Online Health and Safety for Children and Youth: Best Practices for Families and Guidance for Industry

KIDS ONLINE HEALTH AND SAFETY TASK FORCE

Table of Contents

Letter from the Task Force Co-Chairs

Digital technology is ubiquitous in the lives of today's youth. The vast majority of young people regularly use social media and other online platforms to communicate, explore, and learn about topics and express themselves.

In many cases, digital media can be beneficial to youth, allowing them to build community, connect with others, and learn. However, a growing body of research, coupled with the testimonies of parents, caregivers, and young people themselves, indicate that kids can also be negatively impacted by an array of harms that can occur or be facilitated online. These include harassment, cyberbullying, child sexual exploitation and abuse, and exposure to content that exacerbates mental health issues, such as the promotion of eating disorders. These harms threaten the safety and well-being of young people.

In response to these concerns, on May 23, 2023, the Biden-Harris Administration announced a new interagency Task Force to advance the health, safety, and privacy of youth online, as well as identify measures and methods for addressing the adverse health effects minors experience while using online platforms.

The Task Force has been led in partnership by the Department of Health and Human Services (HHS), through the Substance Abuse and Mental Health Services Administration (SAMHSA), and the Department of Commerce, through the National Telecommunications and Information Administration (NTIA). It included a cross-section of leaders and experts from across the federal government.

The report that follows represents the output of this Task Force's efforts. It offers an overarching summary of young people's use of online platforms and the risks and benefits to their health, safety, and privacy. As requested, it provides key Task Force guidance, including: (1) Best Practices for Parents and Caregivers, (2) Recommended Practices for Industry to Promote Youth Online Health, Safety, and Privacy, (3) a Research Agenda identifying domains of further inquiry. The report concludes with a section outlining areas of future work for various stakeholders, including the federal government.

We would like to thank the many people—including youth advocates, civil society organizations, academic researchers, and other experts—who so generously provided input and contributions to the Task Force. We are grateful for their hard work and dedication to youth health and safety in digital environments.

The issues discussed here are complex and important. We are proud of the ongoing work on these challenges at the federal level. But as our report indicates, there is a need for further efforts—including bipartisan legislation to promote accountability for online platforms, as the President has repeatedly underscored. We look forward to further collaboration to protect and strengthen the mental health, safety, and privacy of youth.

Thank you,

Miriam Delphin-Rittmon

Assistant Secretary for Mental Health and Substance Use and Administrator, Substance Abuse and Mental Health Services Administration (SAMHSA)

Alan Davidson

Assistant Secretary of Commerce for Communications and Information and Administrator, National Telecommunications and Information Administration (NTIA)

Introduction

Young people today are surrounded by digital technology and have grown up regularly engaging with social media and online platforms through computers, smartphones, and other electronic devices. Research indicates that approximately 95% of teenagers and 40% of children between the ages of eight and 12 years use some form of social media.[1, 2, 3] Due to the widespread use of social media and online platforms among youth, it is critical to examine the scope of their impact and to cultivate safe and healthy online spaces that help promote overall well-being. This is particularly important given the youth mental health crisis in the United States.[4]

Digital technology use has the potential to both benefit young people's well-being and to expose them to significant harms. The use of social media and digital technology can provide opportunities for self-directed learning, forming community, and reducing isolation.[5, 6] This can be especially important for youth who are marginalized or experiencing mental distress.[7, 8, 9, 10] Despite these benefits, social media use has been associated with harms to physical and mental health,[11, 12, 13] including through exposure to bullying, online harassment, and child sexual exploitation.[14, 15] For example, a 2022 survey of teens found that about half experienced some form of cyberbullying, including being harassed and being sent explicit images that they did not request.[16] And adolescents who seek out information about health and safety topics online risk encountering inaccurate information that can be unhelpful or actively dangerous.[17]

Recognizing the importance of addressing this complex issue, the Biden-Harris Administration announced on May 23, 2023, the creation of an interagency Task Force on Kids Online Health and Safety.[18] The Administration is committed to efforts to strengthen protections for children's health, safety, and privacy online, and has called for bipartisan legislative action.[19] This Task Force builds on prior work on kids' online health and safety across the federal government, including the 2023 U.S. Surgeon General's Advisory on Social Media and Youth Mental Health, and recommendations from the White House Task Force to Address Online Harassment and Abuse.[20, 21]

Over the past year, members of the Task Force have worked to prioritize options and identify best practices for supporting youth and their families who have experienced—or are at risk of experiencing—adverse health effects and harm associated with online platforms. This report highlights those efforts and identifies knowledge gaps where further work is needed.

This report summarizes the evidence on young people's use of online platforms and the risks and benefits to their health, safety, and privacy. Based on the identified challenges to youth health, safety, and privacy, the report includes guidance on the following topics to help accomplish the goals of supporting youth and their families:

(1) Best Practices and Resources for Parents and Caregivers:

- ✓ Overarching framework for children and youth media use.
- ✓ Strategies for parents and caregivers.
- ✓ Handouts and conversation starters to help parents and caregivers engage their children in conversations about online platforms and technology use.
- ✓ A searchable compendium of a set of widely endorsed best practices for parents and caregivers.

(2) A Set of Recommended Practices for Industry, which provides tools and interventions that the Task Force suggests industry implement to improve kids' health, safety, and privacy on online platforms. This includes guidance on ways to:

- ✓ Design age-appropriate experiences for youth users.
- ✓ Make privacy protections for youth the default.
- ✓ Reduce and remove features that encourage excessive or problematic use by youth.
- ✓ Limit "likes" and social comparison features for youth by default.
- ✓ Develop and deploy mechanisms and strategies to counter child sexual exploitation and abuse.
- ✓ Disclose accurate and comprehensive safety-related information about apps.
- ✓ Improve systems to address bias and discrimination that youth experience online.
- ✓ Use data-driven methods to detect and prevent cyberbullying and other forms of online harassment and abuse.
- ✓ Provide age-appropriate parental control tools that are easy to understand and use.
- ✓ Make data accessible for verified, qualified, and independent research.

(3) A Research Agenda that advances youth well-being through the following domain-specific priorities:

Health

- ✓ Multidisciplinary research focuses on a holistic view of youth well-being.
- ✓ Lifespan perspective with comparisons across different age groups.
- ✓ Longitudinal studies.
- ✓ Data-informed theories and conceptual models.
- ✓ Core components of technology.
- ✓ Emerging technologies.
- ✓ The impact of varying levels of exposure.

Safety

- ✓ Prevalence studies regarding youth experiencing harms online.
- ✓ Clinical research when and under what circumstances exposure to problematic content potentially results in harm and long-term impacts.
- ✓ Evaluation research on existing programs to address online safety.
- ✓ Experimental designs randomizing types of safety messages and prevention programming.
- ✓ Contextual factors that increase risk for and fortification against youth online exploitation and abuse.
- ✓ Best practices to prevent child sexual exploitation online.

Privacy

- ✓ Risk profile over course of childhood development.
- ✓ Policy and practice standards on children's online usage and health.
- ✓ Long-term and systemic risks of privacy considerations.
- ✓ Efficacy and effectiveness of privacy protections for children.
- ✓ Effects of the pandemic, including ubiquitous computer use in schools.

The report concludes with a section outlining next steps for policymakers, including:

- ✓ Enacting federal legislation to protect youth health, safety, and privacy online.
- ✓ Advancing industry action to implement age-appropriate health, safety and privacy best practices on online platforms through federal legislation and voluntary commitments.
- ✓ Working to require access to platform data for independent researchers in privacy-preserving ways.
- ✓ Providing support for research into youth health, safety, and privacy online.
- ✓ Promoting youth voices in solution settings.
- ✓ Supporting access to new and updated resources tailored for youth, parents, health providers, and educators.
- ✓ Engaging in international efforts to collaborate on online safety.

Ensuring the online health, safety and well-being of young people in the United States is a critical public health priority. Today's youth are more digitally literate than any previous generation, which creates both risks and benefits of online technology. The strategies described in this report aim to help protect the health, safety, and privacy of youth online, but it will take a whole-of-government approach in collaboration with researchers, industry, civil society, youth, and others to achieve this.

THE DEFINITION OF YOUTH

Throughout this report, various terms are used in reference to youth, including children, kids, teens, boys, girls, LGBTQI+ youth, and minors. Generally, the references match the terminology used in specific studies cited in the report. While we recognize there are multiple definitions—both developmental and legal—related to age and gender, the goal in this report is to address a broad audience while ensuring that our language is inclusive of all young people and reflective of their experiences.

