November 16, 2023

Ruth Yodaiken
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW
Washington, DC 20230

Introduction

The Family Online Safety Institute (FOSI) appreciates the opportunity to contribute to the National Telecommunications and Information Administration (NTIA) Request for Comment related to the interagency Task Force on Kids Online Health & Safety, Docket NTIA-2023-0008.

FOSI is an international, non-profit, membership organization working to make the online world a safer place for children and their families. We achieve this by identifying and promoting the best practices, tools, and solutions in the field of online safety. FOSI convenes leaders in industry, government, academia, and the non-profit sectors to collaborate and innovate new solutions and policies in the field of online safety. Through research, resources, events, and special projects, FOSI promotes a culture of responsibility online and encourages a sense of digital citizenship for all.

FOSI defines online safety as *acknowledging the risks and mitigating the harms in order to reap the rewards of digital life*. Our work is complementary to NTIA's nuanced approach to these issues as this Request for Comment inquires about risks and benefits of young people being online, best practices for online platforms to increase privacy and safety, where to access trustworthy resources, and the role of government and policymakers.

Identifying health, safety, and privacy risks and potential benefits

Regarding Question 1: FOSI works in the harmful but legal, awful but lawful, online safety space. When it comes to some of the most egregious harms that young people may encounter online, such as sexual violence and exploitation, trafficking, and illicit drugs, we defer to others in this space that specialize on those topics, including the National Center for Missing and Exploited Children (NCMEC) and local and national law enforcement including the DOJ and FBI. Some of the harms that we work most closely with include cyberbullying, communication with strangers that could lead to grooming and exploitation (and how to prevent this type of

escalation), exposure to harmful content, and the spread of misinformation (including health misinformation). The emergence of generativeAI has opened up additional potential for harm to minors in these areas.

Regarding Question 1(b): It is important to recognize the different set of risks that exist on different types of online platforms and services. Platforms that allow direct messaging between strangers of any age pose more of a risk for grooming and exploitation than services that restrict who youth users can message, or require mutual known friends/acquaintances in order to direct message. Platforms with publicly visible comments pose more of a risk of cyberbullying than those that do not have that feature. And online services that offer robust safety tools that allow users to customize their experience, including how information is shown to them, would pose less of a risk of spreading misinformation than those with no customization options. More information on the distinction between types of services can be found below in response to Question 9.

Regarding Question 1(c): FOSI has conducted research into the attitudes and use of both parental controls and online safety tools aimed at younger users. We found that parents are overwhelmed by the many different types of parental controls, where to find them, how to use them, and what the tools do. It is a positive development that so many different platforms, apps, devices, and networks have developed parental controls aimed at improving the online safety experiences of young users. Unfortunately, the proliferation of so many different controls has also increased overwhelm for parents and guardians. In fact, we found that when it came to online safety, 61% of Gen Z users feel they teach their parents more than parents teach them - and 50% of surveyed parents agreed. If parents do not fully understand how to effectively use the tools provided to them, it can create a false sense of control, and allow kids to more easily circumvent things like parental controls without parents' knowledge. While we do encourage families to have honest discussions about online safety rules and practices, children setting up their own parental controls is not a reliable solution.

Instead, we want to empower and equip families to have these conversations together. FOSI has spent years developing a set of Good Digital Parenting resources that are available for free on our website. These resources, combined with our broader tips, tools, and blogs, can be used to facilitate family conversations about technology use and how to engage with online platforms. Some offer general guidance while others are practical worksheets that are intended to be filled in by family members to create their own boundaries and age specific agreements. Many of these materials are available in English and Spanish, and are free for anyone to access and download at www.fosi.org/good-digital-parenting.

To assist overwhelmed and busy parents, platforms should use consistent words and phrases, menus, and design/layout (perhaps a one stop shop "safety center" tab in the site menu). Terms

of service/community guidelines should be placed consistently by online platforms, in a "settings" or "about us" menu title. The terms should be written in as plain language as possible. The UK's Age Appropriate Design Code (AADC) Transparency Standard expands on how to provide clear, concise, and prominent information. Parental controls and user online safety tools should also be easy to find in a "settings" or "account info" menu title, and explain how to use the tools, what each is best used for, and generally how the tools work.

