

United States Senate Committee on the Judiciary
***Children's Safety in the Digital Era: Strengthening Protections and Addressing
Legal Gaps***

**Testimony of Stephen Balkam, CEO and Founder
Family Online Safety Institute**

February 19, 2025

Good morning Chairman Grassley, Ranking Member Durbin, and distinguished members of the Committee.

My name is Stephen Balkam and I am the CEO and Founder of the Family Online Safety Institute (FOSI). FOSI is an international, non-profit organization whose mission is to make the online world safer for children and their families¹. FOSI convenes leaders in industry, government, academia, and the non-profit sectors to collaborate and innovate new solutions and policies that ensure a safer, more rewarding digital experience for all. Through research, resources, events, and special projects, FOSI promotes a culture of responsibility online and encourages a sense of digital citizenship for all.

FOSI has worked in this space for the past 18 years, but I have been involved in internet safety even longer, founding the Internet Content Rating Association (ICRA) and leading the Recreational Software Advisory Council (RSAC).

This is the third time I have testified before this committee. The first time was in 1995 at the dawn of the World Wide Web. During that hearing, I committed my organization to creating a content labelling system for websites so that parents could block the content they didn't want their kids to see. Thirty years later, we are working in a profoundly changed environment, though our values and mission remain the same.

¹ FOSI's homepage <https://www.fosi.org/>.

FOSI defines online safety as *acknowledging the risks, mitigating the harms while reaping the rewards of digital life*. This definition grounds our work by acknowledging that there are both positives and negatives that people of all ages experience on the internet.

In the “culture of responsibility” mentioned above, there is a role for all stakeholders to play to improve online safety: policymakers, law enforcement, industry, educators, parents and guardians, and the kids themselves.

FOSI works in the 3 Ps of online safety: enlightened public policy, industry best practices and Good Digital Parenting.

I am grateful for the opportunity to offer FOSI’s perspective and expertise to the committee today.

Our recent online safety work can be summarized by the theme of our last Annual Conference: “From Protection to Empowerment.” This is not an either/or proposition - either we protect our kids or we empower them. It is a “both and more” concept that involves all of the stakeholders in the culture of responsibility. We want to protect kids *on* the internet, not *from* the internet.

We must shield our kids from the worst of the web, particularly younger children. There are parental controls of every shape and size, and it is unthinkable to offer a pre-K or elementary school aged child a device with unfettered access to the internet.

But beginning in the middle school years and certainly into high school, the training wheels start to come off. We as adults move from being helicopter parents to being more like co-pilots with our kids - working together to explore the best ways to use the online safety tools that social media platforms and apps have developed for young people.

From our own research, teens highly value the features that allow them to block, mute, report, or stay private². This agency, the ability to begin to take control of their digital experiences, is the beginning of the kind of independence and resilience we want to encourage in our teens and young people.

Empowerment can be the best form of protection. It's about preparing young people for the moment they step out into the world on their own, ready to face the best and worst of what the digital landscape has to offer.

Young people are citizens, and citizens have rights. We are bringing up the next generation of citizens who are, from a very early age, aware of and engaged in the online world. It is in all of our interests to ensure that these young citizens understand their rights and the awesome responsibilities that come with exercising those rights.

Bans of social media and phones have been proposed in various jurisdictions for teens under 16. Australia has even passed such a ban into law. Blanket bans deprive children from any positive experiences they may find online, are difficult to enforce, and open up too many possible unintended consequences.

Bans affect young people's rights to access content and participate online, which contradict both the US Supreme Court and the UN Committee on the Rights of the Child. Children have rights, including freedom of speech and access to information. Just because we are the only country in the world that has not ratified the UN Convention on the Rights of the Child does not mean that American children have no rights - only that they are being deprived in comparison to children around the world.

On the technical side, implementing a ban effectively remains a daunting challenge as no universal age assurance method has been agreed upon. Bans would also impact innovation by disincentivizing platforms from creating safety features for young users, incorrectly assuming that underage users will no longer be online.

² FOSI's Managing the Narrative: Young People's Use of Online Safety Tools
<https://www.fosi.org/policy-research/managing-the-narrative>.

