Prepared Written Testimony
Dawn Hawkins
Senior Advisor, National Center on Sexual Exploitation (NCOSE)

U.S. House of Representatives Committee on Energy and Commerce
T*he World Wild Web: Examining Harms Online*
March 26, 2025

I. Introduction

Chairman Guthrie, Ranking Member Pallone, and Members of the Committee: Thank you for holding this hearing, because the stakes could not be higher.

My name is Dawn Hawkins, senior advisor at the National Center on Sexual Exploitation, a nonpartisan nonprofit founded in 1962, including a Law Center prosecuting landmark cases on behalf of victims. I've spent 16 years fighting to protect human dignity in the digital age, advocating against all forms of sexual exploitation. I come to you today not only as a national advocate and expert, but as a mother of five children. This fight for me, and millions of other parents, is very personal.

For too long, families and advocates have watched in anguish as America's children are harmed by technologies that the tech companies knew were detrimental to the health and well-being of children. We have worked with these companies, only to see piecemeal steps toward improvement. For too long, we have asked Congress to create the necessary guardrails to hold Big Tech accountable, while Big Tech grew more powerful, more profitable, and less accountable. But today—we are all hoping that this hearing can finally mark a turning point. It can be the beginning of a new chapter where Congress finally says: Enough. Our children deserve better.

I want America's youth to thrive in a connected world. But right now, this digital world is a danger zone for kids. This is not by accident, but by design. I am tired of begging companies to care, only to witness tiny, incremental changes while they rake in record profits.

Thankfully, Congress is not starting from scratch. The House and Senate have spent nearly a decade examining this issue in depth, holding at least 10 hearings since 2019, consulting concerned technologists, whistleblowers, and survivor families, to draft thoughtful, bipartisan legislation.

This is not a new conversation—it is simply Congress' moment to act on it. The groundwork has been laid. It is time to build.

We cannot afford a piecemeal approach. It doesn't work. Take the example of FOSTA-SESTA: a hard fought, bipartisan bill signed into law in 2018, which we all expected would dramatically reduce online sex trafficking. But the law has not been broad enough to overcome Big Tech's immunity under Section 230 of the Communications Decency Act (CDA 230). Today, companies continue to host, facilitate, and profit from sex trafficking—and even openly brag they cannot be held liable.

The window for Congress to act and course correct has narrowed. The question is not whether harm is happening. It is. The question is whether this Congress will be the one to enact the legal tools to stop it.

II. A Crisis of Design, Accountability, and Law

We are living through a seismic shift, and our laws have utterly failed to keep pace with this change. While the technology sector has advanced at breathtaking speed over the past 25 years, the legal framework designed to protect children online has not adapted. In fact, the last major piece of federal legislation to address online child safety passed when I was a teenager. Today, I have a near teenager of my own—and he is navigating an online world exponentially more dangerous than anything Congress could have imagined.

The problem is not just a gap in policy, but a vacuum of accountability. Big Tech's business model is built on capturing attention, maximizing engagement, and pushing users—especially youth—toward increasingly extreme, addictive, and harmful content.[1]

We must say this plainly: **the online sexual exploitation of children is not a glitch in the system. It is a byproduct of the *system as designed.***

[1] Dawn Hawkins and Lily Moric, "#Sunset230: Time's Up for the Greatest Enabler of Sexual Exploitation," *National Center on Sexual Exploitation*, June 17, 2024, https://endsexualexploitation.org/articles/sunset230-times-up-for-the-greatest-enabler-of-sexual-exploitation.

One of the most **devastating enablers of this crisis is Section 230 of the Communications Decency Act (CDA 230)**—a law passed in 1996 to encourage websites to moderate sexually explicit content without fear of being sued. But over the years, Section 230 has been twisted far beyond its original purpose. Today it is used as a legal shield by companies that knowingly host, amplify, and profit from child sexual abuse material (CSAM); grooming networks; sextortion predators; sex traffickers; and abusers who use the internet to intimidate, humiliate, or control their victims—including through stalking, revenge pornography, and domestic coercion.[2]

Even when victims and families beg platforms to take down CSAM—or when law enforcement asks for cooperation—tech companies routinely disregard these requests and claim that they cannot be held liable for any harm caused because of CDA 230. In some cases, they even argue that profiting with sex traffickers would still fall under CDA 230 immunity.[3] This is not hypothetical. These are real legal arguments being made in U.S. courts right now.

