ENOUGH·IS·ENOUGH®

Making the Internet Safer for Children and Families

COMMENTS SUBMITTED BY ENOUGH IS ENOUGH

BEFORE

THE NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

U.S. DEPARTMENT OF COMMERCE

NOTICE, REQUEST FOR COMMENT

Docket No. 230926-0233

Document Citation: 88 FR 67733

Publication Date: November 15, 2023

Submitted By:

Donna Rice-Hughes, CEO

November 14, 2023

Enough.org
InternetSafety101.org

ENOUGH IS ENOUGH

NTIA REQUEST FOR COMMENTS ON KIDS' ONLINE HEALTH AND SAFETY

NOVEMBER 2023

INTRODUCTION

In the rapidly evolving landscape of the digital age, children are growing up immersed in a world where the internet serves as both a vast playground and an intricate labyrinth of information. While the internet opens doors to unparalleled opportunities for learning and communication, it also unfurls a tapestry of dangers that pose significant threats to the well-being of our youngest netizens. This response delves into the multifaceted reasons why the internet can be perilous for children, examining the nuanced challenges they face as they navigate this expansive virtual realm. By shedding light on the various risks inherent in online spaces, we aim to provoke thoughtful discourse and inspire proactive measures to safeguard the digital innocence of our future generations.

Enough Is Enough (EIE), a non-partisan, 501(c)(3) non-profit organization, emerged in 1994 as the pioneering leader on the front lines of efforts to prevent the internet-enabled exploitation of children. On a mission to make the internet safe for children and families, EIE is dedicated to raising public awareness about the dangers of internet pornography, sexual predators and traffickers, and other dangers.EIE advances solutions that promote equality, fairness and respect for human dignity while promoting a shared responsibility between the public, technology, and the law. EIE stands for freedom of speech as defined by the Constitution of the United States; for a culture where all people are respected and valued; for a childhood with a protected period of innocence; and for a society free from sexual exploitation.

EIE is pleased to confirm its endorsement of the joint response crafted by the Ending OSEAC Coalition. In alignment with the principles articulated in that response, EIE also submits this statement independently, reinforcing our commitment to the shared objectives outlined in the coalition's collective effort.

WHAT ARE THE RISKS?

The online world, while offering many benefits, poses significant risks to the mental and physical health, privacy, and safety of children and minors. Exposure to explicit or violent content, cyberbullying, social comparison, and excessive screen time can have detrimental effects on their emotional well-being.

POTENTIAL MENTAL AND PHYSICAL HARMS

One of the most pressing concerns regarding the online environment is the inadvertent exposure of children to inappropriate or obscene content. The unrestricted nature of the internet means that children can come across explicit, violent, or otherwise distressing material. Such exposure can lead to heightened levels of anxiety, distress, and, in extreme cases, desensitization to violence, which can have long-lasting effects on their mental health. The Surgeon Generarecently issued an advisory regarding the online health and safety of children, noting social media presents a ‘profound risk of harm to kids’. Parents and guardians are advised to be vigilant and proactive in monitoring their children's online activities to ensure a secure and healthy digital environment, while calling on governments to take action.[1]

[1] Social Media and youth mental health - hhs.gov. (n.d.). https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf

Another significant threat in the digital age is cyberbullying. This form of harassment involves the use of digital platforms for threats, humiliation, or other forms of mistreatment. Victims of cyberbullying often suffer from depression, anxiety, and feelings of helplessness. Such experiences can erode their self-esteem and have severe consequences for their overall mental well-being. Nearly half (46%) of teens age 13-17 have been bullied or harassed online, with physical appearance being seen as a relatively common reason why.[2] Likewise, young people (10-16 years) who accessed or shared sexual content or images of cyberbullying or violence had up to a 50% higher risk for thoughts of suicide.[3]

Social media platforms encourage users to compare their lives with those of others. This comparison can lead to unrealistic standards of success, beauty, and happiness. Children and teenagers may experience pressure to conform to these standards, resulting in feelings of inadequacy, anxiety, and depression as they strive to meet these unrealistic expectations which lead to further physical consequences, like disordered eating and self-mutilation.

Additionally, excessive screen time, particularly on social media and in video games, can lead to addiction-like behaviors. The consequences include sleep disturbances, impaired academic performance, and emotional instability, and while neglecting their offline responsibilities and relationships, these feelings of isolation and loneliness grow.