What we need instead are thoughtful restrictions: ones that acknowledge the nuances of these issues, allow for flexibility at the local level or within the home, and feature the explicit involvement of young people themselves. The more we involve young people in the creation of thoughtful restrictions, the more they will buy into the rules that are eventually agreed. Bans handed down from on high will create a culture of mistrust and drive young people to find creative and far less safe ways around such laws.

Congress achieved great success when it passed the Children's Online Privacy Protection Act (COPPA). And the FTC has done well in the 25 years since COPPA's enactment, taking significant enforcement actions and issuing updates through the COPPA Rule³. But the law still needs to be updated or expanded upon.

What would be ideal is a federal privacy law covering adults and children alike. This could serve as the basis on which to build online safety legislation on top of. If there are already existing limitations on what data companies can collect and how it can be used, people will be more comfortable providing their personal information in exchange for safer online experiences, such as better online safety tools and age assurance processes.

COPPA effectively treats everyone under 13 as a child and everyone over 13 as an adult. Minors are not a monolith, to all be treated the same, but instead go through phases of development from birth through adulthood. As kids age, they develop more agency, more capabilities, more rights and more responsibilities. A simple binary of over/under 13, or even 18 for that matter, is insufficient in our modern age. Teens still deserve privacy (and safety) protections, but not necessarily identical ones to children under 13. The UK's Age Appropriate Design Code (AADC) does an effective job acknowledging children's different developmental stages, based in research and child psychology⁴.

³ FTC's Kids' Privacy (COPPA)

<https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/kids-privacy-coppa>.

⁴ UK's ICO AADC Annex B: Age and developmental stages

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/annex-b-age-and-developmental-stages/>.

Congress also did well to pass the Children and Media Research Advancement Act (CAMRA) in 2022 and funded it for the past two years. This essential and timely research into the impact of digital technology on children’s physical and emotional development is exactly what the US government should continue funding, and results from the studies should serve as the foundation of evidence-based online safety policy.

The previous administration took a significant step forward in setting up the Kids Online Health and Safety (KOHS) Task Force⁵ through the National Telecommunications and Information Administration (NTIA) and Substance Abuse and Mental Health Services Administration (SAMHSA). The current administration should continue this important bipartisan work.

I was pleased to see the Senate pass the TAKE IT DOWN Act last week. That bill is a strong example of more targeted legislation that directly identifies and addresses a specific and important online safety issue. We hope to work with the House to see that legislation enacted.

The Kids Off Social Media Act is another example of promising legislation that could be effective in its goal. It is reasonable to want to keep children under 13 off of social media, and in most cases they are already excluded in platforms’ terms of service. Getting the definitions correct is important, as we do not want to cut kids off from access to safe spaces that were built with their safety in mind, such as YouTube Kids, Minecraft, Roblox, and educational spaces like Wikipedia.

An additional section of this bill addresses algorithmic or personalized recommendation systems for children and teens. This is another worthwhile area for Congress to explore, and lawmakers should learn from the related laws passed last year in New York and California. I have some concerns about Title II of the bill, as I want to ensure realistic protections for kids on school devices and networks without

⁵ KOHS Task Force Recommendations and Best Practices for Safe Internet Use <https://www.ntia.gov/press-release/2024/kids-online-health-and-safety-task-force-announces-recommendations-and-best-practices-safe-internet>.

imposing surveillance requirements or threatening essential funding for schools and students.

I am not a privacy or free speech absolutist. Of course privacy and free speech are important, protected rights. However, in order to pass effective online safety laws, I believe that there are opportunities for realistic compromises to be made. I expand on this more in the age assurance section below, but there are instances where it is reasonable for adults to give up a little privacy in order to access particularly harmful content or spaces online. I believe we can find a middle ground where young people have online safety protections while still maintaining a degree of privacy and access to consume and publish speech, and I am committed to working with Congress to achieve it.

Age assurance has become an integral part of the online safety policy discussions. We define age assurance as a broad term that describes various methods to discern the age or age-range of an online user including age verification, age estimation, and age gating. FOSI has conducted original research into age assurance in 2022⁶, as well as a white paper after a year's long working group in 2023⁷.