CDA 230 is not the only policy failure we must face. The **Children's Online Privacy Protection Act (COPPA)** was originally designed to protect the privacy of children under age 13. Unfortunately, many tech companies now misuse COPPA as a justification for allowing 13-year-olds to act as digital adults, permitting them to sign app store terms of service contracts without parental involvement.

COPPA was never intended to authorize children to enter into complex contracts. This is not what the law says, nor is it consistent with longstanding principles of contract law. COPPA was about protecting data privacy, not waiving parental rights at age 13. Yet major companies like Apple,[4] Google,[5] Microsoft,[6] Meta,[7] and so on, operate as if parental supervision is no longer needed the

---

[2] John Doe #1 and John Doe #2 v. Twitter, Inc., First Amended Complaint, U.S. District Court for the Northern District of California, Case 3:21-cv-00485-JCS, filed April 7, 2021, https://endsexualexploitation.org/wp-content/uploads/Doe-v-Twitter_1stAmndComplaint_Filed_040721.pdf.

[3] NCOSE, "Twitter Lawsuit Reinforces Critical Need to Reform Section 230," *National Center on Sexual Exploitation,* February 7, 2025, https://endsexualexploitation.org/articles/twitter-lawsuit-reinforces-critical-need-to-reform-section-230.

[4] "Family Privacy Disclosure for Children," Privacy, Apple, accessed March 24, 2025, https://www.apple.com/legal/privacy/en-ww/parent-disclosure.

[5] "How Google Accounts work when children turn 13 (or the applicable age in your country)," Help Center, Google for Families Help, accessed March 24, 2025, https://support.google.com/families/answer/7106787?hl=en.

[6] C Rey, "Why does Microsoft consider a 13 year old an adult?" Microsoft Community, last modified March 10, 2025, https://answers microsoft.com/en-us/msoffice/forum/all/why-does-microsoft-consider-a-13-year-old-an-adult/73cda0a2-4a3a-480e-b9a2-3a564d95dce6.

[7] "What happens to a child's Meta account when they turn 13," Account settings and management, Meta Quest Help Center, Meta, last modified March 3, 2025, https://www.meta.com/help/quest/244488408038461.

moment a child becomes a teenager, ignoring their vulnerability and exposure to exploitation. Some even allow children to independently disable that supervision on their 13th birthday, precisely when they are most at risk.

COPPA was not meant to empower trillion-dollar companies to broker access to children on behalf of other massive corporations. And yet, that is exactly what is happening. Now, Congress will consider COPPA 2.0,[8] and there is a real risk of making the same mistake again by cementing a system where parents have been removed from protecting the very group most targeted by online predators: young teens.

Meanwhile, tech platforms and their trade associations continue to claim that they "can't" make safer systems. But that's not true. They've chosen not to. At every turn, they've prioritized engagement over safety, frictionless access over responsible design, and profits over protection.[9]

The scale of this harm is staggering. According to the National Center for Missing and Exploited Children (NCMEC), there were **36.2 million reports of suspected child sexual abuse material** in 2023 alone.[10] Over the past three years, the number of urgent, time-sensitive CyberTipline reports where a child is at risk of harm has grown by **more than 140%**.[11] And that's just what's being reported. Platforms like TikTok, Instagram, X, and Snapchat are frequently named in these reports, not because they're doing too much, but because they're doing far too little.[12]

We are not dealing with passive failure. We are dealing with systems engineered to enable exploitation, and laws that offer those systems nearly limitless immunity.

---

[8] Children and Teens' Online Privacy Protection Act, S.836, 119th Congress, 1st Session (2025-2026), https://www.congress.gov/bill/119th-congress/senate-bill/836/text?s=1&r=1&q=%7B%22search%22%3A%22Children+and+Teens+Online+Privacy+Protection+Act%22%7D.

[9] "Apple's Faux 'Safety Solution'," Digital Childhood Alliance, March 6, 2025 https://www.digitalchildhoodalliance.org/apples-faux-safety-solution.

[10] "CyberTipline 2023 Report," National Center for Missing & Exploited Children (NCMEC), accessed March 24, 2025, https://www.missingkids.org/cybertiplinedata.

[11] "CyberTipline 2023 Report," National Center for Missing & Exploited Children (NCMEC), accessed March 24, 2025, https://www.missingkids.org/cybertiplinedata.