In 2022, Bark (a parental control tool) analyzed more than 4.5 billion online activities from teens and tweens across the U.S, Bark found that: 35.7% of tweens and 64.3% of teens were involved

---

[2] Vogels, E. A. (2022, December 15). *Teens and cyberbullying 2022*. Pew Research Center: Internet, Science & Tech. https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/

[3] Sumner SA, Ferguson B, Bason B, et al. Association of Online Risk Factors With Subsequent Youth Suicide-Related Behaviors in the US. *JAMA Network Open.* 2021;4(9):e2125860. doi:10.1001/jamanetworkopen.2021.25860

in a self-harm/suicidal situation; 62.4% of tweens and 82.2% of teens encountered nudity or content of a sexual nature; 9.4% of tweens and 14.2% of teens encountered predatory behaviors from someone online; 4.4% of tweens and 15.1% of teens engaged with or encountered content about disordered eating; 19.3% of tweens and 41.2% of teens used language or were exposed to language about anxiety; 71.2% of tweens and 83.3% of teens experienced bullying as a bully, victim, or witness; 23.6% of tweens and 44.1% of teens engaged in conversations about depression; 75.0% of tweens and 88.2% of teens expressed or experienced violent subject matter/thoughts; and 66.0% of tweens and 84.8% of teens engaged in conversations surrounding drugs/alcohol.[4]

POTENTIAL SAFETY AND PRIVACY RISKS

Children's online activities often involve the collection of personal information, such as their name, age, location, and browsing habits. Tech companies and websites gather this data for various purposes, including targeted advertising. This data can be used to create detailed profiles of children, which can be exploited for marketing purposes and potentially invasive surveillance. This personal information can be stored online, making it vulnerable to data breaches. When these breaches occur, the exposed data may be used for identity theft, financial fraud, or other malicious purposes, putting children's privacy and security at risk. Seventy-two percent of Americans believe their accounts are secure with only usernames and passwords, yet every two seconds there is another victim of identity fraud.[5]

Additionally, the internet provides a platform for predators to target children. Children may unknowingly and willingly share personal information online, making it easier for malicious

---

[4] *Bark's annual report 2022*. Bark. (2023, January 10). https://www.bark.us/annual-report-2022/

[5] Stop. Think. Connect .(n.d.) "**Lock Down Your Login**", accessed 1-16-2017 from https://www.lockdownyourlogin.com.

individuals to identify and approach them. This puts children at risk of exploitation, grooming, or harassment. Research conducted by the UK's National Society for the Prevention of Cruelty to Children found that children that have shared feelings of vulnerability online are at higher risk of being targeted and groomed by offenders online.[6]

What children post online can have long-lasting consequences. Content shared on the internet can be difficult to remove entirely, and it may resurface in the future, affecting educational and employment opportunities. Children may not fully comprehend the permanence of their digital footprints.

INDUSTRY FAILURE

THE BURDEN HAS FALLEN ON PARENTS

Without some form of federal regulation or guardrails, the industry will continue to fail to protect children online. Many parents struggle to monitor and control their children's online activities effectively. Children often are more tech-savvy than their parents, making it challenging to implement effective safeguards. Lack of parental oversight can lead to children accessing obscene content, interacting with strangers, or engaging in risky behavior. 79% of parents use controls currently or in the past; 2/3 of parents are generally unsatisfied with the tools they have to keep kids safe online and although house rules are common, 65% of parents have used a type of digital tool in the form of in-app solutions, parental controls, safety features, privacy settings or digital usage restrictions.[7]

---

[6] Nspcc. (n.d.). *Lonely children are twice as likely to be groomed online*. NSPCC. https://www.nspcc.org.uk/about-us/news-opinion/2020/coronavirus-children-groomed-online/

[7] Tools for Today's Digital Parents: The role of parental controls in the digital lives of American parents and children, *Family Online Safety Institute*, (2020).

Online sexual exploitation has irreparable consequences for the most vulnerable in our communities, namely our children. Yet, for decades, children have had unprotected access to the digital world via a myriad of internet-enabled devices. Unfortunately, no child is immune from online sexual exploitation. Vulnerable children are open prey for savvy predators, traffickers and pornographers with a sexual appetite for children. The digital world is the new playground for children and predators. *Predators prey where children play.* Vulnerable children are open prey for savvy predators, traffickers and pornographers with a sexual appetite for children.