THE DEFINITION OF ONLINE PLATFORMS

The term "online platforms" is used generally to describe social media and other online services that allow for interaction between different parties. The Congressional Research Service has defined "online platforms" as "any computer application or service that hosts and provides digital content and services on the Internet and facilitates access, creation, sharing and exchange of information."[22, 23] In this context, the term includes gaming applications ("apps") that allow for multiple players to interact with each other, dating websites, places (including marketplaces) for posting content that users can react to, app stores, and search engines, as well as social media and messaging applications.

Task Force Membership

The Kids Online Health and Safety Task Force is comprised of several agencies, including the Department of Health and Human Services (HHS), the Department of Commerce (DOC), the Department of Education (ED), the Department of Homeland Security (DHS), the Department of Justice (DOJ), the Executive Office of the President and a representative from the Federal Trade Commission (FTC).

TASK FORCE PRINCIPALS

CO-CHAIRS

Miriam Delphin-Rittmon
Assistant Secretary for Mental Health and Substance Use
Administrator, Substance Abuse and Mental Health Services Administration *(SAMHSA)*

Alan Davidson
Assistant Secretary of Commerce for Communications and Information
Administrator, National Telecommunications and Information Administration (NTIA)

MEMBERS

Department of Health and Human Services

Jeff Hild
Principal Deputy Assistant Secretary performing the delegable duties of the Assistant Secretary for Children and Families Administration for Children and Families (ACF)

Debra Houry
Chief Medical Officer and Deputy Director for Program and Science
Centers for Disease Control and Prevention (CDC)

VADM Vivek Murthy
U.S. Surgeon General Office of the Surgeon General (OSG)

Monica Bertagnolli
Director National Institutes of Health (NIH)

ADM Rachel Levine
Assistant Secretary for Health Office of the Assistant Secretary for Health (OASH)

Department of Commerce

Laurie Locascio
Director National Institute of Standards and Technology *and the Under Secretary of Commerce for Standards and Technology* National Institute of Standards and Technology (NIST)

Department of Education	Roberto Rodriguez *Assistant Secretary* Office of Planning, Evaluation, and Policy Development
Federal Trade Commission	Alvaro Bedoya *Commissioner*
Department of Homeland Security	Jeohn Favors *Assistant Secretary* Counterterrorism and Threat Prevention and Law Enforcement Office of Strategy, Policy, and Plans
Department of Justice	Steven J. Grocki Chief Child Exploitation and Obscenity Section
Executive Office of the President	Cailin Crockett *Senior Advisor* *Gender Policy Council* *Director* National Security Council
	Terri Tanielian *Special Assistant to the President for Veteran Affairs* Domestic Policy Council
	Jonathan Donenberg *Deputy Assistant to the President for Economic Policy* National Economic Council
	Chris Fisk *Senior Policy Advisor* Office of the Vice President
	Deirdre K. Mulligan *Principal Deputy U.S. Chief Technology Officer* Office of Science and Technology Policy (OSTP)
	Patricia Liu *Deputy Policy Director* Office of the First Lady
	Vivek Viswanathan *Senior Advisor White House* Office of Deputy Chief of Staff

Identifying Risks and Benefits to Kids' Health, Safety, and Privacy from Their Use of Online Platforms: An Overview of Task Force Findings

Given the complex and multifaceted relationship among health, safety, privacy, and online technology, the Task Force relied on stakeholder listening sessions and other information-gathering efforts, including a formal request for information to the public, reviews of existing research, and expert input in the Task Force subcommittees (described in the Appendix) to enhance understanding of the risks and benefits to young people's health, safety, and privacy. To ensure the robust development of guidance, the Task Force brought together different groups with a diversity of opinions and experiences to inform efforts.

A summary of online harms and benefits to children is outlined below, with separate focus areas based on the impact to health, safety, and privacy, although these categories often overlap. The Task Force found that developmental processes throughout childhood and adolescence, such as identity development and exploration, and relationship formation, can be both enhanced and undermined by interaction with content from online platforms. This impact depends on the characteristics of the individual youth and the specific attributes of the online platforms they use. While more research is necessary to fully understand the impact of online platforms on youth, on a review of the existing research, the Task Force identified a variety of health, safety, and privacy risks to youth related to online platform use, including problematic or excessive use, cyberbullying, bias and discrimination, child sexual exploitation, and privacy violations.

A note on the research summarized below: Given the ubiquity of digital devices, youth typically have their first interactions online before adolescence. However, the vast majority of research conducted assessing the harms and benefits of youth online focuses on adolescents. This may be due to several reasons. Many online platforms prohibit the use of their services by children under the age of 13 in their terms of service—although many children still access these platforms. These platforms typically do not allow users to indicate that they are under 13, which limits the potential data available for research involving kids under 13. For researchers looking to collect data about children interacting with online platforms, federal and some state privacy laws limit the collection and sharing of certain information about individuals under the age of 13. This may affect researchers' ability to collect data directly from children as well as different platforms' willingness to allow researchers to create mechanisms for such data collection.[24, 25]

HEALTH

The impact of the use of online platforms on young people's health has been a focus of significant research and policy deliberation in recent years. In December 2023, the National Academies of Sciences, Engineering and Medicine (NASEM) published a report of a consensus study, ***Social Media and Adolescent Health***, which offers a comprehensive scientific review of existing research.[26] The report found evidence of benefits to adolescents associated with social media usage: social connections, combatting isolation, learning opportunities, self-expression, and civic engagement. It also identified evidence of harms associated with social media usage: social comparison, displacement of other activities, interference with attention and learning, sleep disruption, overuse and problematic use, and sexual exploitation and abuse. As the report and other work has identified, these impacts are gendered: girls may disproportionally have more negative interactions and experiences online than boys do.[27, 28]

There are key limitations in research analyzing the impact of social media on young people. For example, many of the existing studies are correlational and cross-sectional. Such studies find that young people who spend a lot of time online also often have issues with sleep.[29, 30, 31] Whether youth are not sleeping because they are spending time online or are spending time online because they are not sleeping is much more difficult to conclusively establish, thus limiting our ability to evaluate the impact of time spent online or the efficacy of interventions. Studies also demonstrate a wide variation in the impact of social media on individuals, which can make it difficult to draw broad conclusions. For some youth, the impact may be significantly negative, whereas for others, it may be significantly positive.[32] Additionally, many studies lack the specificity necessary to inform specific interventions. For example, many studies use constructs like "screen time"—that is, the amount of time youth spend on their screens—which is not, in and of itself, a robust enough predictor of outcomes.[33] Given differences in research designs and measurements, a number of empirical findings appear to contradict one another, likely indicating, as the Surgeon General has stated, that "the relationship between social media and youth mental health is complex and potentially bidirectional."[34, 35]

However, despite a lack of consensus among researchers about causal links across all demographics, ages, and types of social media and online platform use, there remains significant concern that social media use in general has not been proven safe for youth.[36] The risks of harm raised by the research to date, including potentially increased levels of depression, loss of sleep, and inability to detach from their devices—along with concern expressed among parents, youth, and the general public—warranted the Surgeon General Advisory in 2023 titled ***Social Media and Youth Mental Health***, which concludes that excessive and problematic use of social media and exposure to extreme and inappropriate content can have a profound risk of harm to the mental health and well-being of youth.[37] As the Task Force was finalizing its work, the Surgeon General followed up in June 2024 with a call for warning labels on social media platforms.[38] Current evidence suggests that passive and active social media use are associated with depression, anxiety,[39, 40, 41, 42] and suicide[43, 44] among specific groups of adolescents.

The use of social media and other online platforms can influence key developmental processes that occur throughout childhood, especially during adolescence.[45, 46] These include:

- ✓ **Identity Development and Exploration.** The digital world offers a much larger environment for youth to develop and explore their identities. Many young people curate and post content that projects what they perceive to be the best reflection of themselves. These online images can be psychologically affirming. However, curated content can also have the potential to be psychologically harmful as youth strive to live up to images projected by their peers, corporate influencers, and mass media.[47, 48, 49, 50, 51]

- ✓ **Self-Disclosure.** Some youth may share personal information or secrets about themselves with their friends and peers. This can be instrumental in finding community and belonging.[52, 53] However, when disclosures occur online, they can result in negative outcomes related to exposure to multiple unrelated or unintended audiences,[54] loss of privacy, and increased feelings of vulnerability.[55]

- ✓ **Social Status and Feedback.** Attaining social status and acceptance among peers are central features of adolescent development.[56] In the online world, there are quantifiable ways of assessing status and belonging—for example, the number and identity of "likes"—heightening social comparison in ways that can lead to psychological distress.[57, 58]

- ✓ **Finding People "Like Me."** Young people—including those who feel lonely, different, stigmatized, or ostracized in the offline world—can find community online.[59] However, the public nature of online expression can stifle expression[60] and youth may be drawn into communities that ultimately propel them to commit violence against themselves or others.[61, 62]

