mr. Berkman, specifically, thank you for your work in empowering children and families with the tools they need to navigate social media safely and securely.

Digital technologies change so fast that even the most engaged parents struggle to keep up with the latest apps and features. That is why the Promoting a Safe Internet for Minors Act would direct

the FTC to launch a nationwide education campaign to help kids and parents learn how to stay safe.

Would you share with us why a national education campaign, similar to what the Federal Government has done for seatbelts and cigarettes, is important and what type of information or tools you believe would be the most important to include?

Mr. BERKMAN. Yes. Thank you so much for the question and for your cosponsorship of that legislation. We support it. We are across the country, as you mentioned, educating students, parents, and administrators at schools on how to keep children safer on social media because of that harm.

And so I will say first, on the advocacy part of your campaign, it is absolutely critical—I have mentioned this before in the hearing. There is an alarming disconnect in the awareness of how severe and pervasive the harms are. People are concerned and frightened, but they just don't understand how truly bad this is.

And so your legislation and that campaign is very sorely needed to bring awareness, and that helps us and other NGOs do our job.

In terms of specific education, we need help certainly on the ground. We can't cover every single child in every single school, though that is our goal.

In terms of talking about best practices, there is a lot of talk out there. It seems accessible, when we talk about social media safety. There is a lot of talk out there about social media safety, and the curriculum is not necessarily evidence-based. And that leads to time wasting at best and, at worst, counter-results or detrimental results to the child.

And so we thank you for your legislation. I think it is going to do a lot of good, and I hope it passes.

Ms. LEE. Thank you.

Mr. Lekas, thank you for your work, as well, in protecting the safety of minors online and your perspective on modernizing COPPA for the 21st century. When it was originally enacted, of course, it was well before today's landscape of digital devices and online platforms.

One of the principles that you have discussed is the approach to child and teen privacy and restricting advertising to minors. COPPA 2.0 would prohibit targeted advertising to children and teens.

But would you explain for us how targeted advertising differs from contextual advertising, and the risk that targeted advertising poses to young people?

Mr. LEKAS. Absolutely. Thank you very much for that question.

So targeted advertising involves delivering advertisements that are specific to an individual based on their online behavior and the information that may be collected about them. So think of, perhaps, creating a profile or a dossier on an individual—a machine would do this—and then deliver advertisements that seem suitable, according to the automated system, to that individual.

Ranking Member Pallone raised some concerns earlier today about the way in which data can be used—minors' data can be used, and when they turn 18, there is this dossier on them. And that is what we are seeking to prevent.

We think that contextual advertising, which is based on things like age-appropriate advertising, where your location is, is something that is appropriate because it doesn't require collecting individually specific information and creating a repository of very sensitive information.

Ms. LEE. Thank you, Mr. Chairman. I will yield back.

Mr. BILIRAKIS [presiding]. The gentlelady yields back.

I now recognize Ms. Schrier, Dr. Schrier, for her questioning.

Ms. SCHRIER. Thank you, Mr. Chairman.

Thank you to all of our witnesses for this really important discussion today.

I am very glad to see Sammy's Law included in this hearing. I have worked closely with Representatives Carter and Miller-Meeks and Wasserman Schultz to really carefully craft this bill.

Over and over today and in past hearings, we have heard about all of the tremendous dangers that kids and teens are facing online and the real-world problems and dangers that social media can create or make much worse. And, as discussed, we are talking about anxiety and depression and eating disorders and bullying and sexual trafficking and abuse and exposure to or access to drugs and even suicidality. And it feels really almost impossible for parents to protect their kids online.

This bill—we already saw a picture of Sammy—is named after Sammy Chapman, who, when he was just 16, bought a fentanyl-laced pill over Snapchat, and it killed him. One pill. And Sammy's dad, Sam, is in the room today.

And I just want to thank you, Sam, for your advocacy and for stepping up to protect other kids from that same fate.

Sammy's Law is simple. It would just make sure that parents can monitor their teens on social media. And we worked so hard to find the right balance so that parents are alerted by third-party watchdog apps but kids' privacy is also protected. And so, if certain topics rise up, then a parent gets a warning.

But this only works if the social media companies will allow these watchdog apps to work with them.

Mr. Berkman, thank you for being here today. I was wondering if you could just expand on why the existing settings and controls for minors on social media apps just aren't cutting it and why we need these watchdog apps.

Mr. BERKMAN. Yes. First of all, thank you so much for your co-leadership of this legislation, especially given your background as a pediatrician. And I say that as a son of a pediatrician, so I have reverence for that experience.

Sammy's Law is an essential part of this puzzle in terms of protecting children. First of all, it protects against almost the full spectrum of harms that are impacting children. And you named a lot of them, not even all of them. There's a lot of them, to be clear.

We have mentioned numerous times in this hearing that the social media platforms have an inherent conflict of interest between our children's safety and their profits. They move slowly.

And a perfect example here is drug trafficking over social media. We started—this was not really a major harm when we started our work as the Organization for Social Media Safety. It really exploded on the scene around 2020, and we started seeing a lot of de-

ceased children because of drugs that they purchased over social media.

We saw safety software companies, which do exist today and are actively protecting children, immediately act to make sure that they were keeping up with the language used by dealers to communicate with children—the emojis, the acronyms. Meanwhile, it took the social media platforms years to even acknowledge the problem.

And so that is point number one.

Point number two, really quickly, I will make really quickly, is this technology, sending parents alerts, maintaining your child's privacy as well—alerts just on the harm—is incredible technology. We are able to alert parents to imminent risk. The social media platforms——

Ms. SCHRIER. I am going to have to——

Mr. BERKMAN [continuing]. Cannot do that.

Ms. SCHRIER. Thank you.

Mr. BERKMAN. Thank you.

Ms. SCHRIER. I am going to cut you off there. Just—I want to make a couple more comments.

We have heard about this today. I want to just talk about KOSA, the Kids Online Safety Act, which is a great bipartisan bill that passed, I believe unanimously or almost unanimously, in the Senate, has teeth, has a duty of care for social media companies that really holds them accountable. And yet the version this year that we are taking on of KOSA has been gutted. It is toothless. It does not give the enforcement mechanisms.

And all of the people—I was a colead of the last one—who supported it last time are feeling so frustrated that, like, this is not the best we can do. And I just want to emphasize that the previous bill, the one with teeth, is the one we should be bringing up today to really protect kids online.

Similarly, there is a discussion today about getting kids under 16 off social media. I just want to say that there is a Kids Off Social Media Act, KOSMA, that also has a bill, bipartisan, in the Senate, with a path that could be signed by the President. And we need to be taking that bill up if we are serious about doing something soon to protect our kids.

Thank you. I yield back.

Mr. BILIRAKIS. The gentlelady yields back.

I will recognize Representative Kean for his 5 minutes of questioning.

Mr. KEAN. Thank you, Mr. Chairman.

And thank you to our distinguished witnesses for being here today.

Protecting America's children is of the utmost importance. The internet and social media have brought many opportunities to the American people; however, they have also brought with them dangerous harms to American children. I look forward to hearing from our witnesses on how we can ensure that parents have the tools necessary to safely guide their children through their online activities.

Mr. Berkman, video games are a part of daily activities for many families in New Jersey and across this Nation. While many view

these games as merely toys, the truth is that many video games have become fully functioning social networks.

For years, the gaming industry has defaulted to open communication, letting anyone talk to anyone. That is why I introduced the Safer GAMING Act. My bill requires that for minors the default setting must be the safest one, meaning voice and text chat with strangers is turned off until a parent turns it on.

Can you discuss how minors are using social gaming platforms and the risks to minors using these platforms?

Mr. BERKMAN. Thank you very much for the question, Congressman.

We believe that these types of gaming platforms that you call "social gaming," they are social media. They are a space where children and adults can go on, meet other people on the platform, and exchange content in the gaming situation, context—video and text mainly.

And so, because of that, we see the same risks, essentially, that we see on other types of social media platforms: severe cyberbullying, sextortion, sexual predation, abduction as well. So there is a full range of very serious risks here.

Mr. KEAN. So, as a followup to that, we know that predators often use the shared interest of a video game to build trust with a child. The statistics show that about two-thirds of minors say that an online-only contact has asked them to move from a public chat into a private conversation on another platform.

How would the default safeguards in my bill, which limit communication with strangers automatically, disrupt that cycle before it even starts?

Mr. BERKMAN. Well, the short answer is, it is as effective as you can get with a legislative change to mitigate this threat. If we are removing the ability for adults to contact minors over gaming platforms, that is almost entirely effective in terms of mitigation.

And let's be clear: When children go on these gaming sites, they are spending anywhere from 20 minutes to many hours, to many hours a day, over months, with adults that they do not know in real life. That is a lot of time for adults with malintent to spend with a child and conduct that grooming process.

We saw in April, I should note, in April, a 10-year-old abducted after using the gaming platform Roblox. This is an active, serious threat.

Mr. KEAN. Thank you, Mr. Berkman.

Mr. Thayer, the data is alarming. Nearly 70 percent of teens report they are playing online games with strangers at least weekly, and three-quarters of players have experienced harassment in these games.

My bill takes an important step to address that. The Safer GAMING Act says if a user is under 18 they should not be participating in chats, particularly with adults, unless a parent explicitly allows for it.

Mr. Thayer, what harms can arise when every teenager playing an online video game automatically has an open communication line to a random adult stranger?

Mr. THAYER. Well, Congressman, the short answer is too much.

And I think you have seen that even outside of your typical game that you see on Xbox or PlayStation. You see it even on mobile apps. I mean, this has been a longstanding problem with mobile apps in particular.

Pokemon GO, for instance, was a hot-button game, and it actually indirectly—or, actually, directly led kids to the predators' hands. Because the whole point of the game was to go into public areas and go find Pokemon, which—guess who picked up kids like that and also tracked kids with, you know, Pokemon?

So, again, this is a longstanding issue. It has been something that has been strategically, maybe even categorically, ignored by the tech companies, and maybe it is time for a lot of congressional oversight and legal oversight.

Mr. KEAN. All right.

And I thank our entire panel for being here today and for your insights.

I yield back.

Mr. BILIRAKIS. The gentleman yields back.

Now I will recognize Representative Clarke from the great State of New York for your 5 minutes of questioning.

Ms. CLARKE. Good afternoon, and thank you very much, Mr. Chairman. I thank our Ranking Member Schakowsky for holding this hearing.

And thank you to our witnesses for joining us today.