Predators can hide behind electronic devices as they anonymously groom unsuspecting children, manipulating them into a sexual encounter, blackmailing them into silence and selling images and videos of their abuse, all facilitated by the multi-billion-dollar tech industry. Sadly, millions of children and families have suffered due to greed for profit by interactive technology companies. Instead of protecting children, they knowingly allowed them to be abused and exploited.

It is estimated that online sexual exploitation and abuse of children increased by a staggering 422% over the past 15 years.[8] In 2019, The New York Times ran the article: "The Internet Is Overrun With Images of Child Sexual Abuse. What Went Wrong?" Its reporting exposed the widespread neglect and disregard for child safety shown by large tech companies, even when obvious examples of child sexual abuse material (CSAM) were brought to their attention.[9]

---

[8] Rice-Hughes, D. (2022, February 7). *Dismantling Big Tech's immunity from online child abuse material*. The Washington Times. https://www.washingtontimes.com/news/2022/feb/7/dismantling-big-techs-immunity-from-online-child-a/

[9] Keller, M. H., & X, G. J. (2019, September 29). *The internet is overrun with images of child sexual abuse. what went wrong?*. The New York Times. https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html

Recently, a former Meta security expert turned whistleblower reported he tried to address Instagram's teen safety issues with CEO Mark Zuckerbergbut received no response. [10] What's particularly alarming is that his concerns were brought to light through his 14-year-old child's experience with the app, revealing predatory behavior.[11] Children are in desperate need of Big Tech being held accountable for their exploitation online.

There needs to be a dramatic paradigm shift regarding Big Tech's response to child online sexual exploitation for the internet to be safer for children. While there has been some success with some industry lead efforts to protect children using internet platforms, the industry continues to evade responsibility. This is largely due to the broad liability immunity Congress granted online platforms under Section 230 of the Communications Decency Act passed in 1996. We have seen that after decades of no regulation and liability protection, the Big Tech business model is the problem and we know that we can no longer rely upon the industry to ensure online safety for children.

Compounding issues over the exponential growth of reported online child sexual exploitation is the growing concern of Artificial Intelligence-generated Child Sexual Abuse Material (AIG-CSAM). The White House recently issued an "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," noting the potential of artificial intelligence to "exacerbate societal harms." The EO calls for a report from the Secretary of Commerce, in consultation with the heads of other relevant agencies, to identify the "existing standards, tools, methods, and practices, as well as the potential development of further

---

[10] Horwitz, J. (2023, November 8). *His job was to make Instagram safe for teens. his 14-year-old showed him what the app was really like.* The Wall Street Journal. https://www.wsj.com/tech/instagram-facebook-teens-harassment-safety-5d991be1

[11] ibd

science-backed standards and techniques" for "preventing generative AI from producing child sexual abuse material or producing non-consensual intimate imagery of real individuals (to include intimate digital depictions of the body or body parts of an identifiable individual)."[12] Among the dangers AI poses include the creation of these"deepfake" scenarios — videos and images that have been digitally created or altered with artificial intelligence or machine learning — of a child that has already been abused, or the alteration of the likeness of a real child from something like a photograph taken from social media, so that it depicts abuse.[13]

FEDERAL GOVERNMENT ACTION IS NECESSARY

Protecting children online requires federal leadership. There are several areas where the federal government can lead and help to address the online safety crisis plaguing American children.

OBSCENITY ENFORCEMENT

One immediate step that the Administration can take is to enforce existing obscenity laws that are already on the books. The U.S. Department of Justice has not enforced laws to prevent the online exploitation of children, including federal obscenity laws, since Attorney General

---

[12] The United States Government. (2023, October 30). *Executive order on the safe, secure, and trustworthy development and use of artificial intelligence*. The White House. https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

[13] *Prosecutors in all 50 states urge Congress to strengthen tools to fight AI Child Sexual Abuse Images*. NBCNews.com. (2023, September 6). https://www.nbcnews.com/tech/tech-news/prosecutors-50-states-urge-congress-strengthen-tools-fight-ai-child-se-rcna103587

Ashcroft, under the Bush administration. In the spring of 2005, alongside Assistant Attorney General Christopher Wray, AG Ashcroft established an Obscenity Task Force. This task force was dedicated to addressing issues related to obscenity, specifically in the realm of pornography.[14] The task force cooperated with various law enforcement agencies and U.S. Attorney's Offices across the country to prosecute individuals and entities involved in the production, distribution, and sale of obscene materials. Their efforts led to numerous convictions, significant fines, asset forfeitures, and played a role in deterring criminal conduct within the pornography industry. Under the Obama administration, Attorney General Eric Holder dissolved the Obscenity Prosecution Task Force in the criminal division of the Justice Department in 2011.[15]