Age assurance is not a silver bullet that will solve all online safety concerns. However, it is a powerful tool that can be utilized to improve online safety, especially when thoughtfully considering the tradeoffs and use cases relating to proportionality. We present the tradeoff as that of invasiveness versus effectiveness - that is, to know a user's age with a higher level of certainty will almost always require more personal information. For online experiences that present relatively low risk to young people, it may be perfectly appropriate to use less precise age assurance mechanisms in order to access those experiences. Whereas for the most dangerous experiences or to access clearly harmful content, it would be justified to require a higher level of certainty and full age verification.

⁶ FOSI's Making Sense of Age Assurance: Enabling Safer Online Experiences
<https://www.fosi.org/policy-research/making-sense-of-age-assurance-enabling-safer-online-experiences>.

⁷ FOSI's Coming to Terms with Age Assurance
<https://www.fosi.org/policy-research/coming-to-terms-with-age-assurance>.

With technological advances, we believe that commercially feasible, privacy preserving age assurance is possible and will become even more effective through continued innovation in this space. Successfully incorporating age assurance measures into online safety laws will require risk-based proportionality, thoughtfully considering tradeoffs, and not being overly prescriptive with the technology or methods of assurance.

An alternative online safety perspective is safety by design. Discussing and legislating content moderation has devolved into debating what is actually harmful to kids, cherry picking examples of successes and failures, and legitimate concerns about violating freedom of speech and expression rights. Advancing the conversation to focus on a higher level of baseline protections offered to young users (raising the floor) is a worthwhile progression of the online safety policy discourse.

Australia's innovative eSafety Commissioner has been working on safety by design for years and has produced thoughtful guidance for industry to implement and governments to replicate⁸. The UK has also begun some of this work through its AADC. While it must be acknowledged that their AADC is based in privacy law and is specifically focused on data privacy practices, it still has an impact on children's online safety as its core requirement for industry is to consider and design for the youngest users, thinking critically through multiple stages of child development. We can learn a lot from the successes international regulators have had, and how to benefit from them here in the US while respecting our robust free speech protections.

While considering international approaches to online safety regulation, it becomes clear that the US is falling behind. In addition to the UK's AADC, which has been in effect since 2020, the UK has the Online Safety Act (OSA) which passed in 2023. The EU has the Digital Services Act (DSA), and Australia has its own Online Safety Act and an expert regulator in the eSafety Commissioner. While none of these regulations are perfect, they demonstrate multiple paths to improving online safety. Congress should learn from these creative ideas and improve upon them so that Americans of all ages, especially children and teens, are not left behind by their peers abroad.

⁸ eSafety Commissioner Safety by Design <https://www.esafety.gov.au/industry/safety-by-design>.

I also want to highlight the work of the Global Online Safety Regulators Network⁹ (GOSRN), a forum for independent regulators to exchange best practices and research across their jurisdictions. Current members include online safety officials from the UK, Australia, Fiji, France, Ireland, Republic of Korea, Slovakia, South Africa, and the Netherlands. I agree with the KOHS Task Force recommendation that the US, by way of the FTC, join the GOSRN as an observer until we have an effective online safety law and empowered regulator.

US states have begun to act on their own, with dozens of examples of online safety bills being introduced to require age-appropriate design, assert parental rights and permissions, require age verification, dictate content moderation, prevent addictive algorithms and targeted advertising, protect child influencers, and more.

Unfortunately we have seen that most of these ideas, even if they pass into law, are swiftly challenged in court and blocked from going into effect. While the states are the laboratories of democracy and have offered some thoughtful and innovative solutions, there are significant contradictions between policies and concerns about regulating the internet differently across state borders. There is a role for Congress to play here, ideally setting a high floor of baseline online safety protections that states can build on top of if they choose.

Industry has a significant role to play here as well. Companies can and must do better to create easy to find and easy to use controls for parents and online safety tools for teens and young people. Apps and platforms need to do better to publicize and promote these controls and tools. And industry as a whole must better collaborate with each other - harmonizing tools across the ecosystem so that parents and teens are not overwhelmed with the task of setting and managing controls across countless apps, games, websites, and social media platforms.