[12] *Children's safety in the Digital Era: Strengthening Protections and Addressing Legal Gaps: Testimony Before the Senate Judiciary Committee*, 119th Congress, February 19, 2025 (testimony of John Pizzuro, CEO Raven), https://www.judiciary.senate.gov/imo/media/doc/2025-02-19_-_testimony_-_pizzuro.pdf.

III. Parents Cannot Fight Alone

As a mother, and as someone who has worked in this field full-time for most of my adult life, I want to be honest: I cannot keep up. I cannot monitor every app, every chat, every game, every new loophole. And if I can't do it—someone who breathes this work every day—how can we possibly expect parents working full-time jobs, caring for multiple children, or navigating crisis or poverty to do it?

Tech companies love to say that it's up to parents to keep their children safe. That we should just monitor better, educate more, or keep our kids offline entirely. But how dare they. It is deeply wrong, and wildly out of touch, to place the burden of online safety solely on parents, when *the systems are engineered to override even our best efforts.*

The reality is that parents are not just unsupported, they're actively set up to fail. The tools we're offered are confusing, ineffective, and misleading:

- On Apple devices, activating full parental controls can take more than 20 separate steps.[13] These controls are buried under menus, require multiple changes to settings, and are constantly evolving, making it nearly impossible for even tech-savvy parents to navigate.
- On platforms like Roblox, toggles claim to block strangers from contacting your child—but what they don't say is that predators routinely exploit built-in workarounds to reach kids anyway. They know this is happening to kids daily, yet they don't warn us.[14]
- Snapchat's SnapMap allows children to share their exact real-time location with anyone on their contact list, often without understanding the consequences.[15]
- YouTube Kids and other "child-safe" platforms continue to surface violent, sexualized, or manipulative content because the algorithms are optimized for engagement, not wellbeing.[16]

---

[13] "The Complete Guide to Apple iPhone and iPad Set-up and Parental Controls," Device Review, Protect Young Eyes, accessed March 24, 2025, https://www.protectyoungeyes.com/devices/apple-ios-iphone-ipad-parental-controls.

[14] "The Dirty Dozen List '24: Roblox," National Center on Sexual Exploitation, last modified December 4, 2024, https://endsexualexploitation.org/roblox.

[15] *Children's safety in the Digital Era: Strengthening Protections and Addressing Legal Gaps: Testimony Before the Senate Judiciary Committee*, 119th Congress, February 19, 2025 (testimony of John Pizzuro, CEO Raven), https://www.judiciary.senate.gov/imo/media/doc/2025-02-19_-_testimony_-_pizzuro.pdf.

[16] Concerns with Google products, specifically YouTube, outlined and updated here: "The 2022 Dirty Dozen List: Google," National Center on Sexual Exploitation, last modified October 15, 2024, https://endsexualexploitation.org/google.

Parents aren't just left in the dark. We're handed broken flashlights and told to find our own way.

Meanwhile, tech companies position themselves as leaders in child safety, citing the existence of tools that, in practice, are dysfunctional or deceptive. Their messaging gives Congress and the public the impression that things are under control—when the reality is that families are being crushed by the weight of navigating this crisis alone.

Let's be clear: parents will always play the most significant role in protecting their children. However, they cannot accomplish this with the broken systems or laws that hinder us from doing so. And they shouldn't have to. *When tech companies shift the burden to families, it's not just unfair—it's a deliberate strategy to avoid their own responsibility. A way to deflect, deny, and delay real accountability.*

We need a system where safety is the default, not the exception. Where responsibility to protect children lies also with those who are profiting from their presence online.

IV. The Lies & Loopholes: When Tech Pretends to Act

Big Tech companies want Congress, and the public, to believe they're taking child safety seriously. They testify at hearings, release press statements,[17] and publish glowing transparency reports. But behind the curtain, we see the truth: Most of their "solutions" are either ineffective, misleading, or intentionally designed to do as little as possible.