Focus Issue: Problematic Use/Excessive Use

Even if the activities a young person is engaging in online are not harmful or distressing, the mere experience of excessive use can threaten health and well-being by disrupting healthy behaviors. According to a recent survey, half of U.S. teenagers (51%) report spending at least four hours per day using a particular set of social media apps.[63] Usage varies by age, with 42% of 13-year-olds using these social media apps for more than four hours per day and 62% of 17-year-olds reporting spending more than four hours per day on them.[64] Only 10.5% of teenagers spend one hour or less on social media, while nearly 30% spend six hours or more on social media.[65]

Excessive and problematic social media use is associated with sleep problems, attention problems, and feelings of exclusion among youth.[66, 67, 68, 69] Existing studies have found a consistent relationship among poor sleep quality, reduced sleep duration, sleep difficulties, depression, altered neurological development, and suicidal thoughts and behaviors.[70, 71, 72] On a typical weekday, nearly 1-in-3 adolescents report using screens until midnight or later.[73] Some research suggests that technology's interference with sleep is one of the key ways that social media use may contribute to mental health challenges among young people.[74]

Social media platforms are often designed to maximize user engagement, which has the potential to encourage excessive use and the inability to regulate emotional responses through features such as push notifications, autoplay, infinite scroll, and engagement-driven algorithms for content recommendations. Some experts say that autoplay settings feed into risks of harm by exploiting psychological triggers, such as the fear of missing out, to keep users engaged and scrolling. Dark patterns are user interfaces designed to steer or mislead users into making unintended and potentially harmful decisions. In the context of kids online, dark patterns can be used to nudge or manipulate youth to make it more difficult for them to log off their devices and disconnect.[75, 76, 77, 78]

SAFETY

For purposes of this report, the term "safety" encompasses protection from harms in both the online and physical worlds that youth may experience because of online engagement and interactions. Youth face a multitude of safety issues and associated harms online: they range from cyberbullying and online harassment, to encouraging self-harm, to grooming and child sexual exploitation. Much of the research on safety has focused on quantifying these harms—such as when youth of different ages encounter violence online or sextortion, and there is less material on the efficacy of different measures to keep kids safe.[79] Importantly, these risks to safety affect both youth physical and mental health.

Focus Issue: Cyberbullying and Other Forms of Online Harassment and Abuse

Cyberbullying is a major concern for youth using online platforms.[80] Nearly 16% of U.S. high school students reported being cyberbullied in 2021.[81] Another study conducted by the Pew Research Center suggests that cyberbullying is particularly common for youth. Of those surveyed, nearly half (49%) of 15–17-year-olds, and 42% of those ages 13–14, reported being threatened or harassed, or receiving explicit images that they did not request.[82] Moreover, LGBTQI+ youth, youth from racial and ethnic minority groups, and youth with disabilities are more likely to experience cyberbullying than their

peers.[83, 84, 85] According to one survey, students with disabilities, for example, are more likely than their peers without disabilities to be victims of, and engage in, cyberbullying, controlling for grade, gender, and race.[86]

Bullying among children and youth is defined as "any unwanted aggressive behavior(s) by another youth or group of youths who are not siblings or current dating partners that involves an observed or perceived power imbalance and is repeated multiple times or is highly likely to be repeated. Bullying may inflict harm or distress on the targeted youth including physical, psychological, social, or educational harm."[87] Bullying can happen relationally through social isolation and rumor spreading and can have negative health effects such as depression, anxiety, and substance abuse that last into adulthood.[88, 89] Cyberbullying has been noted as one of the most prevalent preceding risk factors for youth suicide-related behaviors.[90]

Cyberbullying can take place through digital Internet-connected devices and online spaces such as social media, online games, websites, instant messaging, chat rooms, text messages, and forums.[91] Harmful norms around masculinity and femininity can also increase the prevalence of cyberbullying, and influence its perpetration (e.g., the use of homophobic slurs against both LGBTQI+ and heterosexual youth).[92, 93, 94] Other forms of technology-facilitated abuse, such as cyberstalking, or the public sharing of private sexual images, both real and AI-generated, can take place in the context of dating violence, with different considerations and implications for youth safety.

It is important to note that violence does not occur in isolation; different forms of violence are often interconnected.[95] This means that exposure to one type of violence can increase the risk of involvement in other types of violence in the short- and long-term.[96] For instance, research suggests that witnessing violence[97] and associating with peers engaging in high-risk behaviors[98, 99] can increase the risk for cyberbullying perpetration, as can social isolation, lack of social support,[100, 101] and substance use.[102, 103, 104, 105, 106, 107]

Thus, efforts to prevent one form of violence may also prevent other forms of violence and associated negative health outcomes. For example, teen-dating violence-prevention efforts can reduce exposure to bullying,[108] and bullying prevention efforts, online and offline, can improve youth mental health.[109]

However, there is limited understanding about the effectiveness of focused bullying prevention efforts, including cyberbullying prevention strategies, outside the school environment.[110, 111, 112] Rigorous and timely evaluations of strategies to foster safe and healthy online environments for youth are needed[113] to prevent cyberbullying across different online platforms (e.g., social media, online gaming, forums, and electronic sports or esports) and populations (e.g., children, adolescents, older youth, and youth with developmental/physical disabilities or from different racial/ethnic backgrounds).

Youth report being skeptical of social media companies' willingness and ability to effectively respond to bullying online via their content moderation systems and other interventions.[114, 115, 116] They express that the process of using safety tools when they encounter toxic online behaviors is overwhelming.[117]

Finally, it is important to highlight protective factors that may mitigate harms associated with bullying and forms of youth violence. Research suggests that positive, prosocial interpersonal relationships with parents/caregivers, other adults, or peers may protect against bullying,[118, 119] other forms of youth violence,[120] and suicidality or self-harm.[121] Thus, creating protective community environments through community norms or culture change can have protective effects against different forms of violence including bullying,[122] adverse childhood experiences,[123] sexual violence,[124] and suicide or self-harm.[125]

As with the sense of community in offline contexts, virtual community has been associated with benefits to physical and mental health[126]—some of which are shared factors (e.g., connectedness) to protect against different forms of violence. Norms that support online civility and reject violence online could increase overall satisfaction with platform experience.[127]

Focus Issue: Bias and Discrimination

Online spaces are critical for young people seeking community, including those who belong to marginalized groups or otherwise face discrimination. For example, 69% of LGBTQI+ youth report finding affirming spaces online.[128] These youth reported fewer depressive symptoms than their peers and experienced other benefits of online communal spaces.[129]

Different demographic groups and marginalized communities also experience bias and discrimination online.[130, 131] In December 2023, the National Institutes of Health (NIH) held a workshop titled "Understanding and Addressing the Health Impacts of Online Abuse and Harassment" to identify gaps, opportunities, and challenges in advancing a research agenda to better understand the clinical, health, and developmental impacts of online harassment and abuse and develop innovative prevention and intervention efforts. Researchers pointed out that online spaces may be particularly unsafe for disabled Americans, women, nonbinary individuals, people of color, individuals identifying as LGBTQI+, and youth.[132, 133, 134]

Evidence suggests that social media may pose unique harms to the well-being of girls and young women.[135, 136, 137] Research shows that girls are more likely than boys to engage with social media, image, or text messaging platforms, rather than other forms of online platforms (e.g., games).[138] Girls are often exposed to harms in a way that differs from other people. A recent report notes that girls might be more likely than boys to be exposed to pornographic content that they did not request, exposed to content promoting self-harming, and experience offline harms after online attacks.[139] Girls' online experience is correlated with disproportionately negative impacts on well-being. Girls report negative experiences, such as social exclusion and cyberbullying.[140] In addition, girls are exposed to a range of gender-based discrimination and other gender-based online harm. Although girls can derive benefit from online games, research indicates that a majority of female gamers experience gender-based harassment and discrimination online.[141] Many digital spaces, such as online gaming, foster misogyny, which can intersect with anti-LGBTQI+ prejudice and racism: these include, for example, virtual depictions of sexual violence within games, sexual harassment through in-game chat features, threats of sexual violence, and targeting of female gamers both online and offline.[142, 143, 144]

In addition, adolescents of color frequently experience racism online,[145, 146] which has been linked to mental health conditions such as anxiety, depression, and PTSD symptoms.[147, 148, 149, 150] Increased rates of PTSD symptoms and depression symptoms are also linked to suicidal ideation.[151] Thus, exposure to racism online may contribute to the growing rate of suicide among Black children and teens.[152] One study found the suicide rate among Black youth ages 10–17 years to have increased 144% between 2007 and 2020, the greatest increase of any racial or ethnic group in the country.[153]

Young people from different demographic groups can also find their ability to gather and engage in online spaces compromised by biases in platform moderation policies. For example, due to broad or mistakenly applied content policies, LGBTQI+ and Black content creators have seen their content disproportionately demonetized and reduced in distribution on online platforms.[154, 155] This can affect young people's ability both to speak out online and to hear from others from diverse or shared backgrounds, ultimately increasing feelings of isolation and undermining their ability to find or form supportive communities online.