Regarding Question 1(e): Members of marginalized groups can experience the benefits of being online by finding community, but also risk experiencing harms as well. Youth with unsupportive families are most at risk of online harms both because they may be targeted online based on their gender, sexuality, race, religion, disability, and because they are less likely to have honest conversations with their parents/guardians and may be less likely to ask for help from their families when they experience some type of harm online.

For example, research conducted by Thorn found that more than 50% of cisgendered non-heterosexual male teens in their study reported receiving sexually explicit images that they did not solicit. Additionally, this same group reported that they choose to handle feeling unsafe online alone. An alarming illustration of how young people from underrepresented or marginalized groups can often be disproportionately targeted while simultaneously not feeling comfortable or not having access to support systems offline.

A Pew Research study also found disparities in the likelihood of teens to experience cyberbullying and their perceptions of why they are targeted. Cyberbullying is a pervasive issue for young people with nearly half (46 percent) of all teens saying that they have experienced some form of online harm. However, this harm is not evenly distributed. Older teen girls (15-17 years old) reported experiencing cyberbullying at higher rates than teens of any age or gender. Additionally, Black and Hispanic teens are more likely than white teens to say that online harassment and bullying are problems for people their age.

While far too many young people experience online harms, the impacts are not felt equally across all demographics. Young people with unsupportive families or fewer access to offline resources may experience greater difficulty or increased fear seeking help.

Regarding Question 1(h): AI and emerging technologies present an interesting but complicated development, as they can be used to both generate misinformation and detect misinformation, as well as other content that violates a platform's terms of service. These tools and technologies can make content moderation more difficult in terms of how fast content can be produced, but also make it easier to detect harmful content or malicious actors. We appreciate the efforts that this Administration and governments around the world are taking to build safety guardrails around this important and actively evolving technology. There are many complicated issues raised by the

proliferation of AI and FOSI welcomes the thoughtful, nuanced approaches to require transparency, protect civil rights and data privacy, and prevent discrimination.

FOSI's original research into generative AI included quantitative and qualitative surveys of parents and teens in the US, Germany, and Japan. We found that unlike other technologies, parents and teens have a similar awareness of genAI, and teens actually perceive their parents as knowing more about it than they do. Another takeaway is that despite their concerns, a majority of parents feel positive overall about their teens using genAI, and both parents and teens believe genAI will become embedded in their school, work, and personal lives. 65% of parents and 66% of teens said that they expect a future where using genAI tools will be a vital skill for them to remain competitive in school or career.

Regarding Question 3: Finding community is a current benefit of being on online platforms, especially for isolated youth - youth affiliated by gender, sexuality, race, or religion - who do not have similar peers or family members in their immediate physical proximity. Online platforms offer important opportunities to access general and medical information, explore identity, and find communities, unrestricted by geography. This can increase young people's sense of belonging, an important part of adolescent development and wellbeing.

Regarding Question 3(a): Generally yes, these benefits are available to most minors, but there are still significant concerns about the digital divide and how many youth cannot reap the rewards of being online due to access and affordability of both broadband and devices. The FCC, through its Affordability Connectivity Program, the federal government broadly, through significant funding of broadband expansion, as well as many internet service providers, in partnership with the government programs and school districts, have made considerable efforts and progress in connecting all Americans. However, gaps still remain. Accessibility and affordability are central tenets to keep in mind when working towards full broadband adoption.

Certain state policies seek to limit teen's access to social media and other online platforms. State (and federal) laws and regulations should not ban or exclude teens from digital spaces where they can learn, communicate, socialize, and engage with their peers. A recent report published by the American Psychologist Association states that certain young people who have anxiety or struggle socially find social media beneficial to staying connected or practicing social interactions.