Earlier this year, in March, the subcommittee held a hearing titled "Examining Online Harms" with the expectation to discuss how Congress can help protect children from online harms. That hearing was derailed when, in the days leading up, Donald Trump attempted to illegally fire the Democratic Commissioners of the FTC, the very agency tasked with protecting kids and adults online.

The FTC has a long, bipartisan history of working to protect children online through their enforcement of the Children's Online Privacy Protection Act, the FTC Act, and their rulemaking authority. But since March, the FTC has been unable to do its job in good faith and maintain its historic role as a bipartisan, independent cop on the beat.

As I said to this committee 9 months ago, I am curious how Mr. Trump and my Republican colleagues think the firing of Democratic Commissioners furthers the mission of the FTC to protect kids online and the public from deceptive or unfair business practices. If my colleagues, my Republican colleagues, are serious about protecting kids from online harm, we should all be able to agree today that Rebecca Slaughter should be reinstated to the FTC.

But, unfortunately, my colleagues on the other side of the aisle are not serious about this topic. And that is why they continue to entertain the idea of a moratorium on State AI laws, even after it was defeated 99 to 1 in the Senate. In 2025 alone, all 50 States introduced legislation on AI, while Republicans in Congress offered no Federal alternative other than preemption. It is no mistake that the only Republican proposal frees AI and Big Tech companies from all oversight.

Without a comprehensive Federal standard, existing State laws are the only legislation keeping kids safe online right now. Without

a comprehensive Federal online data privacy law, all of these attempts at protecting our children online will be in vain.

Today's legislative package is missing the mark.

The State laws include State bills like the AI companion law in New York that clearly and regularly notify users that they are not interacting with a human and detect signs of self-harm and can direct users to crisis resources.

Any kind of broad preemption or moratorium on existing AI State legislation would kneecap the important work States like New York have already done to protect kids.

Instead of talking in circles and restating the obvious, today I encourage my colleagues to finally act. Demand the reinstatement of Commissioner Slaughter. Demand the exclusion of an AI moratorium in must-pass legislation. Demand that Donald Trump stop giving handouts to Big Tech. And let Congress do our job to protect kids and adults online with comprehensive legislation.

As I look out at the many families representing their loved ones here today, I find today's hearing extremely vexing. My staff has noted that this committee has had at least 5 hearings on the threats to kids online over the past 5 years. This is ridiculous.

It is time for us to act, colleagues. Every moment that we sit here restating the obvious, children and our families are at risk.

With that, Mr. Chairman, I yield back.

Mr. BILIRAKIS. The gentlelady yields back.

I now recognize Mrs. Houchin for her 5 minutes of questioning.

Mrs. HOUCHIN. Thank you, Mr. Chairman, and the ranking member for holding this hearing today and for the bipartisan work reflected in today's hearing.

I thank the witnesses for being here and for offering your testimony.

The importance of this work is impossible to overstate, because behind every policy choice are families who are living with the consequences.

I have been deeply moved by the parents, some of whom are here today, who despite losing a child continue to fight for stronger protections so no other family has to experience the same tragedy. Their experience brings an urgency and a clarity for policymakers, and we owe it to them to turn that into meaningful change.

Every parent I talk to is doing everything they can to guide their kids and protect them online, on social media, through gaming platforms, and now AI. And they are simply overwhelmed and cannot keep up—policymakers can barely keep up—with the advance in technology.

So this Congress we are recognizing how quickly the risks are evolving. I worked to launch the bipartisan Kids Online Safety Caucus so Members can stay current and engage with parents, researchers, schools, and industry.

I am also proud that today's hearing includes bills that I have been working on—the AWARE Act, the SAFE Bots Act, and the RESET Act, as well as the Parents Over Platforms Act, which I am helping colead with Representative Auchincloss.

Kids deserve the same safety mindset online that we have with car seats and playgrounds and other harms. The bills today reflect that approach.

The AWARE Act gives parents and educators clear, accessible guidance on how chatbots work, what red flags to look for, and where to go to for help.

The SAFE Bots Act ensures no AI system can impersonate a licensed professional and requires age-appropriate disclosure so kids always know that they are talking to software, not a human being.

The RESET Act asks whether 13 should still be the standard, the age of internet adulthood. Given that research shows the highest risks for social media harms fall below the age of 16, this bill creates a bright line and a national rule that platforms may not maintain accounts for users under 16. They must delete known under-16 accounts and their data and must follow a single standard enforced by the FTC and State's attorneys general.

The legal and global trends point in the same direction. Protecting minors from high-risk digital environments is both necessary and clearly permissible and possible. Our job is to learn from these developments so we can set guardrails worthy of the moment, and I look forward to working with colleagues on both sides of the aisle to accomplish that.

I do have a few questions with the remaining time that I have. I am going to go to Mr. Thayer.

We have heard a lot of concerns raised about the First Amendment relative to some of these bills. The 11th Circuit decision on H.B. 3, the Florida legislation, emphasized that States can act decisively to protect minors from harmful digital environments even when platforms claim editorial rights.

Does that signal, in your view, that Congress can likewise adopt RESET's type of bright-line Federal standard—under-16 account prohibition and deletion—without triggering First Amendment concerns that Big Tech continues to raise?

Mr. THAYER. Absolutely.

So the 11th Circuit, as you rightly noted, did uphold a law that was somewhat similar to what you are describing. And just to reiterate what the ruling basically said, which was just a rehashing of what was said in the Supreme Court in *TikTok* v. *Garland*, it essentially said that—the court basically clarified that a law has to be based off of what it is attempting to regulate.

If the regulation is attempting to regulate something that is a nonspeech-related thing, even if the ancillary aspects of that regulation does impact speech, it is likely going to be content-neutral, with some provisos.

So I think that what the 11th Circuit did was clarify something that the Supreme Court has said. And I think it would be very wise to heed that guidance and move forward accordingly.

Mrs. HOUCHIN. Thank you.

We have talked some today about preemption. I just want to note that we do seek a Federal standard so that States cannot go below—I certainly wouldn't want a State like California, who has a 13-year-old standard.

So, if we are talking about preemption, I think we have to be cognizant that, if there are—we want the States to be nimble, but we also don't want them to go below a standard set federally that we have determined will protect kids. Otherwise, we might as well not do this work and just leave it up to the States.

Protecting children in the digital age is one of our most important responsibilities that we have as elected leaders. It is clearly one of the most important moral responsibilities we have as parents. AI is not going away. Social media is not going away. It is our obligation to defend and protect the innocent and the next generation.

Thank you, Mr. Chairman. I yield back.

Mr. BILIRAKIS. I thank the lady for all her good work on this issue.

I next will recognize Representative Evans for his 5 minutes of questioning.

Mr. EVANS. Thank you, Mr. Chairman, Ranking Member, and, of course, to all of our witnesses for coming.

My first question will be to Mr. Berkman.

Before I came to Congress, I spent over a decade as a cop in the Denver metro area, and I saw the fentanyl crisis grow in my State and across the country. In 2023, Colorado had the second-highest overdose rate in the Nation for teenagers, and 75 percent of that was attributed to fentanyl. Earlier this year, we had the sixth-largest fentanyl seizure in U.S. history happen on the south side of the Denver metro area—6.8 million lethal doses of fentanyl in that seizure.

And we know a lot of this stuff is trafficked to our kids through things like social media. So, to counter this threat, one of the bills that I am carrying is the No Fentanyl on Social Media Act, which seeks to address this problem by assessing the full scope of how social media is used to be able to traffic fentanyl to our kids.

Can you discuss the role of social media in trafficking drugs and how this piece of legislation can help to resolve that issue?

Mr. BERKMAN. Yes. Thank you for your legislation. We enthusiastically support it, and we need it.

Children are acquiring drugs over social media. The accessibility is astonishing. This is not the situation that we had presocial media in terms of accessibility. They are able to get on, quickly connect with a drug dealer, sometimes one that they don't know. There is solicitation happening with regularity to teens. They are able to conduct a drug transaction and then have drugs delivered to their door like a pizza. This is the tragic story of what happened to 16-year-old Sammy Chapman as well.

I will note, this is also happening cross-platform, which is a safety concern, where drug dealers can advertise on one platform, conduct a conversation and transaction on another, and then receive payment on yet another. That is a very severe problem.

So we need your bill to understand the full facet of how this is happening, the features that are enabling it to happen, as well, and go undetected.

Mr. EVANS. Online games with a chat feature—I mean, again, I saw it during the course of my career.

This is for a situation—what we just discussed—the situations where somebody is potentially looking to go buy drugs, that is their intent. Can you talk a little bit about storefront apps, where maybe somebody is not actually looking to go buy drugs, they just bought a painkiller that they thought was legitimate, but it ends up being counterfeit and so then, when they consume what they thought was

a legitimate product, they end up dying of an overdose because it was an illicit or a fraudulent pill?

So can you just talk about how policy solutions like what we are discussing today can be used to fix some of the storefront nature of these apps, where people are buying something they think is legit but ends up being fraudulent?

Mr. BERKMAN. With the focus of this hearing on children, I will focus on children there. We see this happening with children. And, again, Sammy Chapman thought that he was buying Xanax over social media. I wish I could name all the parents and children here and honor them. That is the case with a lot of the parents here as well.

And so legislation like Sammy's Law would help protect against a child that is otherwise bored trying to go out and get something like Adderall, Xanax, Vicodin, which we are now seeing being poisoned with fentanyl and being lethal. And that education and awareness needs to spread as well. But Sammy's Law is a very strong deterrent to that behavior.

Mr. EVANS. Thank you.

And then a final question here. In your comments, you talked about some of the other harms that come from kids on social media. We have talked a lot about drugs. As a cop, I unfortunately had many situations where I interacted with kids being human trafficked over the internet and over social media.

And for me as a cop, probably the most shocking statistic, once I really got into this space, was understanding that a lot of times this trafficking happens within a half a mile of these kids' home. It is done through peer pressure over social media. And then the exploitation, whether it is digital, whether it is sexting, whether it is an actual in-person encounter—I mean, it can happen in their own home. I had one girl, 14 years old, that was repeatedly trafficked in her own basement through social media and online peer pressure.

So can you just talk about things that this committee can do legislatively to be able to put guardrails around situations like that? Twenty seconds.

Mr. BERKMAN. Yes. trafficking, sextortion—our children are no longer safe in their homes. That includes cyberbullying as well, which does not end at the end of the school day.

And so there are a range of solutions on here. I have 5 seconds. Let me highlight Sammy's Law once again. All the dangers that you mentioned, a parent would get an alert as that risk is imminent and occurring so that they could provide immediate, lifesaving support.

Mr. EVANS. Loop in the parent. Sounds good.

I yield back, Chairman.