Enforcing obscenity laws requires a multi-faceted approach that addresses the challenges of the digital age while respecting constitutional rights. To improve the enforcement of obscenity laws, law enforcement agencies, including the DOJ and the CEOS, need enhanced resources and training to combat these crimes effectively. Allocating sufficient funding and manpower to investigate and prosecute obscenity cases is crucial. Additionally, collaboration and information-sharing between national and international law enforcement agencies are vital to address the transnational nature of explicit content distribution. Emphasizing the use of technology and digital forensics can aid in the identification and tracking of offenders. Encouraging public awareness campaigns to educate individuals, especially parents and

---

[14] US Department of Justice. OBSCENITY PROSECUTION TASK FORCE ESTABLISHED TO INVESTIGATE, PROSECUTE PURVEYORS OF OBSCENE MATERIALS. May 5, 2005. https://www.justice.gov/archive/opa/pr/2005/May/05_crm_242.htm

[15] Gerstein, Josh. "Holder Accused of Neglecting Porn." *POLITICO*, 2011, www.politico.com/story/2011/04/holder-accused-of-neglecting-porn-053314.

guardians, about the risks of obscenity and how to report potential violations can lead to increased reporting of such crimes. Striking a balance between preserving freedom of speech and protecting minors requires ongoing legal refinement and staying current with societal norms and technological advancements. Overall, a comprehensive strategy that combines adequate resources, technological expertise, international cooperation, and public engagement can enhance the enforcement of obscenity laws effectively.

In the past, congressional committees have employed report language to call on the DOJ to prioritize the prosecution of obscenity cases. These reports often highlight concerns about the proliferation of explicit and hardcore pornography, especially content featuring extreme and potentially harmful themes. Such report language serves as a formal communication from Congress to the DOJ, urging the department to take concrete actions in enforcing obscenity laws. Recent report language calling on the DOJ to prosecute obscenity include

> Rept. 117-97 - COMMERCE, JUSTICE, SCIENCE, AND RELATED AGENCIES APPROPRIATIONS BILL, 2022 Monday, July 19, 2021.
>
> P. 63: Federal obscenity prosecution. —The Committee supports the work of DOJ in investigating and prosecuting major producers and distributors of hardcore adult pornography that meets the Supreme Court test for obscenity. Such enforcement is necessary to protect the welfare of families and children as traffickers in illegal adult obscenity seek to extend their influence through advances in technology. The Committee directs DOJ to increase its efforts in enforcing Federal obscenity laws.

While this report language has been ignored by the DOJ, The Supreme Court of the United States has recognized that obscenity and child pornography laws are still in effect, both for

physical transfers and electronic transfers, noting in Reno v. ACLU, 521 U.S. 844, 878 n. 44, 117 S.Ct. 2329, 2347 n. 44 (1997), that “Transmitting obscenity and child pornography, whether via the Internet or other means, is already illegal under federal law for both adults and juveniles.”

The solution to the issue of the proliferation of explicit and hardcore obscenity that meets the Supreme Court's test for obscenity involves a strategic and proactive approach by law enforcement agencies, including the DOJ investigating and prosecuting major producers and distributors of such materials. By focusing on major producers and distributors, law enforcement can have a more significant impact on curbing the spread of obscene content.

Likewise, Enough Is Enough suggests reinstating the Federal Obscenity Training Symposium initiated under AG Ashcroft. This symposium invited federal prosecutors, DOJ officials, US attorneys, and assistant US attorneys to learn how to successfully prosecute obscenity cases.

SUPPORTING CHILD PROTECTION BILLS

In an age where children spend a significant amount of their time online, it is imperative to protect them from the potential dangers and threats lurking on the internet. Enough Is Enough urges the federal government to bring a package of complementary child protection bills to the floor for a vote. This package includes EARN IT (Eliminating Abusive and Rampant Neglect of Interactive Technologies) Act of 2023; Kids Online Safety Act of 2023; Project Safe Childhood Act; REPORT Act (Revising Existing Procedures on Reporting via Technology); and STOP CSAM Act (Strengthening Transparency and Obligations to Protect Children Suffering from Abuse and Mistreatment). By supporting the following bills, legislators can come together in a b-partisan fashion to achieve this goal and keep kids safe online.