Take TikTok, for example. The company publicly bragged about building a "reset" button for teens stuck in dangerous algorithmic loops—videos promoting suicide, eating disorders, pornography, drug use, and other harmful content. It sounded like a step in the right direction. But internal documents revealed in the Massachusetts Attorney General's lawsuit tell a very different

[17] Here are two examples with child safety expert commentary: "Snapchat's Family Center: A New Talking Point Not a Tool," *Organization for Social Media Safety*, August 18, 2022, https://www.socialmediasafety.org/blog/snapchat-family-center-review/?sm_guid=ODM3NjU1fDc4MjkzODIxfC0xfGRoYXdraW5zQHBvcm5oYXJtcy5jb218NzcwNDcxMXx8MHwwfDI0MTkyMTk0MnwxMTMyfDB8MHx8ODMyNzE0fDA1;
"Google's Self-Serving Proposal Fails to Protect Kids," Digital Childhood Alliance, March 12, 2025, https://www.digitalchildhoodalliance.org/googles-self-serving-proposal-fails-to-protect-kids.

story:[18] TikTok made the reset tool hard to find and activate. And even when teens managed to enable it, the platform simply returned them to the harmful algorithm after just 200 videos. That's barely 10 minutes of scrolling.

This was not a safety feature. It was a stall tactic. And it's not unique. Meanwhile, YouTube continues to recommend exploitative content to children through autoplay and algorithm manipulation, even when the platform is in "kid-safe" mode.[19] Many of these videos include inappropriate themes, sexualized images, or abusive behavior masked as entertainment.

The app stores are the gateway to all this, where failure is fundamental.

Apple and Google's app stores serve as the front doors to children's digital lives. And yet, they have created vague, unaccountable systems that let developers assign their own age ratings with little real oversight and few consequences for deceiving parents. They decide what gets listed. They profit from the in-app ads. And they regularly approve apps that are clearly dangerous for children, while claiming these apps are appropriate for 4- or 9-year-olds.[20] These include:

- AI-powered nudifying tools capable of generating child sexual abuse material from innocent photos[5]
- Chat roulette apps that connect children with adult strangers at random
- Sexualized games that mimic dating, strip challenges, or adult content

Astonishingly, Apple has allowed ads for adult content to appear in apps for young children.

---

[18] Hunton, "Massachusetts AG Unveils Internal TikTok Documents in Lawsuit Alleging Child Addiction Strategies," *Privacy & Information Security Law Blog,* February 10, 2025, https://www hunton.com/privacy-and-information-security-law/massachusetts-ag-unveils-internal-tiktok-documents-in-lawsuit-alleging-child-addiction-strategies**.**

[19] *Children's safety in the Digital Era: Strengthening Protections and Addressing Legal Gaps: Testimony Before the Senate Judiciary Committee*, 119th Congress, February 19, 2025 (testimony of John Pizzuro, CEO Raven), https://www.judiciary.senate.gov/imo/media/doc/2025-02-19_-_testimony_-_pizzuro.pdf.

[20] NCOSE, "Deceptive to the Core: How Apple App Store Age Ratings Mislead Parents," *National Center on Sexual Exploitation,* October 5, 2023 https://endsexualexploitation.org/articles/how-apple-app-store-age-ratings-mislead-parents/?sm_guid=ODM3NjU1fDc4MjkzODIxfC0xfGRoYXdraW5zQHBvcm5oYXJtcy5jb218NzcwNDcxMXx8MHwwfDI0MTkyMTk0MnwxMTMyfDB8MHx8ODMyNzE0fDA1.

Yet this entire system—parental controls, safety filters, content restrictions—depends on these broken ratings. That means families are being misled at the most basic level of digital protection. They are trusting the front gate, while the predators wait just inside.[21]

What we are seeing is not meaningful self-regulation. It is reputation management. And our children pay the price.

Congress cannot take these companies at their word. They have shown time and again that they will do the bare minimum to avoid regulation.

V. The Consequences: Children Harmed; Families Destroyed

This is no longer about what *might* happen to children online. It's about what *is* happening—every day, in every state, in every school, and often in every home. Behind the headlines and lawsuits are real kids and real families living through horror. These are just a few of the tragedies I've encountered in my work:

1. Sextortion That Ended in Suicide

A teenage boy connected online with someone he believed to be a peer. Within hours of sending one sexually explicit image, he was being blackmailed. The threats escalated: "Send more or I'll tell your family." "Pay me or I'll send this to your school." He spiraled into panic and despair.

Within 24 hours, he died by suicide.

His parents will never see him graduate. Never hear his laugh again. Because a predator reached into their home through a screen—and Instagram let it happen. Meta later removed **63,000 predator accounts** in one sweep[22]—but only after teens were dead and grieving families refused to stay silent.

[21] Detailed explanations outlining various concerns with Apple products and processes outlined throughout this website: "The Dirty Dozen List '24: Apple," National Center on Sexual Exploitation, last modified October 24, 2024, https://endsexualexploitation.org/apple.