Collection, use, and sharing of young people's personal information also creates specific risks relating to bias and discrimination, which can take a variety of forms online and affect youth in different ways.[156, 157] For example, online ad exchanges use geolocation to serve ads that reach users of all ages, including youth, with specific ads based on their location.[158] As a result, youth from marginalized communities can be subject to further entrenchment of discrimination through technology ("digital red-lining").[159, 160, 161, 162]

Focus Issue: Sexual Exploitation and Abuse

Online services can expose children to an array of harms involving sexual exploitation, including sex trafficking, sextortion, and invasions of intimate privacy. Perpetrators of child sexual exploitation use a myriad of platforms, including social media, gaming systems, and private messaging and chat apps, and undertake a variety of methods in their efforts to sexually exploit children online. For example, perpetrators often engage in "grooming" behavior, in which they establish a connection with the targeted minor by offering support, attention, and friendship—thereby gaining the minor's trust and, in turn, increasing the chances that the minor will engage in sexually explicit acts with or for the offender.[163] Perpetrators may also use their online connection with minors to persuade, induce, entice, or coerce them into engaging in sexually explicit conduct, including, for example, commercial sex acts.[164] Perpetrators may be known to the victim (e.g., a family member or other adult), or strangers that they meet online.

These are not always one-off crimes involving single perpetrators and single online platforms. More sophisticated perpetrators work in concert with one another to sexually victimize minors. Some perpetrators collaborate on identifying minors to victimize, thinking through ways to victimize them, and sharing tips on how to avoid getting caught.[165] Criminal networks abroad undertake organized sextortion schemes targeting minors in the United States.[166] (Sextortion generally refers to the act of an offender threatening to distribute sexually explicit images of an individual unless the individual pays money or sends additional images to the offender or accedes to some other demand.[167]) Moreover, it is becoming increasingly common for perpetrators to make initial contact with a minor on one platform only to move their communications to a different, sometimes encrypted, platform as the discussions become more sexualized.[168]

Sextortion presents a particularly grave and increasing threat to the health and safety of minors online.[169] In 2023, the National Center for Missing and Exploited Children's (NCMEC)'s CyberTipline received more than 186,000 reports of online enticement—including sextortion—and between 2021 and 2023, the number of online enticement reports increased by more than 300%.[170, 171] It is likely that the number of reported cases, the majority of which come from providers through CyberTips, is a small fraction of the number of total incidents of sextortion.

Sextortion has devastating effects on victims. More than 20 minors, all teenage boys, in the United States have died by suicide as a direct consequence.[172, 173] More generally, victims often endure effects such as shame, embarrassment, anxiety, and depression.[174, 175] Studies on sextortion of minors have found emerging threats, including online sexual harassment and the lack of secure technical mitigations to prevent the distribution of child sexual abuse material (CSAM).[176, 177] However, there remain critical questions on how coercion occurs, how minors may become victims of exploitation or abuse, and how best to prevent sextortion.[178]

Artificial intelligence (AI) tools are becoming increasingly easy to use, and their outputs—photos, videos, and grooming language—are becoming increasingly realistic, compounding some harms of social media and online platforms. Offenders have already started using AI to generate CSAM (e.g., manipulating benign images of actual minors to "nudify" or remove clothing from children, or make it appear

that minors are engaged in sexually explicit conduct, including new fake images of existing CSAM victims, or wholly AI-generated CSAM showing a non-existent child). This problem is multi-faceted and severe. In addition to concerns that such material will normalize engagement with CSAM depicting actual minors and lead to the victimization of actual minors, deepfake imagery involving real minors can cause significant harm to the depicted minor. Moreover, the proliferation of AI-generated material of fake minors on online platforms may cause law enforcement to spend their limited time and resources investigating crimes against a minor who does not, in fact, exist.[179]

Youth sometimes consensually share intimate images with one another, which can pose nuanced legal[180] and well-being[181] issues. Like other forms of sexual violence, image-based sexual harassment and abuse, including non-consensual distribution of images, is rarely reported.[182, 183] There are also major gaps in understanding the prevalence of these harms, as well as the effectiveness of technical mitigations.

PRIVACY

Large parts of the digital ecosystem are built using a business model that collects, analyzes, uses, and shares vast amounts of information about individuals, including data about usage and behavioral patterns. This approach has enabled the development of free or low-cost services and allowed for the development of recommendations (of content and contacts) and tailored services. However, data collection infrastructure has generated a wide range of privacy concerns, including the disclosure of personal data in unexpected contexts and support for an industry of data brokers who buy and sell invasive digital dossiers about individuals.[184]

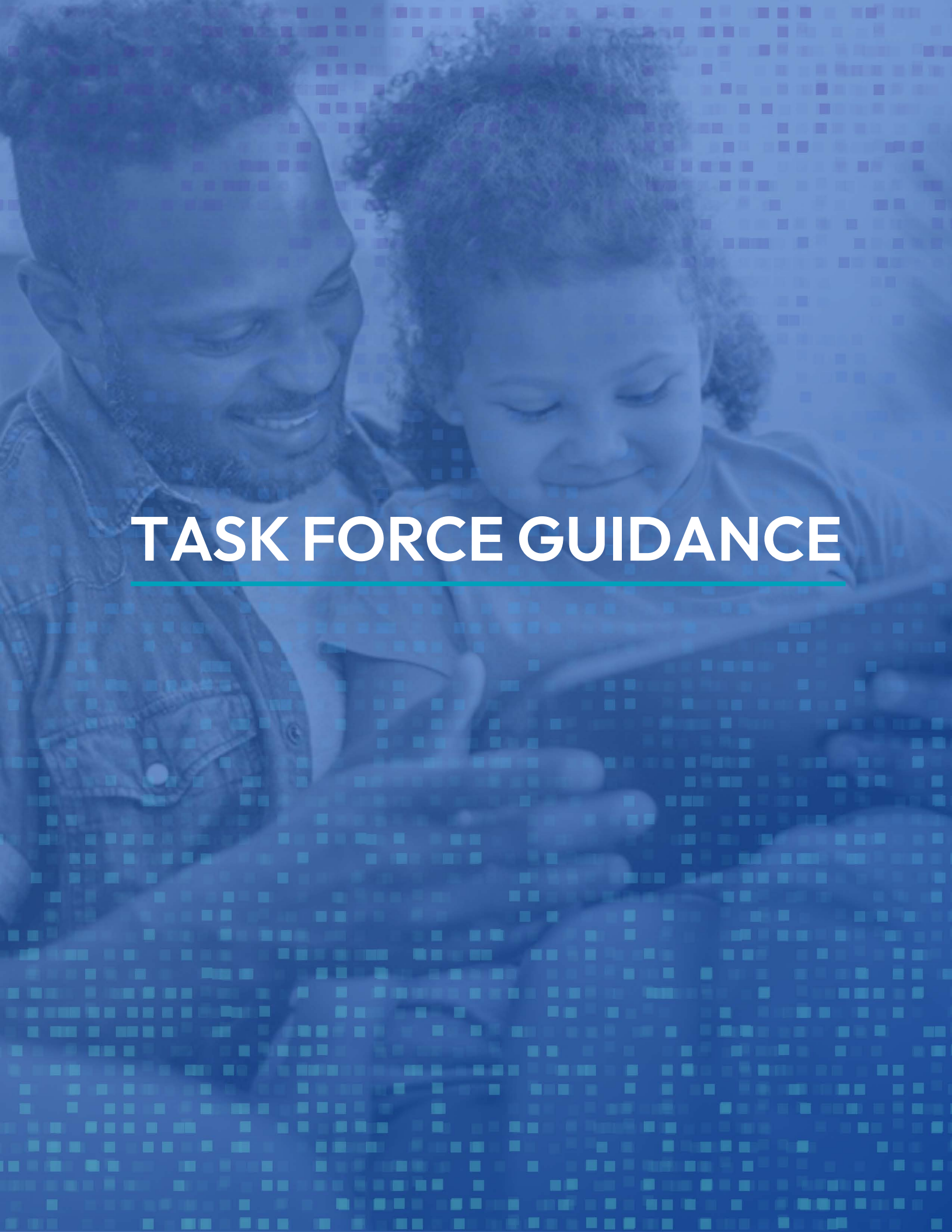
Privacy in the digital space is important for positive youth development,[185] allowing them to develop autonomy, learn critical thinking skills, and build trust. At the same time, young people are less capable and experienced in thinking through the potential impacts of sharing personal information and communications (including images) and may not be aware of the implications of the background collection of data in complex digital ecosystems.

