RPTR KRAMER

EDTR HOFSTAD

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, D.C.

The subcommittee met, pursuant to call, at 10:19 a.m., in Room 2123, Rayburn House Office Building, Hon. Gus Bilirakis [chairman of the subcommittee] presiding.

Present: Representatives Bilirakis, Fulcher, Dunn, Cammack, Obernolte, James, Bentz, Houchin, Fry, Lee, Kean, Evans, Goldman, Guthrie (ex officio), Schakowsky, 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; A.T. Johnson, Special Advisor; Daniel Kelly, Press Secretary; Sophie Khanahmadi, Deputy Staff Director; Alex Khlopin, Policy Analyst, Subcommittee on Commerce, Manufacturing,

and Trade; Brayden Lacefield, Special Assistant; Giulia Leganski, Chief Counsel, Subcommittee on Commerce, Manufacturing, and Trade; Joel Miller, Chief Counsel; Evangelos Razis, Professional Staff Member, Subcommittee on Commerce, Manufacturing, and Trade; Seth Ricketts, Special Assistant; Chris Sarley, Director of Member Services and Stakeholder Engagement; Matt VanHyfte, Communications Director; Hannah Anton, Minority Policy Analyst; Keegan Cardman, Minority Staff Assistant; Kelly Fabian, Minority Chief Counsel, Subcommittee on 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 of Member Services and Outreach; Megan Kanne, Minority Professional Staff Member; Phoebe Rouge, Minority FTC Detailee; and Andrew Souvall, Minority Director of Communications, Member Services, and Outreach.

Mr. Bilirakis. The committee will come to order.

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

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 standalone solutions; they complement and re-enforce 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.

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.

[The prepared statement of Mr. Bilirakis follows:]

******** COMMITTEE INSERT ********

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 -- yeah, 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.

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

[The prepared statement of Ms. Schakowsky follows:]

******** COMMITTEE INSERT ********

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.

With that, I yield back.

[The prepared statement of Mr. Mullin follows:]

******** COMMITTEE INSERT ********

Mr. Bilirakis. The gentleman yields back.

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

The Chair. 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 multifaceted 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.

And I would yield back.

[The prepared statement of the chair follows:]

******** COMMITTEE INSERT ********

Mr. Bilirakis. The gentleman yields back.

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

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.

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

[The prepared statement of Mr. Pallone follows:]

******** COMMITTEE INSERT ********

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 and Information Industry Association, welcome.

Ms. Kate Ruane, director of the Free Expression Project, Center for Democracy and 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, SOFTWARE AND INFORMATION INDUSTRY ASSOCIATION; KATE RUANE, DIRECTOR OF THE FREE EXPRESSION PROJECT, CENTER FOR DEMOCRACY AND 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:]

******** COMMITTEE INSERT ********

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 and 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 youth safe while preserving the internet as a resource for learning and connection.

Thank you.

[The prepared statement of Mr. Lekas follows:]

******** COMMITTEE INSERT ********

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 and 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 real-time, 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.

[The prepared statement of Ms. Ruane follows:]

******** COMMITTEE INSERT ********

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.

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 requiring 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:]

******** COMMITTEE INSERT ********

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 is 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. Okay.

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 techniques 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 follows 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.

The Chair. 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.

The Chair. 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 feeling (ph) 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.

The Chair. 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.

The Chair. 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.

The Chair. Okay. 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. Okay.

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. Yeah.

Mr. Pallone. -- 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?

RPTR MCGHEE

EDTR ZAMORA

[11:19 a.m.]

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. Yeah. 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. Yeah, 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 maligned 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 seat belts 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 contract. 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 internet 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. 4-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. Okay.

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 a antitrust case that involved Apple at the Supreme Court.

Mrs. Cammack. Okay. 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. Okay.

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 techs 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 kid's 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] Okay. 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 ends 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. Yeah. 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, 50/50 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. Yeah, 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.

Okay. 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, relates 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.

RPTR KRAMER

EDTR HOFSTAD

[12:18 p.m.]

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 co-lead 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 co-sponsorship 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. Yeah. 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 is 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 deceased 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. -- 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 co-lead 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 five 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 co-lead 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 States' 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 non-speech-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 pre-social-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. Yeah. 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 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, future-proof 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 is 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 reenforces 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 parent's 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. Yeah, 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 real-time. 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 one-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 follows:]

******** COMMITTEE INSERT ********

Mr. Bilirakis. Okay, 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.

[The information follows:]

******** COMMITTEE INSERT ********

Mr. Bilirakis. 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 1:11 p.m., the subcommittee was adjourned.]