- The EARN IT Act of 2023 is a crucial step in holding online platforms accountable for the content shared on their platforms while ensuring the protection of children from exploitative and harmful material. This piece of legislation removes Section 230 blanket liability protection from service providers in the area of child sexual abuse material on their sites.[16]
- As a complementary bill to the EARN IT Act of 2023, the Kids Online Safety Act of 2023 provides comprehensive measures to enhance the safety of children on the internet, addressing issues such as online bullying, predatory behavior, and the exposure of inappropriate content to minors.[17]
- Project Safe Childhood Act is crafted to combat child exploitation and abuse, with the purpose of protecting children from all forms of abuse and mistreatment, especially in the digital realm.[18]
- REPORT Act focuses on revising existing procedures on reporting via technology, enabling more efficient and effective reporting of online child exploitation and abuse cases.[19]

---

[16] Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2023, S. 1207, 118th Cong. (2023). https://www.judiciary.senate.gov/imo/media/doc/earn_it_act_of_2023_-_s1207.pdf

[17] The Kids Online Safety Act of 2023, S. 1409, 118th Cong. (2023). https://www.congress.gov/118/bills/s1409/BILLS-118s1409is.pdf

[18] Project Safe Childhood Act, S. 1170, 118th Cong. (2023). https://www.congress.gov/bill/118th-congress/senate-bill/1170/text

[19] Revisiting Existing Procedures On Reporting via Technology Act, S. 474, 118th Cong. (2023). https://www.govinfo.gov/app/details/BILLS-118s474rs

- The STOP CSAM Act is a crucial piece of legislation aimed at strengthening transparency and obligations to protect children suffering from abuse and mistreatment online.[20]

These bills strike a critical balance between ensuring children's safety and preserving the fundamental principles of online freedom. By supporting and championing these measures, policy makers across the country can make a significant contribution to the well-being of this nation's children and youth. The Administration should actively support these legislative efforts.

SAFE PUBLIC AND RESTRICTING/EMPLOYEE WIFI

Today, any child with unrestricted internet access is just a click or swipe away from viewing, either intentionally or accidentally, sexually explicit material online, from adult pornography to prosecutable obscene material depicting graphic sex acts, live sex shows, orgies, bestiality, and violence. Even illegal material depicting the sexual abuse of a child—once only found on the black market—is instantly available and accessible on the internet and is easily discovered on unfiltered WiFi networks.

Enough Is Enough's Safe WiFi[SM] campaign calls on the federal government and corporate America to filter pornography and child sexual abuse images on its public WiFi so that children, youth, families and adults can be provided a safer, more secure WiFi environment.[21] By implementing a safe, friendly WiFi policy and effective filtering, the federal government and corporations alike can:

---

[20] Strengthening Transparency and Obligations to Protect Children Suffering from Abuse and Mistreatment Act, S. 1199, 118th Cong. (2023). https://www.congress.gov/118/bills/s1199/BILLS-118s1199rs.pdf

[21] "Enough Is Enough: Porn-Free WIFI." *Enough Is Enough*, enough.org/safewifi. Accessed 9 Nov. 2023.

- Prevent youth from being exposed to pornography and child sexual abuse material when using public and private WiFi services;
- Prevent youth from easily bypassing filters and other parental control tools set up by their parents on their smartphones, tablets and laptops by logging onto open hotspots;
- Prevent sexual predators from accessing illegal child sexual abuse material and flying under the radar of law enforcement by using free WiFi services;
- Avoid a potential hostile work environment for employees; and
- Maintain consistency regarding corporate best practices and family-friendly policies.[22]

We urge the Administration to direct the General Services Administration (GSA) to require that all internal and public WiFi networks be filtered from both CSAM and pornography, on federal tax-payer funded properties and networks. A former federal employee was sentenced to eight years in prison after repeatedly connecting his cellphone to the internet inside the Library of Congress to view and download child pornography.[23]

DEVICE SAFETY

Filtering mechanisms play a pivotal role in safeguarding children from inappropriate content, cyberbullying, and other online dangers. Parents, educators, and device manufacturers can employ various tools and software solutions to regulate the content accessible to children. These filters can be categorized into content filters, application filters, and time controls.

---

[22] "Enough Is Enough: Porn-Free WIFI." *Enough Is Enough*, enough.org/safewifi. Accessed 9 Nov. 2023.