Mr. BILIRAKIS. The gentleman yields back.

I now recognize Mr. James from the great State of Michigan for his 5 minutes of questioning.

Mr. JAMES. Thank you, Mr. Chair. And, first, I want to express my sincere gratitude to you and Chairman Guthrie for your leadership in organizing this amazing hearing.

I also appreciate all our distinguished panelists for being here today. I look forward to hearing from your insight, and I have been enjoying your feedback thus far.

I have said for years Facebook is the Philip Morris of our time. Yet they are just one example of the cesspool that is the modern internet. Americans are waking up to Big Tech's game. They provide lip service on how they are protecting children while actually delivering none of those protections.

Social media has been labeled the primary culprit, and for good reason. Countless studies and multiple congressional hearings make clear that social media is not only an addictive service for children but is also harmful for their mental acuity and overall mental health.

The damage social media is doing to our kids is unconscionable and extremely disturbing. Big Tech is knowingly and willingly wreaking havoc on our kids' mental health. As a father of three school-age boys, the warning signs of social media's impact on kids are abundantly clear to me and to all parents.

My bill, H.R. 3149, the App Store Accountability Act, ensures that children are not accessing age-restricted material through online app stores and gives parents real control over what their kids can download.

In fact, a national poll commissioned by Digital Childhood Alliance found that 88 percent of parents want app stores to require parental approval before minors can download a new app. Eighty-eight percent. Can you imagine any other issue that 88 percent of Americans agree on? We have printed 83 letters just today from parents and groups who agree.

Just as brick-and-mortar stores are held responsible for selling age-restricted materials like tobacco or alcohol to minors, the App Store Accountability Act will hold digital app stores accountable for providing adult or addictive material to minors as well.

Kids cannot consent. I say again: Kids cannot consent. And any company that exposes them to adult or addictive material should and will be held accountable.

The App Store Accountability Act holds Big Tech companies to the same standard as local corner stores. It protects the next generation by empowering parents now and making clear that, when it comes to safeguarding our children, no one gets a free pass.

My time is limited, so I will get right to it.

Mr. Thayer, as excited as I am to lead this App Store Accountability Act, I do want to share, the logic is very simple: App stores are a gateway to the internet, for social media, for our children.

You have played a very critical role in shaping similar legislation at the State level. Can you state one more time why placing the burden to verify a user's age on the app store, rather than on individual websites or apps, is the most efficient and privacy-protective way to ensure online safety for kids?

Mr. THAYER. Well, thank you, Congressman, for all of your work on this. You have been a real champion, and it has been an honor and privilege working with you and your staff.

Actually, I think who said it better was Congressman Obernolte themselves. They have the data already. They already have all of

the access to this information. And not only that, they already are developing the tools currently.

So, in the States, we got, I think, three States to subscribe to the App Store Accountability Act and pass it. Texas is among them. And, as a result, it actually forced Apple to create the API that would be necessary in order to accomplish all of this.

As you say, this is a very simple idea: Leverage the existing infrastructure to do an amount of good. And at the end of the day, they are the ones calling themselves a store, not us. So if they want to be a store, we should hold them to the same accountability as any other store in any other market.

It is absurd that merely because you put electrons into a store it is somehow magically new. No. They know what they are selling, they know what is on their product, and, most importantly, they know the age of their user better than any other company in the world.

Mr. JAMES. That is exactly right.

And maybe you could help me to respond to some of—I won't say the "critics," but those who may not know the intent or the details of what we are trying to do here. Can you help explain a little bit differently privacy concerns that some may rise?

Mr. THAYER. So I actually don't have to, because Apple itself has said that they can actually do all of this in a privacy-conscious way.

So, to be clear, all the Act is really requiring Apple and Google to do is to share an API that is encrypted. And they do this on multiple different layers, not just on—not just to verify age, but actually they have done it—every time you do a financial transaction, that is an API. That is an API that is connecting with some other app that says, "Hey, the transaction has gone through."

Apple and Google act as the direct not only the intermediaries, but they are basically the brokers to all of these issues. And they have been able to say with a straight face that they can do so—privacy—and put all the safeguards in place. All this Act does is hold them accountable to what they tell the American population. That is it.

Mr. JAMES. Thank you, Mr. Thayer.

Thank you, Mr. Chairman. My time has expired.

Mr. BILIRAKIS. Thank you.

The gentleman yields back.

Now, Dr. Joyce, you are recognized for your 5 minutes of questioning.

Mr. JOYCE. Thank you, Mr. Chairman.

Today's hearing is an important step toward protecting our children from the harms of social media. And I want to personally thank Chairman Bilirakis and Chairman Guthrie for their tireless work to protect the most vulnerable among us.

Two weeks ago, the Oversight subcommittee held a hearing on the risks of AI chatbots and the way that these platforms can be improved to keep children safe. As new technologies like AI chatbots are deployed online, we must honestly evaluate the potential benefits and risks and enact operational, futureproof safeguards that will protect current and future generations.

So I welcome the opportunity to learn more about the proposals before us today and how they can achieve our shared goal of protecting children online.

Mr. Lekas, the Don't Sell Kids' Data Act is predicated on the view that data practices of third parties are inherently harmful to children and teens. Yet, while privacy protections are essential, not every use of data is harmful.

In your opinion, as drafted, could the Don't Sell Kids' Data Act bring about unintended adverse consequences for kids and teens?

Mr. LEKAS. Thank you for that question.

In my view, yes.

There are no exemptions in this law. And I think there is something that the general public doesn't understand, which is the many ways in which data is used behind the scenes actually provide us with benefits that we don't see, such as extending auto insurance to teenagers or enabling students to apply for financial aid or be scouted for college scholarships.

There is a range of positive uses that don't rely on social media data that we have been talking about today but they rely on data that actually is protected by other privacy laws—the FCRA and the GLBA and these laws that already provide a means to protect that data so it is only used for legitimate purposes.

Mr. JOYCE. Continuing, Mr. Lekas: The Don't Sell Kids' Data Act includes private right of action to enforce that bill. And in your written testimony, you state that effective enforcement "should be designed to improve privacy and safety practices" and that "enforcement shouldn't be watered down with private rights of action." That is a quote from your testimony.

Can you expand on that point and discuss how a private right of action could actually weaken enforcement and hurt consumers?

Mr. LEKAS. Happy to.

We have seen a number of instances across the country, in State laws especially, with private rights of action that lead to lawsuits that are based on statutory violations even if there is no showing of harm. And the impact of this—there's a number of impacts that result from this.

One is that it causes firms to act in a more defensive posture. They are trying to minimize their legal risk rather than actually trying to fulfill what their duty is to their consumers or their users or, in some cases, as in here, the youth.

And another thing is it drives up costs, especially legal and compliance costs. Particularly hardest hit are the smallest firms—startups, small, medium-size enterprises.

Mr. JOYCE. Could this deter those small startups, those small firms, from entering into the market?

Mr. LEKAS. It very well could. There have been a lot of studies done on this about the actual economic costs on companies based on privacy laws. There is a law in Illinois called BIPA which has been particularly notable in this regard.

So we want meaningful—we want meaningful enforcement and accountability, but we want that enforcement and accountability to lead to change where we need change and for there to be a recourse for individuals who are truly harmed by practices.

And so that is why we would recommend in some of these children-focused laws to really home in on FTC and AG enforcement.

Mr. JOYCE. Thank you.

Mr. Thayer, many proposals rely on age-verification technology. Some have critiqued age verification as violating privacy and age-gating the internet.

What advances in age-verification technology give you confidence that we can effectively verify users' ages accurately while at the same time protecting their privacy?

Mr. THAYER. Well, in short, many.

So you saw this play out in the Supreme Court in the *Paxton* case, where part of the assessment that the Court was grappling with was not just the content that was at issue but also the technological advances since the last time they evaluated this, which I believe was in, like, 1996 or 1992. And the internet has completely changed, right? I mean, with the amount of—the sheer amount of data that we give these companies has completely altered the landscape.

And now you have vertically integrated systems like Apple and Google's systems, for instance, where Apple and Google both own not only the device, they own the operating system, they own the app store, and they even have their own native apps.

So the idea that, you know, somehow they know exactly when you go to the bathroom and what you want to eat but yet your age confounds them, like, is a bit of a ridiculous and almost outdated view.

Mr. JOYCE. My time has expired.

Mr. Chairman, again, I thank you for holding this important hearing, and I yield back.

Mr. BILIRAKIS. Thank you, Doctor. Appreciate it very much.

Now I will recognize last, but certainly not least, Dr. Miller-Meeks for her 5 minutes of questioning.

Mrs. MILLER-MEEKS. Thank you, Chairman Bilirakis and Ranking Member Schakowsky, for allowing me to waive on to this important hearing.

I also want to thank our witnesses for being here today.

Protecting children and teens online is one of the most urgent responsibilities we face as policymakers. As digital platforms become central to how young people learn, communicate, and navigate the world, and, importantly, how much they trust these platforms, we must ensure that these spaces are safe, transparent, and designed with their wellbeing, not corporate profit, as the driving priority.

And to one of the witness's points, it is astonishing to me that we can build computers, build platforms, build apps all through a digital world, but somehow Casey's General Store can verify your age no matter how old you look, but a digital platform that has this remarkable innovation can't verify an age when inappropriate apps or content is accessed.

So my bill, the SPY Kids Act, takes an important step towards that goal by prohibiting online platforms from conducting market or product-focused research on children under 13 and by requiring verifiable parental consent before such research can be conducted on teens.

After all, didn't the public-health community raise red flags about cereal companies marketing directly to children for the type of cereal that they would purchase? So it is not impossible that we do this.

This legislation matters because the online environment our children encounter today is fundamentally different from anything previous generations have experienced. Platforms are engineered to capture attention, collect sensitive information, and shape behavior in ways that young users may not recognize or be able to navigate safely.

Children and teens should not be profited, studied, or targeted for commercial advantage, especially without parental oversight. By limiting how platforms can analyze and monetize minors' data, the SPY Kids Act helps reduce the risk of manipulative marketing practices, strengthens privacy protections, and reinforces the principle that the wellbeing of America's youth must come before business models of technology companies.

Our goal is simple: to build an online ecosystem where children can grow, learn, and connect without being exploited in the process.

Mr. Berkman, before I came to Congress, I was a doctor and director of the Iowa Department of Public Health. The CDC recommended limits to screen time. And in the medical world, we have strict ethical rules about conducting research on children. You cannot just use a child in research without the parents' informed consent, even when it comes to drawing cord blood.

Yet it seems that Big Tech companies run tests and psychological experiments on our children every single day to see which color or sound keeps them addicted the longest.