A recent webinar conducted by FOSI titled: A Connected Community: Empowering LGBTQ+ Teen Online demonstrated the importance of safe online spaces for LGBTQ+ young people. Additionally, research conducted by Thorn acknowledges that while most young people benefit from their online community, LGBTQ+ teens were nearly 20 points more likely to say they felt that their online communities were essential to their lives. This opportunity to connect safely

with people with shared identity, in addition to accessing vital resources, cannot be overstated. Access to information and community is an important right that should not be infringed on.

Regarding Question 5: Yes, young people should be considered and consulted in the design of online products and services that they are likely to use, from the very early stages of design and development of the product and service. Young people should also be consulted regularly about how they are using a product or service, and have the opportunity to offer improvements, suggestions, or ideas about how their experience on the platform or service could be improved. Similarly, young people should be included in efforts to regulate the social media and online spaces that they regularly use. Their ideas and testimony have even led to new laws that better protect young people online. We regularly involve young people in our work, including our research, family resources, and events. Young people have valuable experiences and perspectives that must be used to best inform policies and products that affect them.

The Status of Current Practices

Regarding Question 6(a): There are a variety of tools and features that platforms employ to mitigate harms and improve online experiences. Some include:

- Online safety tools (settings and controls within apps or platforms that empower individual users to take action and customize their online experiences).
    - Hiding, muting, blocking, and reporting are examples of online safety tools - giving a user the ability to avoid interacting with certain users or categories of content if they wish, with an escalating possibility to report other users or content to the platform.
    - Additional options to customize their feeds and experiences.
    - The ability to set screen time limits or limit their time to certain hours.
- Interstitials and content warnings around potentially harmful or inappropriate content.
- Fact checking labels around public health, election, or other official events.
- Pop ups that tell users they've been viewing a specific type of content a particularly high amount and suggesting other topics/categories that they may find interesting - avoiding a rabbit hole.
- Parental controls.

Regarding Question 6(b): An unintended consequence of parental controls is the risk of them turning into surveillance controls. Young people, especially teenagers, have a right to privacy and autonomy, so parental controls should not be overly invasive and able to access 100% of a minor's account.

If platforms have reporting mechanisms it is important for platforms to follow through on such reports - sending replies to the users who make a report and sharing information about what

happened as a result of the report. Young users feel helpless and disempowered when they report harmful or offensive content and users but do not receive any response from the platform and do not see the violative content or user being removed, and become less likely to report content or users in the future, believing it is futile.

Regarding Question 6(c): Behavioral advertising to youth has started to become viewed as an overly invasive violation of privacy that advocates have been criticizing, governments have started to restrict or ban, and industry has started to move away from. Contextual and other types of advertising are more appropriate for youth, in order to limit the amount of personal data about youth that is collected, sold, and used for targeting advertising.

Regarding Question 6(d): As mentioned in 6(c), privacy advocates wanted to restrict/ban targeted advertising to youth, some governments began to regulate accordingly (UK's AADC), and companies fell into compliance.

Regarding Question 8: Publicly quantifying popularity (number of likes, friends, impressions, and interactions) can be especially harmful to teens and preteens, an age group that is particularly sensitive to peer feedback, approval, and belonging.

Regarding Question 9: This is a particularly important question, and one that any policymaker should pay close attention to. The definition of "social media" or "online platform" is critical to determining which platforms and services are included. One category of platforms and services include those where users are shown videos, pictures, and written posts by people they know, people they follow, and popular accounts. There is some level of commenting or communicating between users, most or all content is user-generated content (UGC), and there is some feature of scrolling, swiping, or autoplay to the next piece of content.

Then there is a different category of platforms or services that prioritize direct communication between users - whether it be in large groups or one-on-one. It's also important to distinguish between autoplay on platforms that primarily host UGC vs. autoplay on streaming services that exclusively feature professionally produced content that has been reviewed and assigned a clear age rating.

When considering video games, policymakers should consider online vs. offline video games, where one features communication with others including interactions with strangers and the other does not. Another type of platform that is distinct from but related to video games includes users who stream themselves playing online, and comes with its own unique considerations of benefit and risk.

In attempting to regulate the vast array of online platforms and services, policymakers should be clear about the scope of their regulation. More clarity will help reduce unintended consequences and make relevant platforms better able to comply.