Collectively navigating privacy can be particularly challenging for teens and their families. Older adolescents are at a developmental stage at which they are learning how to make decisions as emerging adults. However, as they become more interested in asserting their independence, some may be more likely to overshare personal information online or to be targeted by advertisers or bad actors.[186] Additionally, the pervasiveness of technology today raises significant questions about the impact of constant surveillance on adolescent development, having an "always-on" online audience, the inability to make mistakes without a permanent record, and social pressures including the fear of missing out.

The economic incentives of online platforms are often at odds with privacy protection. Small companies, including developers that are driven to collect and monetize personal information may not prioritize incorporating privacy or safety features.[187, 188, 189]

Furthermore, it may be necessary, but not sufficient, to focus on helping youth learn to make better decisions in protecting their privacy. Researchers have highlighted the apparent disconnect between the stated value that individuals place on privacy, which tends to be high, and their data sharing and use behaviors on online platforms, which often seem to contradict those values.[190] However, this disconnect may reflect more about the particular design choices of those online platforms than pertain to a contradictory response from users. What data is collected and used about users—including youths—often cannot be modified by users. However, even users who have a clear sense of their privacy preferences may not be able to enact those preferences due to design choices by the online platforms. To the extent that choices are available, it may be especially difficult for youth to exercise those choices, as

they may not be developmentally ready to understand privacy risks or effectively weigh the tradeoffs around privacy. Generally, older teens should be empowered to exercise more control and autonomy over their online experiences, supported by adequate default privacy protections.



TASK FORCE GUIDANCE

Task Force Guidance

Based on information gathered through consultations, comments, and a review of the research summarized in the previous section, the Task Force has developed:

(1) Best Practices to Support Parents and Caregivers,
(2) Recommended Practices for Industry, and
(3) A Research Agenda for studying kids' online health, safety, and privacy.

While more research is needed to fully understand the impact of social media and other online platforms on youth mental health, safety, and privacy, the Task Force has identified concrete interventions that could meaningfully improve young people's well-being.

BEST PRACTICES AND RESOURCES FOR PARENTS AND CAREGIVERS

As part of the Biden-Harris Administration's Strategy to Address the National Mental Health Crisis, SAMHSA funded the American Academy of Pediatrics (AAP) to establish the National Center of Excellence for Social Media and Youth Mental Health (Center of Excellence), which launched on February 7, 2023. The Center serves as a multifaceted platform of informational and educational resources for youth, parents, educators, and other professionals who help youth navigate social media. Parents have a critical role in supporting the social and emotional development of their children, they do not however bear the only responsibility in protecting their children from unhealthy media use or risky exposure. This requires policymakers to consider how to make online environments safer for children. A successful approach also includes multiple parties such as caregivers, pediatricians, teachers, coaches, and other trusted adults in a child's life.

To support and expand on the work of the Center, the Task Force convened a working group in the Fall of 2023 to gather best practices across the federal government that would assist parents and caregivers in protecting the health, safety, and privacy of their children who use online platforms. The Administration for Children and Families (ACF) and SAMHSA led this effort. The working group included senior staff with subject matter expertise from ACF, CDC, NIH, SAMHSA, OASH, OSG, NTIA, DOJ, ED, DHS, and NIST. The working group collaborated with the Center of Excellence to develop new materials for parents and caregivers.

OVERARCHING FRAMEWORK FOR CHILDREN AND YOUTH MEDIA USE

As part of its grant, the Center of Excellence has produced a new framework and mnemonic to help parents and pediatric providers teach and provide timely guidance to children on how to use digital media and manage their presence on online platforms. In the ways that pediatricians provide guidance and parents help ensure that kids appropriately wear seat belts when in a car or wear a helmet when riding a bike, the 5 Cs provide a framework that might be useful for child-serving professionals to use to facilitate communication and ensure that children are safe online.[191]

The 5 Cs include:

Child – Know your child and your child's temperament and the media your child is drawn to; and for what purposes your child uses online platforms. As all children are different, they experience different risks and benefits from online media.

Content – Content quality shapes whether kids have a positive or negative relationship with online media.

Calm – Children are learning strategies to help self-regulate their emotions and sleep well at night. Online media should not be a main go-to strategy for managing big feelings, distracting, or entertaining your child.

Crowding out – Too much online media usage comes at a cost. Encourage families to focus on what they'd like to build back in, such as fun activities that allow children to unplug, learn, move their bodies, get outside, and connect with loved ones.

Communication – Building digital media literacy is critical and early conversation about media usage can help facilitate that. Open-minded conversations allow parents and caregivers opportunities to intervene if they notice concerning patterns or behaviors.

Currently, on the Center of Excellence's website, families can access a user guide for parents as well as the series of five age-based two-page handouts. There are also user guides for pediatricians who can distribute the age-based handouts at Well-Check visits.

In the coming months, the Center of Excellence plans to build out the content from the 5 Cs into easily accessible tips by age range (e.g., tips on Crowding out for school-aged children) that can be shared with families on social media and on posters that can be displayed in doctor's offices, schools, and other settings as part of its 2024 Back to School media campaign.

STRATEGIES FOR PARENTS AND CAREGIVERS

The Task Force convened groups of parents and youth from across the country to discuss a structured set of topics related to online health and safety, including their own experience with navigating social media, strategies for mitigating harms on social media, and how best to access support and resources. Using the information gleaned from these conversations, as well as previous work of the Center, the following five strategies provide practical tools for parents and caregivers implement the 5 C's Framework:

1 Build a family media plan.

Families can build a media plan using a tool designed to manage expectations and create an agreement across all members of a family or household about media use. For families with younger children, parents may need to provide more guidance on the rules, and as youth cross into adolescence, the plan should be revisited so that older youth can participate collaboratively with their parents in setting expectations that are workable for all members of the household.

2 Balance time with and without devices.

Families can intentionally create screen-free times such as during an evening meal and during bedtime hours. Parents are often in the role of planning activities. Rather than just focusing on reducing screen time, help your family think about what they want to get back—such as family quality time, more sleep, time at the movies, playing with pets or time outdoors. This can include neighborhood walks, board games, or listening to music together. Starting when

children are young, families can build a shared expectation for family time that is centered on participating in an activity together.

3 Talk about social media.

Parents of youth of all ages should maintain open and non-judgmental communication about media use. Starting with younger children, parents can position themselves as individuals who can help navigate social media by problem-solving and separating real from edited content. As youth grow older, they seek more autonomy—and with the increasing influence of their peers—so staying connected with open communication is key. Working with the Center of Excellence, the Task Force developed developmentally appropriate conversation starters described more fully in the section below.

4 Set a good example.

Parents are role models for their children. How parents use social media, the time they spend on social media, and their emotional reactions to social media use creates a framework of reference for children. Be mindful of what your children see you doing and consider describing why or what you are using social media for.

5 Optimize your family's online experience.

It is important to choose platforms and content that are developmentally appropriate for your child. Identifying quality online content to engage with together is important. It is critical to set ground rules around whom children can engage with online, while also ensuring that the strongest privacy settings are enabled. Privacy-preserving age-appropriate parental controls are important tools parents can use to help support safe online experiences for children. Be aware of warning signs of problematic online use including withdrawing from activities they previously enjoyed or changes in their routine including eating patterns and sleep habits.

BUILDING HEALTHY RELATIONSHIPS AND CONVERSATION STARTERS FOR FAMILIES

In collaboration with the Center of Excellence, the Task Force developed a series of tools to help parents and caregivers engage in conversations with their children related to digital technology and media use (full text in Appendix E).

Building Healthy Relationships with Media: Essential Skills for Children 10 and Younger

Building Healthy Relationships with Media: Essential Skills for Children 10 and Younger presents practical strategies for families to build balance, critical thinking, and safety skills for toddlers through elementary school-aged children. It includes activity cards designed to be accessible and enjoyable for child- and family-serving providers and organizations to help promote dialogue between parents and caregivers and their children about online health and safety. Topic areas and activities addressed include:

- ✓ **Make it a Low-Drama Part of the Family Conversation** – Practical tips for parents and caregivers who often find discussion with children about screen time to be fraught with struggle.
- ✓ **Normalize Having Boundaries** – Ways to prevent technology from crowding out healthy behaviors such as sleep and quality time with family, by providing developmentally appropriate language to help limit device and online platform use.
- ✓ **Pick Good Content** – Ensuring children are engaging with age-appropriate content with appropriate parental monitoring of media use, given the plethora of content available online.
- ✓ **Teach Non-Screen Ways to Manage Emotions and Boredom** – Devices are often used to manage stress or boredom, and finding appropriate alternatives is important to help limit online media use.
- ✓ **Build Digital Smarts and Kindness** – When children see something upsetting online, empowering them to pause, think about it, block it, and report it. Kids should know that kindness and respect should be the expectation online, and rudeness or violence should not.
- ✓ **Teach Safety Skills** – When kids are young, we talk to them about street safety, swimming safety, and other rules that come with exploring the world. This tool describes safety rules for the digital world.
- ✓ **"Sharenting": Thinking Before You Share** – Tools for parents to appropriately share content on social media that includes their children (e.g., pictures). Discussing this with children teaches them about consent and privacy, which may help them be a more responsible social media user as a teen and into adulthood.