[22] "Combating Financial Sextortion Scams From Nigeria," Meta, July 24, 2024 https://about fb.com/news/2024/07/combating-financial-sextortion-scams-from-nigeria.

And the system that allowed it all to happen? Still largely unchanged.

In the 18 months between October 2021 and March 2023, the FBI and Homeland Security Investigations received over 13,000 reports of online financial sextortion of minors. The sextortion involved at least 12,600 victims (primarily boys) and led to at least 20 suicides. This was a 20% increase over the prior timeframe.[23] Thousands of families are living with the trauma. And we know many more cases go unreported.

2. AI-Generated Child Sexual Abuse Material

In another case, a 15-year-old girl rejected a classmate's advances. He retaliated by using an AI app to generate sexually explicit images, CSAM, that looked just like her. He uploaded the images to mainstream pornography websites and circulated them on social media groups with classmates. She was humiliated, retraumatized, and devastated.

Platforms have been slow to respond—or refused to remove them at all. She's still fighting to get them down and, in many cases, they just continue to be reuploaded.

Apps that allow this kind of abuse—AI nudification filters and deepfake generators—are readily available in Apple and Google's app stores. Some have been rated as appropriate for ages 4 and up. Most of this technology was hosted by Microsoft's Github.[24] This crisis is exploding across K–12 schools. ***These apps are not buried in the dark web—they're in kids' pockets.***

3. Platforms That Refused to Remove CSAM

One of NCOSE Law Center's clients, a young teenage boy, was manipulated on Snapchat by someone posing as a teenage girl. He and his friend were tricked into creating sexual abuse material. Their abuser uploaded the footage to Twitter, where it was viewed over 160,000 times.

---

[23] Federal Bureau of Investigation Nashville Field Office, "Sextortion: A Growing Threat Targeting Minors," FBI, January 23, 2024, https://www.fbi.gov/contact-us/field-offices/nashville/news/sextortion-a-growing-threat-targeting-minors.

[24] Stephanie Trendell, "Kids Are Using AI to Violate Their Peers – and Microsoft's GitHub Is the Cause," *National Center on Sexual Exploitation,* September 5, 2024, https://endsexualexploitation.org/articles/kids-are-using-ai-to-violate-their-peers-and-microsofts-github-is-the-cause.

The boy and his mother begged Twitter to remove it. They submitted a government-issued ID to prove he was a minor. Twitter responded: "reviewed the content, and didn't find a violation of our policies, so no action will be taken at this time."[25] In other words, Twitter made an active choice to continue distributing CSAM on its platform even when presented with direct and documented evidence that the content was in fact CSAM depicting a 13-year-old child. The platform continued to profit from views and engagement as this child's trauma was consumed by hundreds of thousands.[26]

When sued, Twitter (now X) argued that even if they were profiting alongside sex traffickers, they were immune from liability under Section 230.[27] In their motion to dismiss to the Court they argued, "the law does not punish a defendant [Twitter] for participation in a lawful venture with sex traffickers, or knowingly but passively receiving the financial benefits of sex trafficking . . . merely failing to remove third-party content, even if abhorrent, is precisely what CDA §230 immunizes." Thus far, the courts have agreed with X. The case is on appeal in the Ninth Circuit.

4. Grooming That Led to Abduction

In another devastating example: a 13-year-old boy was first groomed on Roblox—a platform that built its business model on targeting kids under 13.[28] With 12.8 million U.S. children under the age of eight on the platform daily, it has become a playground for predators. The teen's abuse moved from Roblox to Snapchat, and eventually to X, where the predator also bragged about what he was doing and posted publicly about his plan to kidnap the boy. The predator followed through, abducting the child across state lines. Users alerted X and local law enforcement. ***X refused to help law enforcement. He was only rescued because a gas station attendant noticed something was off and intervened.***

[25] 25 Mot. to Dismiss, *Doe v. Twitter, Inc.*, Case No. 3:21-cv-00485-JCS (N.D. Cal. Mar. 10, 2021).
[26] First Am. Compl., *Doe v. Twitter, Inc.*, Case No. 3:21-cv-00485-JCS (N.D. Cal. Apr. 7, 2021), https://endsexualexploitation.org/wp-content/uploads/Doe-v-Twitter_1stAmndComplaint_Filed_040721.pdf.
[27] NCOSE, "Twitter Lawsuit Reinforces Critical Need to Reform Section 230," *National Center on Sexual Exploitation,* February 7, 2025, https://endsexualexploitation.org/articles/twitter-lawsuit-reinforces-critical-need-to-reform-section-230.
[28] John Tuason, "Roblox: A Tool for Sexual Predators, A Threat for Children's Safety," *National Center on Sexual Exploitation,* July 11, 2024, https://endsexualexploitation.org/articles/roblox-a-tool-for-sexual-predators-a-threat-for-childrens-safety.