Parental controls would be more effective and more utilized if they were standardized, interoperable, and unified between apps, devices, and brands. This is an opportunity for industry to work with lawmakers to improve the online safety experience for all families.

⁹ Global Online Safety Regulators Network, Ofcom
<https://www.ofcom.org.uk/about-ofcom/international-work/gosrn/>.

While FOSI primarily works with online safety issues that are harmful but legal (awful but lawful), I must acknowledge that there are some severe risks and harms to young people being online. When it comes to illegal content and action such as child sexual exploitation, human trafficking, and sextortion, we defer to our friends at NCMEC, Thorn, and law enforcement (including the DOJ and FBI) who have direct expertise and do excellent work in these disturbing areas.

However, FOSI can still be helpful in this space, serving as an upstream intervention with our preventative work. If our Good Digital Parenting resources¹⁰ are used effectively, they can help curtail kids from getting into positions where they can be exploited. The goal of our resources is to improve online safety conversations and restrictions as a family: more frequent, more informed and educated, more specific, more trusting discussions so that if a child encounters anything uncomfortable online (including the beginning of being groomed by a predator), they can bring their concerns to their family without fear of punishment or overreaction, successfully cutting off access to harmful content and conversations before the situation escalates. We have free resources available to facilitate these family conversations and restrictions, as does the US government thanks to the KOHS Task Force report¹¹ from last year.

This is also an opportunity to raise the importance of digital media literacy at home and in schools. Our friends at the National Association for Media Literacy, My Digital Tat2, Common Sense Media, and MediaSmarts have excellent resources for educators, and policymakers interested in improving media literacy education across the country.

FOSI's latest research report "Promoting Wellbeing in a Digital World"¹² from December 2024 offered a quantitative and qualitative look into teens' wellbeing. We

¹⁰ FOSI's Good Digital Parenting Resources

<https://www.fosi.org/good-digital-parenting-resource/resources>.

¹¹ KOHS Task Force Report Best Practices and Resources for Parents and Caregivers

<https://www.ntia.gov/report/2024/kids-online-health-and-safety/online-health-and-safety-for-children-and-youth/taskforce-guidance/best-practices-resources-for-parents-caregivers>.

¹² FOSI's Promoting Wellbeing in a Digital World

<https://www.fosi.org/policy-research/promoting-wellbeing-in-a-digital-world>.

released a subsequent analysis¹³ to highlight some key findings that could help inform policymakers in producing effective, nuanced regulation. Our top takeaways should not be surprising because they are outlined elsewhere in my testimony: think beyond bans; continue to fund research; and listen to the experts. I would also like to point out a couple more specific findings and related recommendations.

One is that definitions matter: lawmakers should carefully consider which services and platforms they intend to include in specific legislation. There are a variety of types of online spaces and platforms, and each may be used in distinct ways, with different purposes, risks, rewards, and impacts on digital wellbeing. Legislation that makes sense for social media platforms may be ill-suited to regulate gaming companies, streaming services, and possibly even adjacent spaces like livestreaming and discussion platforms. Some legislation takes a more thoughtful approach to definitions and scope than others. A possible path forward may be crafting narrower, more targeted online safety legislation that is focused on one sector or one aspect of being online.

I would be remiss if I did not also acknowledge that there are also significant benefits of digital experiences to teens' wellbeing. Both parents and teens reported that connecting with peers and learning new skills are the top benefits from being online. These positives are important to remember as online experiences have been incorrectly compared to tobacco or alcohol, which decidedly have no benefits to teen wellbeing. Congress can keep these findings in mind in order to mitigate online risks and harms while empowering teens to reap the rewards of their digital lives.

Let us challenge ourselves to reimagine what online safety can look like - not just as a range of restrictions, but as a foundation for resilience, confidence, and opportunity. Let's move from fear to trust, from limits to possibility, and from protection to empowerment.

Thank you for your time this morning and I look forward to your questions.

¹³ FOSI's Policy Implications of FOSI's 'Promoting Wellbeing in a Digital World' Research <https://www.fosi.org/policy-research/policy-implications-of-fosis-promoting-wellbeing-in-a-digital-world-research>.