Conversation Starters for Families of Tweens and Teens

Conversation Starters for Families of Tweens and Teens is intended for parents and caregivers of tweens and adolescents (ages 10–18). It includes conversation starters and follow-up prompts for a variety of scenarios that parents and caregivers may have with their child about cell phones, screens, social media, and other online platforms. Similar to the handout for younger children, these conversation starters and prompts were designed to be easily accessible for parents and caregivers. Topic areas that the conversation starters address include sample conversation starters with follow-up prompts:

- ✓ **Setting initial boundaries around technology and digital media use** – "I'd like us to talk about our family's approach for setting some boundaries around technology and media use. I was thinking that this is something we could work on together as I'd like to include your input in these decisions."
- ✓ **Initial check-ins after setting guidelines and boundaries** – "It's been about a month since we set our guidelines around technology and digital media. I wanted to check in on how things are going."
- ✓ **Social media-specific check-ins** – "I know that social media is important to you. I wanted to check in about it; how do you think things are going with your social media use?"
- ✓ **Checking in on unwanted contact** – "One aspect of social media use that is really important is protecting our privacy. Have you looked at the privacy settings on all your accounts? How are things going with those settings?"
- ✓ **Checking in on unwanted content** – "As you probably know, your social media platforms track your search and viewing patterns. They try to get to know you, and an algorithm (a set of rules that rank content across the platform) decides what to put in your feed. How is the algorithm working for you at this point? Is there content you don't want to see? Can we look at ways to reset your algorithm?"
- ✓ **Struggles with meeting family expectations around digital media use** – "I feel like it's a good time for us to check in on how our family media expectations are going. How are we all doing with using our devices? I've noticed a few times that I've needed to remind you about our agreement to not have devices at the dinner table so we can spend time together (or other area that is a struggle). What ideas do you have to make that rule work better for you? What would work about that plan and what wouldn't?"
- ✓ **Tween/teen gaming too much** – "Let's talk about gaming. I'd like to share a few things I've noticed about your gaming behaviors, and then hear from you. My goal is for us to get on the same page about this."
- ✓ **Media and technology interfering with sleep** – "Sleep is really important for everyone. I know you aren't able to [show up to an activity, have the energy to do all the things you want to do, etc.] when you don't get enough sleep. Let's talk about some ideas for how to help you get better sleep."

- ✓ **Overheard conversation about social media** – "When I was driving you and your friends today, I heard you talk about something you saw on social media last week. I'm interested in what's going on for you, so I'd like to hear a little more from you about what happened."
- ✓ **Prompts to encourage reflection around relationships with media** – "What does it feel like when you've lost track of time in your phone, versus [other favorite activities like a book, doing artwork, playing basketball, etc.]?"
- ✓ **Reflecting on other peoples' tech use** – "When you're hanging out with friends, and they are all on their phones and not paying attention to each other, how does that feel?"
- ✓ **Parents talking about their own media use** – "I sometimes have a hard time not checking my phone or feeling the need to respond to texts or emails. I'm working on how to be better about my own boundaries. Let's help each other find a good balance."

The conversation starters and scenarios were developed based on recurring themes identified from: (1) the Center of Excellence "Questions and Answer" portal, (2) presentations and convenings of parents, and (3) pediatric clinical experience. The educational messaging and activities take into account the developmental stage of the child and are framed to alleviate feelings of guilt or shame parents often report around their children's use of screens. The activities and prompts also draw from literature reviews on social media and youth mental health and motivational interviewing techniques. For example, these resources encourage parents and caregivers to have open and collaborative communication about their child's online use and family expectations because children are more likely to follow rules when they have the opportunity to provide input and discuss their concerns about online safety. And close relationships between parents and their children are associated with fewer online risk-taking behaviors in children.

COMPENDIUM OF BEST PRACTICES RESOURCES FOR PARENTS AND CAREGIVERS

Finally, in addition to the learnings from the conversations with parents, youth and other stakeholders, the Task Force collected an extensive array of federal and non-federal best-practice resources to promote the online health and safety of children and adolescents.

This compilation resulted in the identification of over 30 resources covering various age ranges of children and youth, target audiences, and categories. These resources have been organized into an annotated compendium into the following six categories:

1. **General Information about Youth and Social Media Platforms**
2. **Tools to Support Parents**
3. **Digital Citizenship**
4. **Bullying and Cyberbullying**
5. **Child Sexual Exploitation and Abuse**
6. **Teen Dating Violence and Other Forms of Gender-Based Violence**

The Center of Excellence team evaluated each of the resources using a standardized approach to determine whether the resource meets the criteria for recommendation and to help determine relevant

placement and integration into Center products. This vetting process reviews various features of each resource. Emphasis is placed on determining whether the resource employs an evidence-based, strength-focused, and child-centric methodology that is also pragmatic.

These and other materials developed by the Center of Excellence are housed and managed on the Center of Excellence on Social Media and Youth Mental Health American Academy of Pediatrics website.

Industry's Role in Promoting Kids' Online Health, Safety, and Privacy: Recommended Practices for Industry

There are many practices that developers of online platforms can implement to help protect youth online and enable them to thrive. The structures and functions of online platforms are the result of specific design choices, including, in many cases, choices to collect and use data about people for commercial purposes, maximize how much time people spend online, and target users with commercial and non-commercial content. These trends are concerning for all users but pose a distinct threat to youth.

Below are 10 important recommended practices that online service providers should take to develop platforms with youth well-being in mind.

1. **Design age-appropriate experiences for youth users**
2. **Make privacy protections for youth the default.**
3. **Reduce and remove features that encourage excessive or problematic use by youth.**
4. **Limit "likes" and social comparison features for youth by default.**
5. **Develop and deploy mechanisms and strategies to counter child sexual exploitation and abuse.**
6. **Disclose accurate and comprehensive safety-related information about apps.**
7. **Improve systems to identify and address bias and discrimination that youth experience online.**
8. **Use data-driven methods to detect and prevent cyberbullying and other forms of online harassment and abuse.**
9. **Provide age-appropriate parental control tools that are easy to understand and use.**
10. **Make data accessible for verified, qualified, and independent research.**

Each section below provides a brief discussion of specific challenges to youth well-being as well as interventions (i.e., tools, techniques, features, and settings) that providers and developers can employ to mitigate health, safety, and privacy risks to youth while maximizing their beneficial use of online services. Many of these best practices and tools use the language of "minimization," drawn from the data-protection concept of "data minimization," or collecting and using no more data than is necessary to perform a specific function. Of note, certain online services already implement—or have started to offer—some or many of the tools mentioned below for users outside of the United States (e.g., in the United Kingdom and Australia), and implement some protections as defaults (e.g., privacy protections in California). For example, some companies started preventing unknown adults from messaging children and have removed video autoplay and nighttime notifications for youth accounts.[192] Companies and services providing these protections to young people living elsewhere should offer those options to parents, caregivers, and youth across the United States.

1 DESIGN AGE-APPROPRIATE EXPERIENCES FOR YOUTH USERS

There is a huge diversity in the online platforms and services that young people use, and there is no one-size-fits-all approach to making platforms safer for kids. Thus, it is pivotal that platform operators design their services with kids' health, safety, and privacy in mind. A platform operator should employ well-known design methodologies of human-centered design (HCD)[193] and value-sensitive design (VSD)[194] and consider the unique aspects of its technology (hardware and software), its users (including youth), and other relevant stakeholders (e.g., parents, caregivers, and educators) when developing its service and incorporating any interventions.

Cognitive factors (e.g., attention, information processing, reasoning, and decision-making) are particularly relevant for platforms to promote youth health, safety, and privacy. Research indicates that youth undergo key developmental milestones that help them acquire certain competencies, more developed comprehension, and agency.[195, 196, 197] For example, health experts recognize that a pivotal part of adolescent development is the need to exercise some autonomy.[198] It can be challenging for young people to exercise autonomy in a digital ecosystem designed to influence their behavior. Likewise, technology may shape how some young people achieve key competencies and develop a sense of agency.[199, 200, 201, 202]

Crucially, HCD principles should be coupled with values-based approaches to design, such as design processes that are rooted in a desire to promote the health, safety, and privacy of youth. Technology developers and providers should use such values-sensitive approaches to design products and services that prevent and mitigate harm while providing youth with the ability to make age-appropriate choices about the material and features to which they are exposed.