In your view, what are the most pressing risks minors face from being profiled or studied for commercial purposes online?

Mr. BERKMAN. Yes, I would refer the Members to the former Surgeon General's advisory on mental health. First of all, the longer our children are online, the more at risk they are for adverse mental health outcomes, including suicide. They are also more at risk for all the acute harms that we see through social media: cyberbullying, sextortion, and trafficking as well.

So innovation in the social media industry means, "How many features can we design to get our children to use the social media platforms more?" Our children's time is their profit.

Mrs. MILLER-MEEKS. Thank you.

Mr. Thayer, how can behavioral research targeting minors be used to shape features that may increase addictive or manipulative design patterns?

Mr. THAYER. Well, we are seeing it play out in realtime. I mean, Big Tech's big experiment on our kids is evidence of that.

Not to mention, as Congressman James noted, there is an immense amount of research that demonstrates that these addictive behaviors will actually manifest in multiple different ways even outside of the use of the app. So, even after the app is long turned off, they are still susceptible to all of the harm that has been caused based off of the repetitive nature of the videos, based off of the inundation of all the materials and even the features themselves, which happens not just at the app layer but at the app store and the operating system.

These devices, on the whole, are designed to keep you addicted and designed to keep you—I guess the kids don't call it this anymore, but it is called FOMO. And so, ultimately, if you take—I mean, just ask any parent who has ever taken a tablet or phone away from a child. I mean, you will recognize that these kids do not look like themselves after that. They act a lot like your average drug addict.

Mrs. MILLER-MEEKS. Right. I have seen it in my doctor's office with both the parents and with children.

Thank you so much.

With that, I yield back.

Mr. BILIRAKIS. The gentlelady yields back.

All right. So we have finished with questioning. However, now I would like to recognize Representative Castor.

Now, I will tell Representative Castor that the documents that she is going to propose have already been submitted for the record, but you are recognized to elaborate on that if you would like.

Ms. CASTOR. Well, thank you very much, Mr. Chairman, for adding to the record a past KOSA letter of 10/15/25 from 408 organizations in all 50 States calling on House and Senate leadership to pass the Senate version of KOSA.

Also, a parent letter to Congress of November 24th. It is a letter from over 300 parents to the House Energy and Commerce urging them to pass the Senate KOSA and stand strongly against the demands of the tech industry to gut this and other children's online privacy and safety legislation.

The Common Sense Media opposition letter of December 1st opposing these versions of KOSA and COPPA 2.0.

And the ParentsSOS KOSA 1-pager of December 1st, a coalition of over 20 families who have lost their children to online harms, with significant concerns about the House Republican KOSA draft.

Mr. Berkman mentioned the U.S. Surgeon General's advisory of 2023. It is very important that that is in the record.

The 2023 American Psychological Association advisory examining the potential beneficial and harmful effects of social media, including 10 recommendations based on scientific evidence.

The Pew Research Center report on teens, social media, and mental health of 2025 saying that roughly one in five teens say social media sites hurt their mental health and a growing share think that they harm people their age.

Also, the 2024 Federal Trade Commission report, "A Look Behind the Scenes." That is the detailed report finding large social media and video-streaming companies have engaged in vast surveillance of users, with lax privacy controls and inadequate safeguards for kids and teens.

The Design It For Us letter of December 1st, 2025. Several organizations, led by Design It For Us, in support of a strong KOSA; in opposition to a Federal provision that would undermine existing State protection for kids.

And the Senate Judiciary hearing materials. If you haven't read through the whistleblower materials or the transcripts and the questions, that would be very edifying for legislation.

And the master complaint in the Meta lawsuit, 2025.

And "Teen Accounts, Broken Promises: How Instagram Is Failing to Protect Minors," the 2025 Fair Play report on the weaknesses of Meta's teen accounts, spearheaded by a whistleblower and verified by university researchers.

Thank you for including these in the record today.

Mr. BILIRAKIS. Absolutely.

I ask unanimous consent that the documents on the staff documents list be submitted for the record. If I don't hear any objections, so ordered.

[The information appears at the conclusion of the hearing.]

Mr. BILIRAKIS. OK, folks. Thank you very much.

Again, I remind Members that they have 10 business days to submit questions for the record. And I ask the witnesses to respond to the questions promptly. Members should submit their questions by the close of the business day on December 16th.

And I would like to thank everyone for being here today. The testimony was excellent. I thought it was a great hearing.

And I want to thank the parents—the parents that are here today on behalf of their children and other children. We appreciate you so very much, and the personal stories definitely do matter.

So, without objection, the subcommittee is adjourned.

[Whereupon, at 1:10 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

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.[1]
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 FabrizioWard.
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.

[1] The information has been retained in committee files and is included in the Documents for the Record at https://docs.house.gov/meetings/IF/IF17/20251202/118714/HHRG-119-IF17-20251202-SD003.pdf.

Minority

1. Letter from various organizations to Chairman Guthrie and Ranking Member Pallone.
2. Letter from various parents to Speaker Johnson, Minority Leader Jeffries, Chairman Guthrie, Ranking Member Pallone.
3. Letter from AAJ in opposition to KOSA and COPPA.
4. Letter from Apple to Chairman Bilirakis and Ranking Member Schakowsky.
5. Letter from California Privacy Protection Agency to Chairman Guthrie, Ranking Member Pallone, Chairman Bilirakis, Ranking Member Schakowsky.
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).[1]
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".[1]
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".[1]

[1] The information has been retained in committee files and is included in the Documents for the Record at https://docs.house.gov/meetings/IF/IF17/20251202/118714/HHRG-119-IF17-20251202-SD003.pdf.

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

P.O. BOX 34300 □ WASHINGTON, D.C. 20043 □ (202)488-7000
CONCERNEDWOMEN.ORG

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

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.

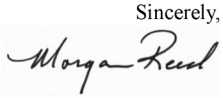
Conclusion

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://cppa.ca.gov/pdf/enfadvisory202401.pdf

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

Sincerely,



Morgan Reed
President
ACT | The App Association

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.

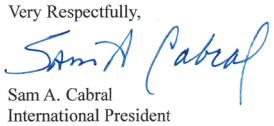
Support for this legislation is strong throughout the law enforcement community. In addition to the International Union of Police Associations, the following organizations stand united in urging action:

- 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 Comme'ns & 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-$120,000[3]—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 startups[5] (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 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: 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.R3149 / 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,

Erich Mische
Chief Executive Officer
SAVE

FabrizioWard

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 ±3.1% at the 95% confidence level. The margin of error for parents is ±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

LATINOS FOR TENNESSEE

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,

Hilary Ware
Global Head of Privacy
Apple

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

OpenAI

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

OpenAI

1455 3rd Street
San Francisco, CA 94158

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,

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

NetChoice

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

cloaked

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,

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 identity[1]. 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 suicide[2]. 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

[1]Documentation 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 care[3], and the bill's own sponsor explicitly states its goal is preventing the "indoctrination" of children with transgender content[4], 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 Amendment[5].

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 rejected[6].

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 moderation[7]. 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-conten-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 care[8], and the 45% who face barriers to parental consent for services[9] 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 locally[10]. 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

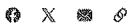
Beginning January 1, 2026, a new state law in Texas — SB2420 — introduces age assurance requirements for app marketplaces and developers. While we share the goal of strengthening kids' online safety, we are concerned that SB2420 impacts the privacy of users by requiring the collection of sensitive, personally 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.



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

112 3108

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

122 3237

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

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

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 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 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 Hakeen Jeffries
House Energy & Commerce Committee
House Energy & Commerce Committee Subcommittee on Commerce, Manufacturing, and Trade

ALABAMA POLICY INSTITUTE

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.

ALABAMA POLICY INSTITUTE

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,

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 Dexton, 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 Moliie, 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
Dondee, 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 Alexus 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 Dexton, 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,

Hilary Ware
Global Head of Privacy
Apple

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

STATE OF CALIFORNIA

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.

- **Heighted 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

---

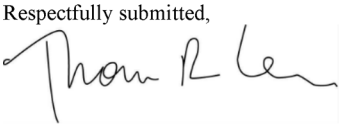
[6] Cal. Civ. Code § 1798.100 et seq.
[7] Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, Oregon, New Hampshire, New Jersey, Rhode Island, Tennessee, Texas, Utah, and Virginia. *See*, IAPP, US State Comprehensive Privacy Laws Report: 2024 Legislative 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,



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/

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

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.

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

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

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

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

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
Whitington 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

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

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

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

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

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

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

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

ParentsSOS
PARENTS FOR SAFE ONLINE SPACES

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.

ParentsSOS
PARENTS FOR SAFE ONLINE SPACES

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.

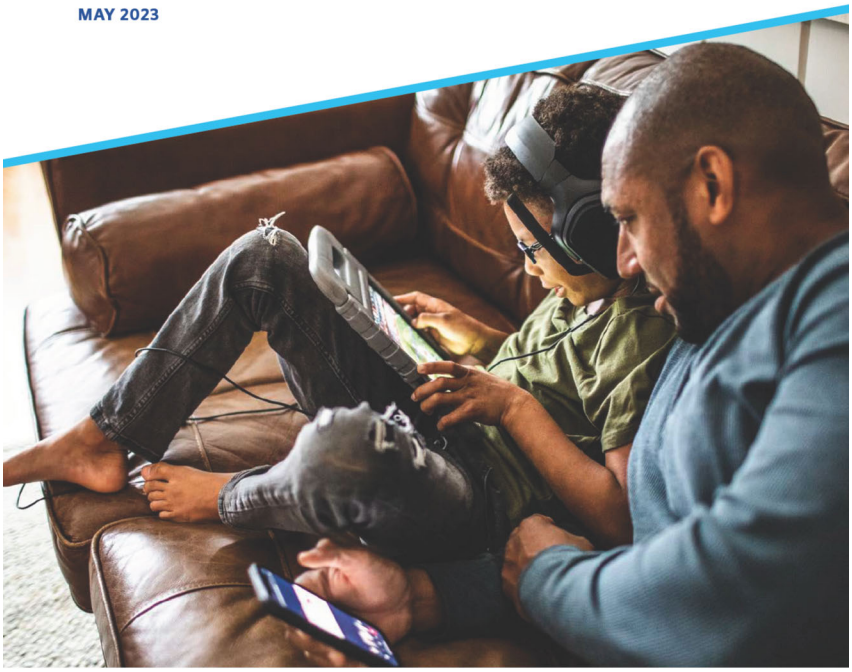
The House's decision to introduce a large package of bills, including many discussion drafts and bills that do not have Senate companions, will further delay what families have been asking of Congress for years: Real accountability to protect children online. **ParentsSOS is asking members of the Commerce, Manufacturing and Trade Subcommittee to support a strong KOSA that has a Duty of Care and no federal ceiling preemption.**

AMERICAN PSYCHOLOGICAL ASSOCIATION

AMERICAN PSYCHOLOGICAL ASSOCIATION

Health Advisory on Social Media Use in Adolescence

MAY 2023



Copyright © 2023 by the American Psychological Association. This material may be reproduced and distributed without permission for educational or research purposes provided that acknowledgment is given to the American Psychological Association. This material may not be translated or commercially reproduced without prior permission in writing from the publisher. For permission, contact APA, Rights and Permissions, 750 First Street, NE, Washington, DC 20002–4242.