These stories are not outliers. They are symptoms of a system that is optimized for harm. Every time a platform ignores a takedown request, fails to flag known predatory patterns, or refuses to redesign dangerous features, it is making a choice. A choice to protect profit, not children. And unless Congress steps in, this pattern will continue.

VI. We Need a Multi-Layered Response

If a child is riding in a car, we don't ask whether they're protected by a seatbelt *or* an airbag. We require both—plus crash-resistant frames, speed limits, licensing rules, and drunk driving laws. Because when lives are on the line, we don't rely on one tool. We build systems.

The same must be true online. There is no single bill that will fix this crisis. But together, we can create a safe, digital environment by changing the legal incentives facing tech corporations and giving victims more paths to justice.

The bills I outline below are the result of years of collaboration and refinement, and they have earned bipartisan support and widespread backing from families, youth advocates, and survivors themselves.

Critical solutions include:

1. CDA 230 Reform – Restoring Accountability

The Communications Decency Act was originally passed by Congress to encourage platforms to protect children—not to give legal immunity to those who knowingly enable their abuse. But today, Section 230 is the single greatest barrier to justice for victims of online exploitation and incentivizes platforms to monetize harm when it's profitable and not to invest in safety measures.[29]

Tech companies routinely use CDA 230 to avoid responsibility for:

- Hosting or refusing to remove CSAM
- Ignoring law enforcement or victim takedown requests
- Amplifying trafficking networks or monetizing sexual abuse
- Denying survivors access to justice in civil court

[29] Learn more about these concerns here: "The Dirty Dozen List '24: Communications Decency Act Section 230," National Center on Sexual Exploitation, April 10, 2024, https://endsexualexploitation.org/cda-230.

- Not investing in safety features, procedures, and products

Congress should:

- Sunset CDA 230, forcing Big Tech to come to the table to negotiate and develop a new standard that works for all.
- Reform CDA 230 in a major way that no longer protects platforms for their own negligence, their facilitation of criminal activity such as sexual abuse and sex trafficking, and their own harmful design features.
- If Big Tech continues to stonewall reasonable reforms to CDA 230 then Congress should repeal it. Big Tech does not deserve special protections that no other consumer product industry enjoys—especially when they know their products are causing massive harm.

It should never be protected conduct if a company knows, or refuses to know, when a child is being abused on its platform and then does nothing to stop it.

2. The App Store Accountability Act – Empowering Parents at the Gate

The app stores are the chokepoints to most youth digital experiences, yet they are completely unregulated—leaving parents without even the most basic safeguards. Earlier this month, Utah became the first state to require app store providers to verify users' ages and obtain parental consent for minors before app downloads. Variations on federal versions of this approach were introduced in the House by Rep. John James and in the Senate by Senator Mike Lee last December and deserve renewed consideration.

This bill would:

- Require accurate app age ratings and content descriptors
- Require verified parental consent before minors can agree to complex terms of service contracts and make in-app purchases
- Use the data app stores *already collect* on users in order to verify the age category of users and provide a signal to app developers

Currently, youth can download nearly any app, with no oversight, which also means signing terms of service contracts that give access to their camera, microphone, contacts, location, and other personal data.[30] Since when can corporations contract with children?

3. The Kids Online Safety Act (KOSA) – Redesigning for Safety

Today's platforms are designed to maximize engagement—not wellbeing. KOSA as passed by the Senate last July, 91-3, would establish a commonsense "duty of care" requiring platforms to:

- Design their platforms with the best interests of minor users in mind and turn on the strongest safety settings by default for minors
- Restrict dangerous features like auto-play, algorithmic amplification, and unsolicited direct messaging
- Give researchers access to platform data to understand harms that children are facing online
- Give parents new controls and create easier pathways for them to report harms to their children

If KOSA had been in place years ago, it's likely many children who were driven to self-harm, suicide, or addiction by algorithmic feeds would still be alive today.[31]