RECOMMENDED PRACTICES

Creating age-appropriate experiences requires youth input, research, and continuous performance evaluation. Recommended practices include:

- ✓ Identify the types of youth who will be using the technology, including potential and unintended (e.g., prohibited) users. Consider the varied experiences of youth users across different

demographics, developmental stages, needs, anticipated uses, home environment, and experience level.

- ✓ Take youth's different contexts into account. Identify features that may be beneficial or neutral in some contexts but harmful in others in product design and risk mitigation efforts (e.g., features designed to encourage daily use in an education app versus a gambling app).[203]
- ✓ Use methodologies for human-centered design and value-sensitive design to identify product features that support well-being.
- ✓ Design based on research and performance assessments (e.g., user experience testing) focused on youth's experiences.
- ✓ Engage youth, parents and caregivers, relevant stakeholders, and experts from the field throughout the entire product development lifecycle—including young people from different backgrounds and age groups.
- ✓ Develop research and evaluation partnerships that include youth (e.g., efforts with independent research groups, academia, and government).
- ✓ Continuously evaluate harm-prevention efforts to ensure their effectiveness across time, platform, and contextual changes.

AGE ASSURANCE AND AGE VERIFICATION

There are two main routes for protecting youth health and safety on general-audience platforms:[204] (1) designing services to prioritize the health, safety, and privacy of all users in the same way, regardless of age; and (2) designing different experiences for the participant age groups (e.g., adults, all minors, or minors under 13). Designing for all users can be ideal for services that seek to minimize overall data collection about users or that generally pose low health and safety risks to users. Many users of all ages seek out privacy-protective services due to concerns about corporate, government, and interpersonal surveillance of their online activity. Designing and implementing different experiences for adults and minors requires the service provider to know or estimate the ages of all its users.

Core techniques to ascertain the age of an individual through online "age assurance" mechanisms include asking users to provide their age (self-certification or "age gating"), age estimation, inference based on usage or other data, and age verification relying upon existing credentials.[205] Some methods being used and explored include photo identification matching, facial age estimation, mobile operator network age verification (parents purchasing phones set for an age), and credentials for digital wallets and credit cards. Companies may use multiple methods to determine the predicted age of a user depending on the risks.[206, 207, 208, 209]

Many age assurance techniques raise concerns regarding accuracy[210] (e.g., falsifying age or birthdate[211]), privacy (e.g., from documentation, biometric data,[212] or data from other sources[213]), and equity.[214, 215, 216, 217, 218, 219, 220] For example, many online services in the United States have historically asked users to self-certify by providing their age or date of birth. This information is then employed as an "age gate" allowing users who say that they are above a certain age access to the service. Age-gating based on self-certification has been criticized as an age assurance method due to the ease of circumventing it. It is easy for young people to offer a false age or birthdate that enables them to access the service. Moreover, research has found that relying on self-certification alone is not an accurate method for ascertaining age.[221]

Each mechanism discussed above comes with trade-offs—from the burden of complying in an often otherwise frictionless ecosystem, to potentially deterring users of the service to invasion of privacy. Additional efforts are underway to improve techniques, technologies, and approaches, including an ongoing initiative with the International Organization for Standards[222] and industry-led proposals.[223] However, there is much work to be done on this fundamental issue. Efforts to ascertain the age of an individual online through "age assurance" mechanisms[224] have not been standard in approach or technology.[225, 226] Globally, regulators offering guidance on age assurance have noted the lack of robust evidence on efficacy and risks of various age assurance mechanisms.[227] Effective methods of age assurance ideally could help prevent children from accessing potentially harmful online material (e.g., pornography) and could be applicable in other digital technology settings such as social media platforms.

2 MAKE PRIVACY PROTECTIONS FOR YOUTH THE DEFAULT

Gathering, using, and sharing data (including images) can pose risks to anyone, and these risks can be amplified in their potential to negatively affect youth. Certain commercial practices can potentially impact youth users by profiling or targeting them with malicious activity. For example, the risks include safety concerns from disclosures of information (whether intentional sharing or data breaches), as well as risks from third-party access to interactions with youth (whether companies or individuals). The Children's Online Privacy Protection Act (COPPA),[228] Family Educational Rights and Privacy Act (FERPA),[229] and laws from states such as California,[230] provide certain privacy protections for children. Certain platforms and services also operate under business models that do not rely upon the collection of personal data. However, existing laws and industry practices are insufficient to address all harms and ensure platforms support children's well-being. In response, the Biden-Harris Administration has called upon Congress to enact better privacy protections.[231, 232] But industry should not wait to implement stronger protections for children. Developers of online platforms and services can provide enhanced privacy protections for minors in a variety of ways.

RECOMMENDED PRACTICES

- ✓ Strictly limit the collection of minors' data and personal information.
  - Do not condition a minor's use of the platform on collection of personal information or disclosure of personal information to third parties.
  - Collect only the personal information that is reasonably necessary for a minor to participate in the specific offerings of the service (e.g., game, prize, or activity), as is already required in certain circumstances by federal law under COPPA.[233, 234]
  - Retain and use personal information of minors only as long as necessary to fulfill the purpose for which it was collected, as is already required in certain circumstances by federal law under COPPA.[235]
  - Establish, and make public, a written data retention policy for minors' personal information that minimizes the retention period.[236] COPPA requirements on data retention and deletion can be a good model even for services outside its scope.
  - Minimize or disable platform and service collection of geolocation and biometric information.
  - Enable data portability and interoperability tools that allow young users to easily switch to platforms that best fit their needs. Such tools should support the user's ability to maintain their social graph.
- ✓ Make minors' accounts private by default.
  - Automatically implement the strongest available privacy settings.[237, 238]
  - Turn off direct messaging for minors by default but allow teens to opt into this feature.

- Make accounts and personal data easy to delete.[239, 240, 241]
- Avoid recommending connections between minors' accounts and other users' accounts.[242, 243, 244]
- Allow other users to connect with minors only after obtaining consent or specific information from the minor's account.
- Prevent sharing of minors' data by default.
- Disable sharing of minors' precise geolocation or biometric data, except when necessary (e.g., with a caregiver). Alternatively, turn off sharing of minors' location data by default, and permit sharing only with consent.
- Ensure that the visibility of children's posts is limited by default—that is, content that children post should only be shared with and visible to contacts and friends, unless the child who posted affirmatively chooses otherwise.

✓ Do not enable targeted advertisements or personalized algorithmic recommendations of content by default for minors.

- Do not enable targeted advertising to minors based on their activities, whether on or off the platform.[245, 246, 247]
- Ensure any remaining non-targeted advertising that appears alongside content intended for a young audience is also age appropriate.
- Do not enable by default content recommendation algorithms that are based on personalized profiling of a minor.

3 REDUCE AND REMOVE FEATURES THAT ENCOURAGE EXCESSIVE OR PROBLEMATIC USE BY YOUTH

Any digital technology commonly accessed by minors should incorporate intentional design features that promote health and well-being and limit features that maximize time, attention, and engagement.[248] Industry can provide minors and their parents or caregivers with tools to choose features based upon their needs and opt out of those that provide no benefit or pose risks. Software designers and product developers can take measures to help ensure that their products reduce risk of harm, benefit adolescents and support youth development and well-being.

RECOMMENDED PRACTICES

✓ Avoid unnecessary notifications and engagement-driven nudges.

- During the design process, consider the necessity of notifications and the disruption they cause for youth's sleep and attention.[249, 250]
- Mute notifications during certain times of the day (e.g., school and sleep hours), or

avoid them altogether, except for key safety and medical notifications or communication channels.[251, 252]

- ✓ Avoid the use of infinite scroll and autoplay features that load content continuously as a user scrolls.
  - Consider populating feeds chronologically by default, or other measures to replace infinite scroll, which places an emphasis on prolonged engagement.[253]
  - Provide minors with controls that allow them to adjust what is presented to them in their feeds and to use timers to limit total daily usage.
  - Disable any features that automatically continue to play content (e.g., videos) by default.[254]
  - Deploy default settings that include auto-shutoff and do-not-disturb features or minimize blue light at certain times of day and night.[255]
- ✓ Provide teens and parents or caregivers of younger children the ability to change minors' default settings to more protective settings.[256, 257]
- ✓ Minimize addictive features of mobile games and other services.
  - Minimize the use of random action-based rewards (e.g., loot boxes),[258] especially those that require a form of payment.
  - Minimize the use of limited time offers and other incentives and disincentives that lure people into playing for longer due to fear of missing out, loss of a reward, or other impacts to a minor's gameplay.
- ✓ Minimize ephemeral content and contingent rewards.
  - Set longer time limits for stories or ephemeral content, to reduce the sense of urgency that keeps users unnecessarily engaged for fear of missing out. Alternatively, make them available until a user accesses them within a longer set time period. For example, rather than setting a cap of 24 hours, change to 48 hours or until someone views them, with a specific cap such as 48 or 72 hours.
  - Eliminate rewards (e.g., interaction streaks) that require minors to keep coming back to the app or staying on the app to reach a special status or to get some type of reward.
- ✓ Stop use of dark patterns aimed at increasing minors' time online.
  - Remove specific design features that make it hard for minors to exercise options to get out of a content stream or back to the home screen without viewing more content (e.g., hiding the "X" button or making it hard to go back to the prior screen).