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.

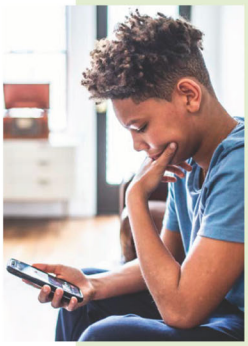
- Brain regions associated with a desire for attention, feedback, and reinforcement from peers become increasingly sensitive beginning in early adolescence, and regions associated with mature self-control are not fully developed until adulthood.[5] Parental monitoring (i.e., coaching and discussion) 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 removed[23]; moreover, technology should not drive users to this content.

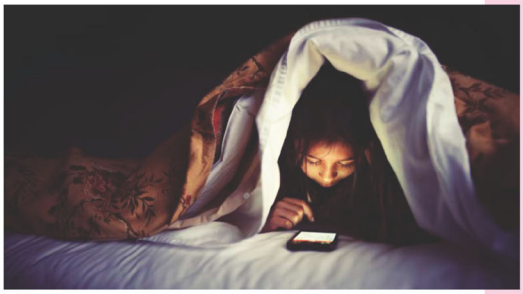
- Evidence suggests that exposure to maladaptive behavior may promote similar behavior among vulnerable youth, and online social reinforcement of these behaviors may be related to increased risk for serious psychological symptoms, even after controlling for offline influences.[24]
- Reporting structures 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.

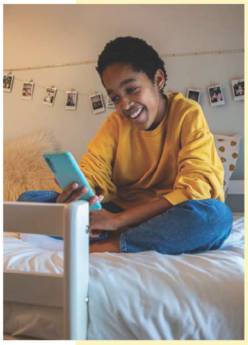
- Research recommends adolescents get at least 8 hours of sleep each night and maintain regular sleep-wake schedules.[32] Data indicate that technology use particularly within 1 hour of bedtime, and social media use in particular, is associated with sleep disruptions.[33,34] Insufficient sleep is associated 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 online[47]; 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 "misestimation" 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

1. 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
2. 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
3. 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
4. Valkenburg PM, Peter J. The differential susceptibility to media effects model. *J Commun*. 2013;63(2):221-243. doi:10.1111/jcom.12024
5. 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
6. 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
7. Magis-Weinberg L, Ballonoff Suleiman A, Dahl RE. Context, development, and digital media: implications for very young adolescents in lmics. *Front Psychol*. 2021;12:632713. doi:10.3389/fpsyg.2021.632713
8. 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
9. Noble SU. *Algorithms of Oppression: How Search Engines Reinforce Racism*. NYU Press; 2018. doi:10.2307/j.ctt1pwt9w5
10. 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
11. 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
12. 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
13. 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
14. 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
15. 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
16. 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
17. 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
18. 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
19. 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:10.1080/15374416.2020.1750019
20. 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
21. 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
22. 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
23. 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.
24. 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
25. 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.2014.3232

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. Cantaro-Pulgarín SA, Suárez-Betancur N, Vega MB, López HMH. 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;14:16–72. 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-Rodriguez ME, Ramer JD. Unlocking the promise of physical activity for mental health promotion. *JAMA Pediatr*. 2023;177(2):111–113. doi:10.1001/jamapediatrics.2022.5196

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;51:2–10. 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, Cerrigli 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

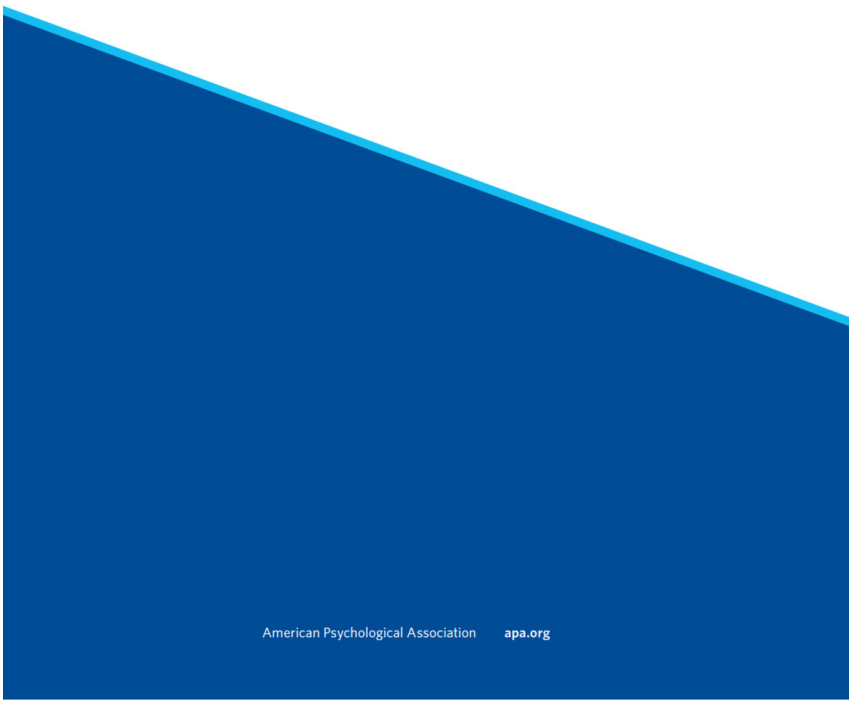
45. Kleemans M, Daalmans S, Carbaat I, Anschütz D. Picture perfect: the direct effect of manipulated instagram photos on body image in adolescent girls. *Media Psychol*. 2016;21(1):1–18. doi:10.1080/15213269.2016.1257392

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.12007

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 Peru (a pilot quasi-experimental study). *Child Adolesc Ment Health*. 2022;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


American Psychological Association apa.org

WHISTLEBLOWER AID

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.

WHISTLEBLOWER AID

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,

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

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.

WHISTLEBLOWER AID

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.

WHISTLEBLOWER AID

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.

WHISTLEBLOWER AID

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.

WHISTLEBLOWER AID

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:

WHISTLEBLOWER AID

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.

WHISTLEBLOWER AID

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

WHISTLEBLOWER AID

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

WHISTLEBLOWER AID

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.

WHISTLEBLOWER AID

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.

BRETT GUTHRIE, KENTUCKY
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED NINETEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115
Majority (202) 225-3641
Minority (202) 225-2927

December 22, 2025

Mr. Marc Berkman
CEO
Organization for Social Media Safety
6442 Platt Avenue, Suite 1914
West Hills, CA 91397

Dear Mr. Berkman:

Thank you for appearing before the Subcommittee on Commerce, Manufacturing, and Trade hearing on Tuesday, December 2, 2025, to testify at the hearing entitled, "Legislative Solutions to Protect Children and Teens Online."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached.

To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on Monday, January 12, 2026. Your responses should be mailed to Alex Khlopin, Policy Analyst, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to alex.khlopin@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Gus M. Bilirakis
Chairman
Subcommittee on Commerce, Manufacturing, and Trade

cc: The Honorable Jan Schakowsky, Ranking Member, Subcommittee on Commerce, Manufacturing, and Trade

The Honorable Russ Fulcher (R-ID) *Mr. Berkman, in 2020 AI was a background tool for companies. Today, it's everywhere on the user and customer side, especially with kids. It's prevalent in social media platforms they're on, the games they play and sadly, and even the so called "relationships" they form. The AI landscape is rapidly evolving, forcing parents and policymakers to scramble to keep up to ensure our vulnerable youth are safe. Mr. Berkman, what's the biggest gap between how fast AI is evolving and how slowly our policies are responding…what do you see are some of the biggest risks and issues that we are not addressing right now?*

Response for the Record (Marc Berkman, CEO, Organization for Social Media Safety)
Thank you for the question. To clarify the Organization for Social Media Safety's scope: we approach AI through a consumer-protection lens, particularly as it is deployed via social media, and so, we do not focus, at this time, on any broader existential or systemic risks regarding AI, including singularity, national security implications, or macroeconomic impacts.

As suggested in the question, AI features and products are being launched and iterated rapidly. Major changes to existing features accessed by millions of American children, including social media algorithms, chatbots, and synthetic media capabilities, can roll out with minimal public notice, and any resulting harms can scale immediately. Yet our public policy protections move more slowly than both this pace of technological development and its related risks. This creates a situation in which families alone bear the burden of protecting against risks that are unobserved, poorly measured, or poorly understood, even as AI features become widely adopted and more embedded in our children's daily lives.

The currently identified concerns include:

1. A rapidly growing risk category is AI systems that simulate relationships, trust, intimacy, or authority, often referred to as "social AI" or "chatbots." We already have evidence that chatbots are causing severe, acute harms, including the following reported cases:

    - Megan Garcia alleged that her 14-year-old son Sewell Setzer III fell victim to a chatbot that pulled him into what she described as an emotionally and sexually abusive relationship that led to his suicide in February 2024.[1]

    - The Raine family has alleged that another chatbot caused 16-year-old Adam Raine's death by distributing ChatGPT to minors despite knowing it could encourage psychological dependency and suicidal ideation. [2]

---

[1] Associated Press. (2026, January 7). *Google and chatbot maker Character to settle lawsuit alleging chatbot pushed teen to suicide.* AP News. https://apnews.com/article/ai-chatbot-lawsuits-character-google-fbca4e105b0adc5f3e5ea096851437de

[2] Tiku, N., & Schaul, K. (2025, December 27). *74 suicide warnings and 243 mentions of hanging What ChatGPT said to a suicidal teen.* The Washington Post. https://www.washingtonpost.com/technology/2025/12/27/chatgpt-suicide-openai-raine/

- In another case, a chatbot suggested violence against parents, and other self-harm content.[3]

- Another report alleged a young person sought repeated drug-use advice from a chatbot over time and later died of an overdose.[4]

- An internal Meta Platforms document detailing policies on chatbot behavior permitted the company's artificial intelligence creations to "engage a child in conversations that are romantic or sensual" and generate false medical information, among other concerns.[5]

- Another report found that AI chatbots are now encouraging dangerous weight loss and eating habits in teen users.[6]

We are particularly concerned about AI's long-term mental health risks for children. Chatbots may materially displace human interaction and affect children's social, emotional, and cognitive development.[7] One study has raised concerns that heavy reliance on ChatGPT-like tools may erode critical thinking in some contexts.[8] By the time these longer-term risks are properly understood, millions of children might have already suffered irreparable harm. Congress must play a role in ensuring that we develop a robust, fully funded infrastructure to study these risks so that developers, non-governmental organizations, and families can react with due speed in an evidence-based manner to protect children.