[23] Mondeaux, C. (2022, July 21). *Ex-federal employee sentenced for viewing child pornography on Library of Congress Wi-Fi*. Washington Examiner. https://www.washingtonexaminer.com/news/crime/ex-federal-employee-sentenced-viewing-child-pornography-library-congress-wifi

In five states including UTAH, device filtering legislation has been successfully adopted and implemented. Utah Code §76-10-1231 modifies the Utah Criminal Code regarding an internet service provider's responsibility to offer content filtering methods for materials harmful to minors. Customers of internet service providers now have the right to request that material harmful to minors be blocked.[24]

Safety by design is a proactive approach to device safety, emphasizing the integration of safety features during the development phase of digital products. By embedding safety measures into the design of devices, manufacturers can create an environment that prioritizes the well-being of young users. Devices should be designed with age-appropriate interfaces, ensuring that young users can navigate them comfortably and safely. User interfaces should be intuitive, minimizing the risk of accidental exposure to inappropriate content. Children's privacy is a crucial consideration in device safety. Manufacturers should implement robust privacy protection measures, such as strict data encryption and secure authentication processes, to safeguard children's personal information from potential threats. Safety by design can also involve integrating educational features that promote digital literacy and responsible online behavior. Devices can include built-in tutorials, pop-up notifications about potential risks, and interactive content that educates children about online safety.

The Administration should advocate for similar federal legislation to encourage device filtering.

---

[24] *Internet service provider content filtering*. dcp.utah.gov. (2023, April 21). https://dcp.utah.gov/education/internet-service-provider-content-filtering/#:~:text=Utah%20Code%20%C2%A776%2D10%2D1231%20modifies%20the%20Utah%20Criminal,harmful%20to%20minors%20be%20blocked.

NTIA SHOULD ESTABLISH AN OFFICE OF INTERNET SAFETY

We urge the Administration to establish an Office of Internet Safety within NTIA. To date, there are no federal grant programs focused on internet safety prevention and education. Currently, NTIA is distributing billions of dollars to expand internet access which is vital for our nation's economy and to address social and economic barriers faced by millions of Americans. We believe that it is equally important that NTIA have a similar focus on internet safety and that the agency establish an office that would focus federal leadership to promote best practices, encourage industry participation in internet safety efforts, and fund internet safety education at the national level.

The online landscape is dynamic and constantly evolving, presenting new challenges and threats to children's safety. Cyberbullying, inappropriate content, online predators, and other risks persistently emerge, necessitating a swift and adaptive response. Establishing an Internet Safety Grant Program would empower organizations to stay ahead of these challenges, enabling the development of innovative solutions and strategies to protect children in the ever-changing digital environment.

The Internet Safety Grant Program would empower non-profit organizations, educational institutions, and community groups to actively engage in initiatives that promote online safety for children. By providing financial support, the federal government can catalyze the efforts of these stakeholders, fostering collaborative projects that leverage diverse expertise to address the multifaceted nature of online threats. Likewise, a dedicated grant program can support research and development activities focused on understanding the evolving digital landscape and its impact on children. By funding studies, surveys, and analyses, the NTIA can ensure

evidence-based policymaking, leading to effective interventions that resonate with the realities of children's online experiences.

The NTIA has an opportunity to facilitate the creation of educational campaigns and outreach programs targeting parents, educators, and caregivers through the grant program. These initiatives can raise awareness about online risks, equip adults with the knowledge to guide children responsibly, and promote a collective commitment to fostering a safer online environment.

The implementation of this grant program can be accomplished through strategic and competitive granting process, collaboration and partnerships, and periodic evaluations and reporting.

The NTIA should institute a competitive granting process, inviting proposals from qualified organizations with a demonstrated commitment to online safety. Rigorous evaluation criteria should prioritize initiatives that are innovative, scalable, and have the potential to make a lasting impact on children's digital well-being. Additionally, the NTIA would encourage collaborative projects that involve partnerships between non-profit organizations, academic institutions, industry stakeholders, and government agencies. By fostering collaboration, the grant program can leverage a diverse range of perspectives and expertise, ensuring comprehensive approaches to online safety. Finally, implement a robust system for monitoring and evaluating the effectiveness of funded projects. Grantees should be required to provide regular progress reports, enabling the NTIA to assess the impact of the initiatives and make informed decisions about ongoing support and future program enhancements.