Regarding Question 10: As already mentioned above there are a number of best practices for maximizing benefits to minors' health, safety, and/or privacy. These include:

- The shift from targeted advertising to contextual advertising improves minors' privacy.
- Offering robust user online safety tools, allowing young users to customize their online experiences. More user empowerment and agency is a best practice.
- Thoughtful restrictions on time spent on the platforms, especially for young users:
    - Take a break reminders.
    - Diversity in algorithmic recommendations.
    - Limited push notifications (especially late at night).
    - The Surgeon General has said that much of the harm youth experience online comes from what time online is replacing, i.e. sleep, exercise, quality time with friends and family, and that important developmental time should be protected.

Regarding Question 10(a): Yes, the ideas in question 10 are not platform specific and could be adopted by many online platforms.

Regarding Question 10(c): The UK's AADC is a good example of imposing new restrictions on platforms and services to prioritize the wellbeing of youth. The incentive is to comply with the regulation or face significant fines, but the UK's ICO has been thoughtful and willing to work with industry to provide more guidance and clarity in order to bring companies into compliance, instead of seeking to sue immediately over any noncompliance.

Regarding Question 12: As the APA health advisory acknowledges, youth development is gradual and continuous, so as young people grow up their rights, understanding, and agency change as well. A 17 year old should have more independence from their guardian with more nuanced, detailed online safety tools offered to them and less surveillance-style parental controls than a 13 year old. Neither platforms nor governments should treat everyone under 18 as a monolithic group that needs the same protections, features, and consideration.

Identifying Proposed Guidance and/or Policies

Regarding Question 16: The US government should encourage and fund research in this area. One bill passed at the end of 2022, the Children and Media Research Advancement Act (CAMRA), establishes through the NIH longitudinal studies on the physical, emotional, and developmental effects of digital media on infants, children, and adolescents. This is vital research

that must continue to be funded, and the results of which should inform further guidance and recommendations.

When considering guidance, the government should bring nuance and thoughtfulness to all guidance and recommendations related to online health and safety, and ensure such communication is based on evidence. Guidance could include sections about what policymakers, platforms/services, and parents/guardians can do - just like the Surgeon General's advisory from earlier this year. Reminding all parties that they have a role to play will build a culture of responsibility where everyone feels that they have agency and the ability to take concrete steps to increase young people's online health safety.

Regarding Question 16(a): It is critical that when platforms offer (or regulation requires) parental controls, these controls must at some level still protect kids' privacy and not allow such controls to become surveillance tools. Youth have privacy rights and parents/guardians should not be allowed to have full, unfettered access to their accounts, including the ability to view their messaging and everything they view, watch, or say. Government guidance should be rights respecting, including children's rights.

Regarding Question 16(b): The UK ICO's iterative process of implementing and enforcing the AADC is a good example. Instead of prioritizing litigation and bringing lawsuits against companies struggling to comply, the priority is to bring as many platforms into compliance as possible. The ICO has spent years conducting research, issuing and updating public guidance, and meeting with companies in order to ensure the AADC is being complied with, and therefore youth in the UK are safer online.

Regarding Question 16(c): FOSI has long called for the creation of a Chief Online Safety Officer position in the US government, to coordinate and oversee all online safety activity across the administration. We welcome the creation and progress of this interagency Task Force, and still believe that having one office responsible for the coordination of all of these efforts would be efficient and productive.

As you are aware, the NTIA has overseen a historic investment to increase broadband access across the country. This office, as congressionally authorized, is well suited to work on expanding internet access to all Americans.

The FCC has also spent significant time working on these issues. They have produced and have been working diligently to update maps of broadband coverage across the country, so that additional investments can be put to the best use in places that have no or severely limited broadband access. The FCC has also worked on making internet access more affordable, including their Affordable Connectivity Program offering free and heavily discounted broadband

to millions of people. The FCC has also worked to improve equity in internet access, studying and working to minimize the digital divide and homework gap. It has also housed the E-rate program to ensure all students have the ability to learn online and access classes, lessons, and other digital work. The FCC has even started to consider rules to ban digital discrimination. This commission should certainly be included in working to improve youth online health and safety.