Furthermore, in January 2026, Google and AI chatbot maker Character Technologies agreed to settle a lawsuit from a mother who alleged a chatbot pushed her teenage son to kill himself.[9] We are concerned that with the settlement, these companies have avoided necessary scrutiny of risky operations and feature designs. With millions of child users and the massive potential scale of harm, Congress should consider sunshine in litigation legislation for AI-related lawsuits, that limits confidentiality provisions which conceal public safety hazards, to ensure that secret lawsuit settlements in this area do not become an avenue to hide clear and present

---

[3] Tiku, N. (2024, December 10). *An AI companion suggested he kill his parents. Now his mom is suing.* The Washington Post. https://www.washingtonpost.com/technology/2024/12/10/character-ai-lawsuit-teen-kill-parents-texas/

[4] Black, L., & Council, S. (2026, January 5). *A Calif. teen trusted ChatGPT's drug advice. He died from an overdose.* SFGATE. https://www.sfgate.com/tech/article/calif-teen-chatgpt-drug-advice-fatal-overdose-21266718.php

[5] Horwitz, J. (2025, August 14). *Meta's AI rules have let bots hold sensual' chats with kids, offer false medical info.* Reuters Investigates. https://www.reuters.com/investigates/special-report/meta-ai-chatbot-guidelines/

[6] Upton-Clark, E. (2024, December 6). *Character.AI is under fire for hosting pro-anorexia chatbots.* Fast Company. https://www.fastcompany.com/91241586/character-ai-is-under-fire-for-hosting-pro-anorexia-chatbots

[7] Xu, Y., Prado, Y., Severson, R.L., Lovato, S., Cassell, J. (2025). Growing up with artificial intelligence: Implications for child development. In: Christakis, D.A., Hale, L. (eds) *Handbook of Children and Screens*. Springer, Cham. https://doi.org/10.1007/978-3-031-69362-5_83

[8] Chow, A. R. (2025, June 23). *ChatGPT may be eroding critical thinking skills, according to a new MIT study. TIME.* https://time.com/7295195/ai-chatgpt-google-learning-school/

[9] The Associated Press. (2026, January 7). Google and chatbot maker Character to settle lawsuit alleging chatbot pushed teen to suicide. AP News. https://apnews.com/article/ai-chatbot-lawsuits-character-google-fbca4e105b0adc5f3e5ea096851437de

risks for children.

2. Social media platforms have used evidence of vulnerability or emotional fragility to target advertisements to teens, exacerbating depression, distress, eating disorders, body image issues, and self-harm, among other outcomes.[10] With more advanced AI systems in place, the ability to analyze our children's data has grown exponentially, and with that ability comes the opportunity for increased manipulation and exploitation of vulnerable youth. Congress needs to enact data minimization, limits on sensitive inference, and guardrails on profiling-based targeting, particularly where minors are foreseeable users.

3. Voice cloning, deepfakes, synthetic images, and highly targeted persuasion enable scams and coercion to scale faster than traditional enforcement models.[11] The FTC's September 2025 inquiry into consumer-facing AI "companion" chatbots underscores the growing concern about how companies test, monitor, and mitigate negative impacts on children and teens. The tools for deception are scaling faster than those for detection, deterrence, and remedy. We do applaud Congress for passing the Take It Down Act to protect against Intimate Imagery Deepfakes targeting minors.

4. Social media consumers cannot protect themselves from risks they cannot perceive, and right now, there is no consistent, enforceable requirement across social media platforms to clearly disclose when a user is interacting with an AI chatbot or avatar versus a real person.[12] Without upfront transparency, users, especially children and other vulnerable individuals, may share highly sensitive information, place undue trust in advice, or become emotionally reliant or emotionally dependent in ways they would have avoided had they known it was AI. This is a classic consumer-protection failure: the absence of clear disclosure prevents informed consent and blocks basic self-protective best practices. It also raises serious privacy and data-security concerns, because users may reasonably assume they are in a human-to-human exchange when their messages are instead being collected, processed, and potentially retained or used to train systems. Congress should require clear, conspicuous AI interaction disclosures and meaningful guardrails so people can make informed choices before harm occurs.

These are some, not all, of the AI-based risks that need more Congressional attention. Congressman, you also asked about what the *biggest* gap is between how fast AI is evolving and how slowly our policies are responding. We are concerned that the answer to that question may well be that the public lacks sufficient visibility into the largest AI risks that

---

[10] Wynn-Williams, S. (2025). *Careless People A Cautionary Tale of Power, Greed, and Lost Idealism.* Flatiron Books.

[11] L. S., Aslett, D., Mekonnen, G., & Zecevic, M. (2024). The dangers of voice cloning and how to combat it. The Conversation. https://theconversation.com/the-dangers-of-voice-cloning-and-how-to-combat-it-239926

[12] See Kenny R, Fischhoff B, Davis A, Carley KM, Canfield C. Duped by Bots: Why Some are Better than Others at Detecting Fake Social Media Personas. Hum Factors. 2024 Jan;66(1):88-102. doi: 10.1177/0018720821107264 2. Epub 2022 Feb 24. PMID: 35202549; PMCID: PMC11370216.

could cause mass harm, especially among youth. As discussed in my earlier testimony, given the durable conflicts of interest between safety and profits in the social media industry, we cannot trust the industry to conduct measured assessments of the risks associated with new features or capabilities, to mitigate appropriately for such risks, nor to alert the public to these risks in a responsible manner.

For the unknown risks and for the ones I just articulated, Congress should prioritize the following legislation:

- Pre-deployment and ongoing risk/impact assessments, with clear documentation of foreseeable harms and mitigations.
- Independent audits/evaluations for high-risk systems, not only internal testing.
- Stronger safeguards for AI chatbots, including heightened protections where minors are foreseeable users, and restrictions on under-18 access absent effective safety protocols.
- Meaningful transparency and disclosures so consumers know when they are interacting with AI and can understand the basis for personalization.
- Whistleblower protection for employees to alert the public to risks and unsafe business practices in the AI field.
- Funding for an ongoing, independent research infrastructure to identify, understand, and alert the public to any risks to children associated with AI features and products.
- Real enforcement and remedies when companies deploy systems that create foreseeable consumer harm or make misleading or inaccurate safety representations.

Since Congress can implement these common-sense measures without hindering American competitiveness in AI development, it must do so with expediency to protect a generation of American children from potential harm.

SIIA

January 15, 2026

The Honorable Gus M. Billirakis
Chairman
Subcommittee on Commerce, Manufacturing, and Trade
Committee on Energy and Commerce
U.S. House of Representatives

The Honorable Jan Schakowski
Ranking Member
Subcommittee on Commerce, Manufacturing, and Trade
Committee on Energy and Commerce
U.S. House of Representatives

Re: December 2, 2025 Hearing, "Legislative Solutions to Protect Children and Teens Online"

Dear Chairman Billirakis and Ranking Member Schakowski:

Thank you for the opportunity to testify before the Subcommittee on December 2, 2025, in the hearing "Legislative Solutions to Protect Children and Teens Online." I am writing to provide a written response to the one additional question for the record, submitted by Representative Russ Fulcher.

Question for the Record:

1. In your testimony, you noted the importance of "evidence-based" and "risk-proportionate" requirements, rather than "broad restrictions" when it comes to regulations on AI chatbots. I worry about the use of AI chatbots that incorporate Large Language Models (LLMs) that offer responses based on data fed to them to reinforce the behavior of the user that comes across as "personalized conversations." Tell me about your members' experience with the Federal Trade Commission (FTC) when it comes to working with social media companies, and the responsibility you all expect from those social media companies in ensuring the health and safety of children and teens? For example, do you see any updates on the work of "CHAT SAFE" to continue to improve health and safety for the FTC?

Response to Question for the Record:

Thank you for this thoughtful question. AI chatbots, like many technological innovations, have the potential to provide users with extraordinary benefits but also carry risks. On the positive side, chatbots offer opportunities for communication, learning, and innovation across every sector of society, providing people with accessible information tailored to their needs, level of background knowledge, and context. On the other hand, like other types of generative AI tools, chatbots carry a range of potential risks that developers and deployers seek, in varying degrees, to mitigate through governance. Most relevant to this issue are risks of misuse and misalignment in the context of companion chatbots.

The challenge for lawmakers, as explained in my testimony, is to craft measures designed to address the key concerns associated with chatbots without impeding the positive use cases. We recommend that lawmakers consider the suitability of measures in three categories.

The first focuses on governance. Industry-led approaches have a meaningful role to play in raising the bar on governance. The SIIA *CHAT SAFE Principles*, which will be published this month, will provide a framework for developers and deployers to protect youth safety when using AI chatbots, with guidance on disclosures, risk mitigation, accountability, trust, reliability, security, and privacy. This approach is designed to align safety and innovation. It also recognizes that there is a range of different applications for chatbots that pose different risk profiles. Chatbots that can serve as "companions" present a different risk profile than chatbots developed for specific and narrow purposes. In addition to serving as a framework for industry, the *CHAT SAFE Principles* will also serve as a guide for lawmakers about where to supplement industry efforts with legislation.

Legislation is most important to ensure that industry actors are acting responsibly. Companies should adhere to best practices, but not all do, and that is where Congress can step in. The approach taken by California SB 243, which was enacted late in 2025 and has already gone into effect, provides a model for legislation focused on governance. SB 243 directs AI developers to implement protocols, increase transparency, and include protections to address the concerns around AI chatbot safety. SB 243 avoids First Amendment concerns raised by bills that would impose content restrictions and avoid functioning as de facto bans by requiring AI chatbots to be free of risk.