4. The Take It Down Act, PROTECT Act, SHIELD Act, & Defiance Act, NO FAKES Act – Combating Image-Based Sexual Abuse and the Misuse of a Child's Name, Image, and Likeness

Image-based sexual abuse (IBSA) is the creation and/or distribution of non-consensual, sexually explicit content, including AI-generated "deepfakes." It is ruinous to victims' lives, negatively impacting their mental health, causing them to live in extreme fear and shame. Once IBSA is uploaded and circulates worldwide, it exists forever. NCOSE's Law Center issues take down notices to platforms circulating this material and only a fraction of the time do companies remove it in response. Currently, IBSA is not a federal crime, and there currently is no federal civil causes

[30] Coalition of 60+ organizations leading a campaign for App Store Accountability. More can be learned here: "App Store Accountability Act Frequently Asked Questions," Digital Childhood Alliance, accessed March 24, 2025, https://www.digitalchildhoodalliance.org/faq.

[31] 200+ organizations support KOSA. More can be learned here: "It's time to put kids before profits," Pass KOSA, accessed March 24, 2025, https://www.passkosa.org.

of action that would give victims recourse. ***These bills are vital to stop the epidemic of IBSA and AI-generated CSAM.***

5. The Screen Act – Protecting Youth from Exposure to Hardcore Pornography

Children have widespread access to hardcore pornography, which is also exceedingly violent (based on academic research)[32] has led to dramatic increases in child-on-child sexual assault[33] and increases in, for example, teen strangulation.[34] As a result, states are moving to require pornography platforms to mandate commercially reasonable age verification. Another approach is to mandate built-in filters on cell phones and tablets registered to minors be turned on by default (device filter bills). A federal version of website-level age verification, the Screen Act, has been introduced in the Senate by Senator Lee. Isn't federal action the most effective method to protect our youth from exposure to hardcore pornography?

VII. The Moral Imperative to Act

The status quo allows tech companies to grow rich while children are manipulated, violated, and discarded. It's a system that places convenience over conscience. Engagement over ethics. Virtue signaling over wellness.

The truth is: Technology is no longer in its infancy. It's a multibillion-dollar force shaping childhood. The companies behind it are some of the most sophisticated entities in human history.

---

[32] Lisa Thompson, *The Most Dangerous Playground is Now…in our Kids' Pockets: Hardcore Pornography on Digital Devices Is Damaging America's Children* (Washington, DC: National Center on Sexual Exploitation, October 2024), https://endsexualexploitation.org/wp-content/uploads/2024-1022-Most-Dangerous-Playground_Citations.pdf; NCOSE, *Pornography & Public Health Research Summary* (Washington, DC: National Center on Sexual Exploitation, 2019), https://endsexualexploitation.org/wp-content/uploads/NCOSE_Pornography-PublicHealth_ResearchSummary_1-14-19_FINAL.pdf.

[33] NCOSE, *Confronting the Rise of Child-on-Child Harmful Sexual Behavior Research Summary* (Washington, DC: National Center on Sexual Exploitation, 2019), https://endsexualexploitation.org/wp-content/uploads/COCSA_Research-Summary_FINAL_3-12-19-1.pdf.

[34] Debby Herbenick, et al., "'It Was Scary, But Then It Was Kind of Exciting': Young Women's Experiences with Choking During Sex," *Archives of Sexual Behavior* (2021), https://doi.org/10.1007/s10508-021-02049-x; Debby Herbenick, et al., "Prevalence and Characteristics of Choking/Strangulation during Sex: Findings from a Probability Survey of Undergraduate Students," *Journal of American College Health* (2021), https://doi.org/10.1080/07448481.2021.1920599; Debby Herbenick, et al., "Frequency, Method, Intensity, and Health Sequelae of Sexual Choking Among U.S. Undergraduate and Graduate Students," *Archives of Sexual Behavior* 51 (2022): 3121-3129, https://doi.org/10.1007/s10508-022-02347-y.

Every delay has a cost. Every month that passes without change, more children are being groomed, exploited, and lost. Parents are burying children who never should have died. Survivors are reliving trauma every time a platform refuses to remove their abuse and allows it to be reuploaded. And predators are thriving in the absence of regulation.

But it doesn't have to be this way. Make this pledge: *It should never again be easier to groom a child than to protect one.* The 119th Congress has the chance to lead where others have stalled. To say: we see the evidence, we hear the cries, and we will not look away.

Thank you.