The FTC has also been involved in youth online health and safety in a couple of areas, most specifically as the COPPA-empowered privacy regulator. The FTC has been the lead enforcer of COPPA for more than 20 years and has continued to use its authority on an ongoing basis. It has promulgated rulemaking, brought many enforcement actions, and issued guidance and policy statements. It is positive that the FTC has become COPPA experts, but the Commission is in need of more staff and funding in order to better protect children online. As countries around the world regulate in this space, they either set up whole new agencies or dramatically increase staffing and funding for existing departments to the point that the FTC is dwarfed in its size and limited in its efficacy on these important issues.

Regarding Question 16(d): These experts and medical professionals should be included from the onset and on an ongoing basis, if/when the United States provides guidance about this. These individuals should be hired as part of the staff that is overseeing this guidance, and its implementation to ensure that it is evidence-based and reflects the latest research and medical recommendations.

Regarding Question 16(e): Learn from the UK's iterative approach, particularly the ICO enforcing the AADC. Instead of immediately seeking to sue, have productive conversations with industry about where the pain points in compliance are, issue more detailed guidance, and potentially update or clarify regulations as necessary.

Regarding Question 17: Whatever legislation or regulation is pursued, it should be evidence-based. We are grateful for the passage of CAMRA last Congress, but the essential research that will be funded by it is overdue. Other countries have conducted very valuable research into youth health, privacy, and safety, and we should follow their lead and learn from their efforts by taking a thoughtful and nuanced approach to regulation. There is no easy, one size fits all approach, but instead a balance to aim for and tradeoffs to consider between different priorities.

Regarding Question 18: Establishing the office of Chief Online Safety Officer to serve as a point person would help the US government speak with one voice. It would also fit well internationally, as countries set up their own online safety commissioners and the Digital Services Act requires a point of contact person to be named by each EU government. There is also the Global Online Safety Regulators Network that was launched at FOSI's 2022 annual

conference and has since expanded to include more countries as online safety becomes a key policy priority for governments around the world. A US Chief Online Safety Officer could be the US representative to that international network.

Identifying Unique Needs of Special Communities

Regarding Question 19: More information can be found above in relation to Question 1(e).

Reliable Sources of Concrete Information

Regarding Question 20(b): As explained in the answer to question 18, the Chief Online Safety Officer would be a trusted source for relevant information in this area.

Regarding Question 21(a): Longitudinal studies are particularly important to track the impact of technologies and platforms on youth development over time. As mentioned above, passing CAMRA was a great step since it creates exactly these types of studies. However, it will take years to glean the results of this type of research, and we must ensure that Congress continues to fund such efforts.

Regarding Question 22: Yes, transparency is generally good and an important best practice. But any transparency or researcher access requirements must carefully consider how much personal data would be shared and handled in the most privacy preserving way possible. Also, consistency and harmonization are important. It would be a best practice to make similar platforms have to issue substantively similar and comparable transparency reports, that are also consistent internationally, so that not each country (or even each state) requires different information from each other.

Conclusion

FOSI commends the NTIA for examining the harms, benefits, current best practices, research, and role of government in keeping young people safe online. FOSI hopes that the interagency Task Force on Kids Online Health and Safety is only the beginning of this Administration's work in online safety. Ideally, this work would be concentrated in a new office of the Chief Online Safety Officer that would coordinate across agencies and departments, the government would continue to address youth online safety with a nuanced perspective that takes into account both the harms and benefits of digital life, relevant research (such as that directed by CAMRA) would be funded and prioritized, industry best practices would be adopted by platforms to create a minimum standard of online protections for young users, and policymakers would pass thoughtful, evidence-based regulations.

Thank you for the opportunity to comment. FOSI looks forward to working with NTIA on these important issues, and hopefully participating in the Roundtables on this subject.

Respectfully submitted,

Andrew Zack
Policy Manager
Family Online Safety Institute