The second category for lawmakers is to address discrete harms associated with chatbots that are not covered by existing law. This is the approach taken by the TAKE IT DOWN Act (TIDA), enacted in 2025 and set to go into effect in May 2026. TIDA addresses the growing threat of non-consensual intimate imagery (NCII), including deepfakes, by criminalizing the knowing publication of NCII, requiring platforms to take down NCII, and giving the FTC authority to regulate platform compliance under its unfair or deceptive acts or practices (UDAP) authority. SIIA supported TIDA because of concerns about the spread of NCII, especially AI-facilitated NCII, and a gap in the law.

Relatedly, lawmakers should take steps to ensure that governments are equipped to enforce existing tech-neutral laws that can address discrete harms. Many existing laws against creating, processing, and distributing CSAM and against harassment and cyberstalking apply in the context of chatbots just as much as they apply in other contexts. TIDA filled a gap in federal law around NCII deepfakes, but the possession and distribution of CSAM has long been illegal.

The third is education. Improving digital literacy must remain an essential focus of any effort to improve youth online safety - both in the chatbot context and more broadly. Congress and state legislatures should help K-12 schools to implement programs for media and digital literacy. Children and teens are growing up in a digital world, and it is critical that we prepare them to be responsible digital citizens.

At the state level, dozens of chatbot-related bills have been introduced and many have passed into law in the past two years. There is growing fragmentation at the state level and a range of approaches that have created inconsistent requirements. We believe there is a need for uniformity across the nation. Congress should enact preemptive legislation governing AI chatbots that draws from lessons learned from those laws that have gone into effect, balancing the impact of these laws on reducing risk to youth safety while allowing innovation and beneficial chatbot use to flourish.

The current FTC has taken an appropriately measured approach to AI chatbots. Recognizing concerns associated with how the Commission, under the prior administration, expanded its "means and instrumentalities" theory to target general-purpose AI tools, the current FTC has instead sought to gather evidence about AI chatbots. That 6(b) investigation is ongoing and we anticipate it will be instructive in identifying practices that may warrant action under the FTC's current authority.

In addition, when TIDA goes into effect in May, the FTC will have added authority to ensure the health and safety of children and teens. TIDA will provide the FTC with clear authority to police non-compliance with TIDA's requirements around CSAM and NCII which will help to address the unfortunate proliferation of deepfake pornography and "nudify" applications.

Ultimately, the health and safety of youth online and in their interactions with chatbots needs an open conversation among government, civil society, and industry about how to promote responsible industry practices and discourage unsafe or unhealthy practices. This conversation should lead to solutions that leverage different tools available - industry best practices, legal requirements, education, and more - in a way that balances competing interests.

Thank you for your consideration. We look forward to continuing to work with you and other Subcommittee members on the important issue of youth online privacy and safety.

Sincerely,

Paul Lekas
Executive Vice President
Global Public Policy & Government Affairs
Software & Information Industry Association

BRETT GUTHRIE, KENTUCKY
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED NINETEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115
Majority (202) 225-3641
Minority (202) 225-2927

December 22, 2025

Ms. Kate Ruane
Director of the Free Expression Project
Center for Democracy & Technology
1401 K Street NW
Suite 200
Washington DC 20005

Dear Ms. Ruane:

Thank you for appearing before the Subcommittee on Commerce, Manufacturing, and Trade hearing on Tuesday, December 2, 2025, to testify at the hearing entitled, "Legislative Solutions to Protect Children and Teens Online."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached.

To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on Monday, January 12, 2026. Your responses should be mailed to Alex Khlopin, Policy Analyst, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to alex.khlopin@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Gus M. Bilirakis
Chairman
Subcommittee on Commerce, Manufacturing, and Trade

cc: The Honorable Jan Schakowsky, Ranking Member, Subcommittee on Commerce, Manufacturing, and Trade

Hon. Brett Guthrie
Chair
House Committee on Energy and Commerce
2161 Rayburn House Office Building
Washington, DC 20515

Hon. Frank Pallone
Ranking Member
House Energy & Commerce Committee
2107 Rayburn House Office Building
Washington, DC 20515

Hon. Gus Bilirakis
Chair
House Committee on Energy and Commerce,
Subcommittee on Commerce,
Manufacturing and Trade
2306 Rayburn House Office Building
Washington, DC 20515

Hon. Jan Schakowsky
Ranking Member
House Energy and Commerce Committee,
Subcommittee on Commerce,
Manufacturing, and Trade
2408 Rayburn House Office Building
Washington, DC 20515

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

This letter responds to the question for the record submitted to the Center for Democracy & Technology (CDT) by the Honorable Russ Fulcher (R-ID) following the Subcommittee on Commerce, Manufacturing, & Trade Hearing Entitled "Legislative Solutions to Protect Children and Teens Online." The question follows:

> Ms. Ruane, I often look at these issues through a constitutional lens. You have written about how the Senate KOSA's duty of care raises significant First Amendment issues considering it focuses on constitutionally protected speech. No law blocked by the courts will protect a single child. Can you outline the First Amendment issues associated with the Senate KOSA's "duty of care" and the impact of recent key court decisions?

CDT's Response:

The Senate version of the Kids Online Safety Act's (KOSA's) duty of care provision should be subject to strict constitutional scrutiny for at least three reasons and likely would not survive that standard of review.[1] First, it restricts the constitutionally protected speech minors can access via

[1] Kids Online Safety Act, S. 1748 (119th Cong. 1st Sess.), https://www.congress.gov/bill/119th-congress/senate-bill/1748. The question refers to the Senate version of KOSA, but it is worth noting that there also may be lingering constitutional concerns with the duty of care in the pared down version of KOSA currently being considered by the House. Kids Online Safety Act, H.R.___, (119th Cong. 1st Sess.), https://docs.house.gov/meetings/IF/IF17/20251202/118714/BILLS-119pih-HR____KidsOnlineSafetyAct.pdf. The House version of the duty of care narrows the categories of content to be considered to include content that is illegal or otherwise

covered platforms. Second, it burdens the editorial judgment of covered platforms, forcing them to alter their decisions about what content to publish, what content to recommend, and to whom to recommend it. Third, it burdens adults' access to constitutionally protected speech by incentivizing platforms to verify their age prior to allowing users unfettered access to speech on any covered platform. Each of these issues provides a basis to subject the law to the highest degree of constitutional scrutiny, known as strict scrutiny, which the provision should fail. Recent cases, including *Moody v. NetChoice*[2] and *Free Speech Coalition v. Paxton*,[3] provide significant support for this conclusion.

1. Senate KOSA's duty of care provision burdens minors' access to and ability to engage in constitutionally protected speech.

Senate KOSA's duty of care provision would require covered online services to exercise reasonable care in the creation and implementation of any design feature to prevent and mitigate enumerated harms such as "depressive disorders and anxiety disorders" in minors under the age of 17.[4] That would effectively require covered platforms to restrict access to a wide range of constitutionally protected content on various subjects that might be linked to "depressive disorders and anxiety disorders" in minors, including but not limited to content related to climate change, weight loss, violence in schools, ongoing international conflicts, and any number of other topics that an individual

---

unprotected by the constitution. This is beneficial from a practical perspective in that it narrows the amount of speech platforms would be incentivized to censor under the legislation, but it may not fully cure the constitutional concerns, because determining whether particular speech falls outside the ambit of the constitution's protections is a fact-specific endeavor. *See Counterman*, 600 U.S. at 73 (recounting tests for unprotected speech); *Central Hudson*, 447 U.S. at 563 (describing false commercial speech as unprotected). When applying restrictions on the distribution of content, even illegal content, courts have been wary of the chilling effects the application of liability to distributors of speech might have. *See Bantam Books, Inc. v. Sullivan*, 372 U.S. 58, 71 (1963). Even the pared down version of the duty of care currently before the House requires covered services to make speculative judgments about what content should be covered by its policies, often based upon imperfect information and potentially no information regarding the original speaker's intent. Mike Masnick, *Masnick's Impossibility Theorem: Content Moderation at Scale Is Impossible To Do Well*, TechDirt (Nov. 20, 2019) ("[T}o to make good decisions you often need a tremendous amount of context, and there's simply no way to adequately provide that at scale in a manner that actually works."). This uncertainty in a legal requirement to remove or reduce the distribution of speech receives close constitutional scrutiny even when the targeted speech is not constitutionally protected because of the chilling effect it visits upon protected speech.

[2] *Moody v. NetChoice, LLC*, 603 U.S. 707, 144 S. Ct. 2383 (2024).

[3] *Free Speech Coalition v. Paxton*, 606 U.S. 461, 478 (2025) (hereinafter "*FSC*").

[4] Kids Online Safety Act, S. 1748 (119th Cong. 1st Sess.), https://www.congress.gov/bill/119th-congress/senate-bill/1748. *See* danah boyd, *KOSA Isn't Designed to Help Kids*, Substack (Jan. 31, 2024), https://zephoria.substack.com/p/kosa-isnt-designed-to-help-kids.

might find distressing. Moreover, *different kinds of content* might qualify as harmful depending on the age category of a particular minor.[5] What triggers anxiety in 8-12 year olds might be quite different from what does so for 15-17 year olds. Triggering content is also likely different based upon individual minors, who are far from monolithic.

KOSA's duty of care essentially would force covered platforms to make speculative judgments about which content and design features may contribute to these outcomes and then "mitigate" those harmful impacts. Mitigation strategies will include actions to reduce the publication and recommendation of content within the categories identified as potentially harmful. This tactic will undoubtedly sweep beneficial and educational content into the censorship dragnet. Content filtering technology that will be used to comply with KOSA's duty of care is unable to parse intent or nuance and is trained on keywords or associations between text to detect content and take action at scale. If a content filter is trained to detect and prevent recommendation of content with the hashtag #thinspo or #skinnygirlhacks to reduce content that relates to eating disorders, it is likely to remove not only content that uses those hashtags to promote an eating disorder, but also content that condemns, provides education about, or seeks to help people find pathways to treat and recover from eating disorders.[6] As such, KOSA's duty of care could prevent users from accessing important content they need, undermining its very purpose of protecting minors from harm.

Those content restrictions are not saved by their application to minors rather than to adults. A long line of precedent establishes that children have First Amendment rights and "only in relatively narrow and well-defined circumstances may government bar public dissemination of protected materials to them."[7] For example, in *Brown v. Entertainment Merchants Association*, the Supreme Court struck down a California statute restricting the sale of violent video games to minors. In that decision,

---

[5] Michal Luria & Aliya Bhatia, *The Kids Are Online: Research-Driven Insights on Child Safety Policy,* at 17, Ctr. for Democracy & Tech. (Feb. 2025), https://cdt.org/wp-content/uploads/2025/02/2025-02-14-Child-Safety-Symposium-Summary-report-final.pdf.