The establishment of an Internet Safety Grant Program by the NTIA represents a critical step toward addressing the complex challenges posed by children's online experiences. By fostering innovation, collaboration, and research, this initiative can empower stakeholders to create lasting solutions, ultimately contributing to a safer and healthier digital environment for our nation's youth.

FUTURE INDUSTRY EFFORTS TO MITIGATE HARMS

The NTIA's request for comment also seeks input regarding future industry efforts to mitigate online harms. Like the national public education campaign on the risks of smoking funded by Big Tobacco, there needs to be a national public education campaign on the risks of online harms funded by Big Tech. The Nation's tobacco industry was forced to fund the outreach effort to help undue some of the harms it unleashed on society. That approach was largely successful and smoking rates among key demographics greatly reduced. That same approach can be applied here to reduce online harm currently destroying children's lives and our society. Further, the campaign should be conducted through both traditional and digital media. This will help ensure the messaging reaches all the necessary stakeholders, including parents.

The NTIA can play a powerful role in encouraging industry to create a national public education campaign funded by Big Tech. Concurrently, the NTIA could support legislation establishing such a program. The NTIA would be uniquely positioned to provide oversight of this critical effort.

A national public education campaign would be one of the most impactful in mitigating online risks to our children. The two most important resources are our children and time. If the federal government does not create this now, we will never get the future back.

INDUSTRY BEST PRACTICES

As we advocate for robust federal initiatives to enhance online safety for children, it is imperative to acknowledge and promote best industry practices that can serve as a model for creating a safer digital environment. Industry stakeholders, including technology companies, social media platforms, and content providers, play a pivotal role in shaping the online experiences of children. By adhering to and advancing best practices, these entities can contribute significantly to the overall goal of fostering a secure online space for our nation's youth.

Industry leaders should prioritize the development of age-appropriate content and user interfaces tailored to the cognitive and emotional capacities of different age groups. Implementing intuitive design features and robust content filtering mechanisms can help prevent inadvertent exposure to inappropriate material, creating a safer online space for children. In conjunction with age-appropriate content, companies should adopt transparent privacy policies that clearly outline data collection practices and ensure compliance with relevant privacy regulations. Furthermore, providing robust parental controls empowers caregivers to monitor and control their children's online activities, striking a balance between privacy and protection.

Encouraging digital literacy and responsible online behavior should be integral to industry practices. Educational initiatives, tutorials, and age-appropriate content can help children

develop the skills needed to navigate the online world safely. Additionally, platforms can promote awareness among parents and educators regarding the importance of active involvement in children's digital lives. This may include content moderation. Social media platforms and online communities must implement proactive content moderation strategies to swiftly identify and remove harmful content. Implementing reporting mechanisms empowers users, including children, to flag inappropriate content or interactions, fostering a sense of community responsibility for online safety.

As always, collaboration between industry stakeholders and child advocacy organizations, like Enough Is Enough, is essential. By working together, these entities can share insights, best practices, and technological advancements to collectively address emerging challenges. Establishing regular forums for collaboration can foster an ongoing dialogue and contribute to the development of effective strategies.

Last but not least, it is critical for companies to conduct regular audits of their safety features, privacy policies, and content moderation systems. Transparently reporting the results of these audits demonstrates a commitment to accountability and continuous improvement, instilling confidence in users and regulatory bodies alike.

As we navigate the ever-evolving digital landscape, industry leaders must embrace a shared responsibility for children's online health and safety. By adopting and championing these best practices, technology companies can not only comply with regulatory standards but also become advocates for positive change, fostering an online environment where the well-being of children is prioritized. This collaborative effort between government, industry, and advocacy groups is crucial for creating a holistic and effective approach to protecting our youth in the digital age.

CONCLUSION

Enough Is Enough extends our sincere gratitude to the NTIA for its dedicated commitment to fostering the well-being of our nation's youth. By proactively seeking input from stakeholders through its request for information, the NTIA demonstrates a keen understanding of the evolving challenges in the digital landscape. This inclusive approach is critical in ensuring that the unique needs of children are not overlooked or left behind. The time and resources invested by the NTIA to gather insights and perspectives from diverse stakeholders are invaluable steps toward crafting comprehensive policies that prioritize the online safety of our children. Together, through collaborative efforts and open dialogue, we can create a digital environment that nurtures the growth and development of our youth while safeguarding them from potential harm.

Respectfully Submitted

Donna Rice-Hughes, CEO and President
Enough Is Enough
Date: November 15, 2023