[6] Copia Institute, *Content Moderation Case Studies: The Challenges In Moderating Information Regarding Eating Disorders (2012)*, TechDirt (Mar. 10, 2021), https://www.techdirt.com/2021/03/10/content-moderation-case-studies-challenges-moderating-information-regarding-eating-disorders-2012/.

[7] *Brown v. Ent. Merchs. Ass'n*, 564 U.S. 786, 794 (2011) (quoting *Erznoznik v. City of Jacksonville*, 422 U.S. 205, 212-13 (1975)).

the Court noted, "No doubt a State possesses legitimate power to protect children from harm, [...], but that does not include a free-floating power to restrict the ideas to which children may be exposed."[8] The Seventh Circuit, reviewing a similar ban on minors' access to violent video games, explained, "[minors] must be allowed the freedom to form their political views on the basis of uncensored speech before they turn eighteen, so that their minds are not a blank when they first exercise the franchise."[9] The court reasoned that "[t]o shield children right up to the age of 18 from exposure to [disfavored or harmful ideas] would not only be quixotic, but deforming; it would leave them unequipped to cope with the world as we know it."[10]

The only exception to the general rule that minors' First Amendment rights cannot be restricted simply because they are minors (outside of the public school context) is for speech that is obscene for minors, a narrow category of sexually explicit content.[11] In *Free Speech Coalition v. Paxton,* the Court reiterated that content that is obscene as to minors includes only "works that (a) taken as a whole, and under contemporary community standards, appeal to the prurient interest of minors; (b) depict or describe specifically defined sexual conduct in a way that is patently offensive for minors, and (c) taken as a whole, lack serious literary, artistic, political, or scientific value for minors."[12] As to what kind of content that might entail, the Court in *Ginsberg v. New York* had found that "girlie magazines," like *Playboy*, could be considered to fall in this category.[13] The *FSC* Court in a footnote gave additional guidance illustrating how limited this category of speech is, explaining that it "cannot conceivably be read to cover, say, a PG-13 or R Rated movie."[14] Senate KOSA's duty of care sweeps in content far beyond that which is obscene as to minors – which is limited to content such as adult magazines like Playboy or websites like Pornhub or OnlyFans – leaving no doubt that it applies to speech that minors have the constitutional right to access and should be subject to strict scrutiny.

---

[8] *Id.* at 794.
[9] *Am. Amusement Mach. Ass'n v. Kendrick*, 244 F.3d 572, 577 (7th Cir. 2001).
[10] *Id.*
[11] *Ginsberg v. New York*, 390 U.S. 629, 634 (1968).
[12] *FSC*, 606 U.S. at 472.
[13] *Ginsberg*, 390 U.S. at 634.
[14] *FSC*, 606 U.S. at 481 n.7.

2. Senate KOSA's Duty of Care burdens the editorial judgment of covered platforms.

Implementation of Senate KOSA's duty of care requires changes to covered platforms' content moderation rules and processes. Under the bill, platforms would have to decide what kinds of content might lead to enumerated harmful outcomes for minors, change their content policies to reflect this assessment, alter what content they recommend to their users, and make changes to the ways in which that content is presented and to which users that content may be presented or recommended. In other words, KOSA's duty of care is a regulation of covered platforms' editorial judgment.

Burdens on editorial judgment are treated skeptically by courts and rightfully so.[15] Speech intermediaries are tremendously important to freedom of expression.[16] They represent the most efficient way for ideas and speech to reach broader audiences. This is particularly so when the speech intermediary is a social media platform, where anyone from a head of state to a preschool teacher can reach audiences far beyond those they would have without the platform.[17] In the recent case, *Moody v. NetChoice,* the Supreme Court made clear that laws that regulate social media platforms' decisions regarding which content to display and how to display it burden their editorial judgment and are subject to the highest degree of scrutiny a court can apply.[18] Because Senate KOSA would require covered platforms to change which content to display, to whom they display it, and how, under *Moody* it would be subject to strict scrutiny.

---

[15] *Miami Herald Pub. Co. v. Tornillo*, 418 U.S. 241 (1974) ("The choice of material to go into a new paper, and the decisions made as to limitations on the size and content of the paper, and treatment of public issues and public official -- whether fair or unfair -- constitute the exercise of editorial control and judgment. It has yet to be demonstrated how governmental regulation of this crucial process can be exercised consistent with First Amendment guarantees of a free press as they have evolved to this time.").

[16] *See Bantam Books, Inc. v. Sullivan*, 372 U.S. 58 (1963) (invalidating a scheme of government notice to booksellers that certain books may be obscene because it provided insufficient safeguards for First Amendment protections and aimed to suppress speech rather than aid publishers with legal compliance).

[17] *Packingham v. North Carolina*, 582 U.S. 98, 105–06 (2017) (describing social media as containing democratic forums with the "vast potential to alter how we think, express ourselves, and define who we want to be").

[18] *Moody*, 603 U.S. at 743.

3. Senate KOSA's duty of care burdens adults' access to constitutionally protected speech by incentivizing covered services to verify users' ages prior to allowing unfettered access to speech on the platform.

Finally, Senate KOSA's duty of care burdens adults' access to constitutionally protected speech by subjecting them to age verification. While the Supreme Court in *FSC v. Paxton* recently upheld an age verification requirement for access to adult web sites under intermediate scrutiny, the Court was very clear in its reasoning that it was upholding the state statute at issue because it barred minors' access to content they do not have the constitutional right to view, and the burden it placed on the speech of adults was tailored to service the goal of restricting access to that narrow category of content by minors.[19] That is simply not the case for KOSA, which would erect age verification barriers to access all sorts of content beyond that which might be obscene for minors, and clearly targets fully protected speech. Strict scrutiny is "the standard for reviewing the direct targeting of fully protected speech."[20] Therefore, Senate KOSA's duty of care is subject to strict scrutiny, as previous laws that have required age verification to access or communicate constitutionally protected have been.[21]

While Senate KOSA contains language purportedly not requiring platforms to verify age to comply, that language is functionally meaningless.[22] To comply with the law, covered platforms need to know to at least some degree which of their users are under the age of 18 and to do so means verifying all of their users' ages in some way. That means that all users, including adult users, would need to undergo an age verification process to access their social media accounts, erecting a high barrier to accessing services the Supreme Court has termed "the modern public square"[23] and an insurmountable barrier to those who would prefer not to share additional data with covered services or who do not

---

[19] *FSC*, 606 U.S. at 499.
[20] *Id*. at 484.
[21] *NetChoice v. Bonta I*, 113 F.4th 1101,1121 (9th Cir. 2024) (upholding a preliminary injunction against the enforcement of a requirement for covered services to assess what content might harm children and take action to address that content because it regulated constitutionally protected speech and did not survive strict scrutiny).
[22] Kids Online Safety Act, S. 1748 (119th Cong. 1st Sess.), https://www.congress.gov/bill/119th-congress/senate-bill/1748.
[23] *Packingham*, 582 U.S. at 99.

have the needed documentation to verify their ages. Strict scrutiny, therefore, should apply to the duty of care because of the burden the provision would place on adults' access to protected speech.

4. KOSA's Duty Of Care Provision Likely Would Not Survive Strict Scrutiny.

Strict scrutiny "requires a restriction to be the least restrictive means of achieving a compelling governmental interest,"[24] and Senate KOSA's duty of care fails that test. Although courts have recognized that protecting children is a compelling interest, to survive strict scrutiny, the government must demonstrate that the requirement at issue would achieve that compelling interest.[25] It is questionable at best whether the government could make such a demonstration with respect to Senate KOSA's duty of care. When California attempted to require parental consent for minors to purchase violent video games, the Court noted that the state could not show that violent video games caused violence in minors.[26] California had put forth studies demonstrating a link between playing violent video games and violent behavior, but the Court rejected these studies as insufficient because they did not show that playing violent video games *caused* violent action.[27] The state was not permitted to rely on the judgment of the legislature that the evidence was sufficient to justify the restriction because the law was subject to strict rather than intermediate scrutiny and strict scrutiny requires a causal connection.

The result should be the same for Senate KOSA. While some studies have linked social media use to certain risks of harm for minors, no study has shown that social media was its cause. Moreover, research on the effects of social media on minors is mixed. Many studies show that social media has benefits for minor users who are able to find communities they cannot find offline and information they otherwise might not have learned.[28] It further shows that social media's impacts are different for

---

[24] *FSC*, 606 U.S. at 484 (cleaned up).
[25] *See Brown*, 564 U.S. at 799 ("The State must specifically identify an 'actual problem' in need of solving, and the curtailment of free speech must be actually necessary to the solution" (internal citations omitted)).
[26] *Id*. at 799-800.
[27] *Id*.
[28] Berger, Matthew N., Melody Taba, Jennifer L. Marino, Megan S. C. Lim, and S. Rachel Skinner. "Social Media Use and Health and Well-Being of Lesbian, Gay, Bisexual, Transgender, and Queer Youth: Systematic Review." *Journal of Medical Internet Research* 24, no. 9 (September 21, 2022): e38449. https://doi.org/10.2196/38449.; Duplaga M, Szulc K. The Association of Internet Use with Wellbeing, Mental Health and Health Behaviours of Persons with Disabilities. Int J Environ Res Public Health. 2019 Sep 4;16(18):3252. doi: 10.3390/ijerph16183252.

minors depending on their age.[29] It is unlikely that the government could demonstrate sufficiently that social media use causes any particular harm to minors or that any of the potential actions covered services might take to comply would mitigate the harms enumerated in Senate KOSA. Under the Supreme Court's reasoning in *Brown* that would doom the provision.

Even if a reviewing court were to find the evidence of social media's harmful impacts sufficient to demonstrate that the duty of care would achieve the government's goals of reducing harm, Senate KOSA's duty of care likely would still fail strict scrutiny because it is not the least restrictive means for achieving the government's legitimate ends. Rather than restricting the publication of poorly scoped categories of content, the government could pursue less intrusive regulations, including supporting user controls, protecting users' privacy by requiring data minimization and use restrictions, or supporting the creation of more child-friendly spaces on the internet. Each of these alternatives would restrict less constitutionally protected speech than Senate KOSA's duty of care, demonstrating that the provision is not the least restrictive means of achieving the government's legitimate goals.

For those reasons, a reviewing court would likely find Senate KOSA's duty of care to be unconstitutional under the First Amendment.

[29] Orben, Amy. "Teenagers, Screens and Social Media: A Narrative Review of Reviews and Key Studies." *Social Psychiatry and Psychiatric Epidemiology* 55, no. 4 (April 1, 2020): 407–14. https://doi.org/10.1007/s00127-019-01825-4.