4 LIMIT "LIKES" AND SOCIAL COMPARISON FEATURES FOR YOUTH BY DEFAULT

Interaction mechanisms and features can over-engage minors in areas that are known to be unhealthy,

such as social comparison features.[259] As with other features, in different contexts these can have either beneficial or negative effects on kids.[260] Networking and reaction features that encourage increasing the number of contacts a minor has on a social network and that convey quickly that something has been viewed and liked can have a negative effect if used by youth to gauge the popularity of themselves and their posts.[261] These features can also encourage young people to expand their connections to strangers and nonfriends, potentially increasing their risk of negative or dangerous interactions.[262, 263]

RECOMMENDED PRACTICES

- ✓ Minimize quantifying "likes" and social comparison features.
  - Hide by default the visibility of the number of connections, friends, or followers for a minor's account or piece of content.[264]
  - Cap or remove by default—as appropriate for age—likes and related emojis, views, dislikes, or other interactions for a minor's posts and others' posts that the minor views.[265]
  - Minors should be able to easily disable comments on their own posts. Settings should be defaulted to only allow friends and contacts to comment on children's posts.

5 DEVELOP AND DEPLOY MECHANISMS AND STRATEGIES TO COUNTER CHILD SEXUAL EXPLOITATION AND ABUSE

Online sexual exploitation and abuse can occur on a myriad of platforms, including social media, gaming systems, and chat apps, and young people may be targeted both by adult strangers or someone they know and trust. This exploitation often takes advantage of common features of online platforms, including direct messaging, the ability to share photos, and the ability to identify and connect with groups and networks of other users. Designers of online platforms should evaluate their services through the lens of potential abuse by users who plan to engage in child sexual exploitation and abuse (CSEA); this will help identify risks present in the design and operation of their service and implement safety-by-design safeguards against CSEA. Designers of online platforms should also evaluate their services from the perspective of young people who may be targeted for exploitation and abuse in order to ensure the availability of resources and interventions that can interrupt pathways to abuse.

RECOMMENDED PRACTICES

- ✓ Join the National Center for Missing and Exploited Children's (NCMEC) "Take it Down" initiative that helps children anonymously seek the removal of sexually explicit material of themselves from online platforms.[266]
- ✓ Develop and enforce policies making clear that child sexual exploitation and abuse in any form, including AI-generated images of children, is prohibited.
  - Provide detailed and timely reports to the NCMEC's CyberTipline.[267]

- Implement measures to detect and respond to grooming language.
- Explore ways to identify and disrupt problematic interactions between adults and minors, or between minors, online.
- Incorporate pop-up messages or other "friction points" to warn children that they might be encountering or becoming involved in a dangerous situation, or to warn would-be offenders that they are about to engage in illegal conduct.
- Respond promptly to user-submitted reports of online child sexual exploitation and abuse.

✓ Incorporate other technical measures to reduce child sexual exploitation and abuse.

- Incorporate screenshot and screen-recording prevention features using existing operating system-provided tools.
- Automatically remove hidden data from shared content.
- Do not automatically download or display shared content.
- Build user interface measures that create hurdles (i.e., friction) to limit the easy sharing and re-sharing of sensitive content.
- De-index child sexual abuse material (CSAM), and remove links to websites and services that are known to carry CSAM.
- Display warnings before sensitive content is shared using on-device and privacy-preserving detection methods.
- Provide prompt and thorough responses to legal process from law enforcement.[268]

✓ Share information with other online platforms about users who have engaged in child sexual exploitation, in a privacy-protective manner—including through privacy-enhancing technologies—to ensure information is only shared as necessary to identify those specific potential threats to youth safety.[269]

✓ Develop and implement mechanisms to detect and disrupt sextortion schemes.

✓ Invest in education and prevention efforts to help children learn ways to stay safe online and parents and caregivers identify risks or indicators of online sexual exploitation, such as DHS' Know2Protect campaign.[270]

✓ Implement best-practice mitigation measures throughout the AI lifecycle (such as red-teaming[271] and ensuring that models are not trained on CSAM) to minimize the ability for AI tools to be used to generate child sexual exploitation and abuse.

✓ Develop and use mechanisms to monitor and stop live-streaming videos showing child sexual exploitation and abuse, while safeguarding privacy.[272]

6 DISCLOSE ACCURATE AND COMPREHENSIVE SAFETY-RELATED INFORMATION ABOUT APPS

Millions of apps are available for download on app stores,[273] typically accompanied by a rating and other information including features, reviews, pictures, and privacy information. Descriptions in app stores could provide valuable information to parents and children about potential safety, and risks that a particular app may pose to a child. But safety-related information is often lacking in meaningful detail, if it is there at all, and may therefore be misleading. For example, it would be useful for caregivers and youth to know if an app allows for users to be contacted by strangers. Although apps are typically assigned age-ratings (*e.g.*, 4+, 12+, etc.), those ratings do not always align with parents' needs or expectations and often do not correspond with stages of children's social and emotional development. These ratings could provide a false sense of assurance or safety (including the privacy of information about the user). App developers and app stores should focus on improving the accuracy and consistency of app rating and labeling and work with experts in child social and emotional development to determine thresholds for appropriate age ratings.

RECOMMENDED PRACTICES

- ✓ Provide detailed safety information in descriptions of apps in app stores, including, for example:
  - Informing parents of the possibility of communication between adults and children on the app.
  - Developing and informing parents about age verification tools built into the app or available at the device level.
  - Maximizing protections on devices belonging to minors and making use of operating system provider functionality linking minors to family accounts with adjustable permissions.[274]
  - Informing users whether communication on the app between users is monitored.

7 IMPROVE SYSTEMS TO IDENTIFY AND ADDRESS BIAS AND DISCRIMINATION THAT YOUTH EXPERIENCE ONLINE

Young people may experience bias and discrimination online both in their interactions with other users and in the ways in which their data is collected and used by online platforms. Young people who belong to racial, ethnic, religious, gender identity, gender expression, sexual orientation, disability status, or other marginalized identities may be exposed to hateful and harassing comments from other users that target them based on those identities. They also experience abusive conduct, such as "Internet banging," swatting, stalking, trolling, or "griefing."[275, 276] Developers of online platforms should understand the particular risks of discriminatory interactions faced by young users based on their different demographic backgrounds and develop mitigation and intervention measures. Platform developers should also evaluate their own data collection and use practices for bias to minimize the risk of biased and discriminatory treatment of youth users.

RECOMMENDED PRACTICES

- ✓ Deploy and improve the use of manual and automated moderation of discriminatory content and activity.
  - Train moderators in the different ways in which discrimination is experienced by young people online, including the use of reclaimed words in non-pejorative contexts, and the use of words in languages other than English that convey hate based on cultural context.[277]
  - Evaluate the operation and impact of automated content moderation tools, specifically for bias and discrimination, including across multiple languages.[278]
  - Prioritize moderation systems for features that pose the highest risks of discriminatory conduct against young people (e.g., voice chat in gaming).[279]
  - Establish and meaningfully uphold anti-discrimination community standards and codes of conduct and enforce platform terms of service that prohibit users from engaging in threatening or abusive behaviors towards marginalized communities.
- ✓ Evaluate the outputs of automated content-generation systems such as autocomplete and generative AI tools for bias.

8 USE DATA-DRIVEN METHODS TO DETECT AND PREVENT CYBER-BULLYING AND OTHER FORMS OF ONLINE HARASSMENT AND ABUSE

Various data-driven methods and models are used across online spaces and platforms to detect cyberbullying.[280] While different methods and models are best suited for different types of content and platforms,[281] challenges persist in the consistent identification of cyberbullying across social media spaces.[282]

Some youth experience bullying more than others. In fact, stigma plays a role in groups expressly targeted for bullying (e.g., LGBTQI+ individuals, persons with disabilities, and persons who are overweight/obese) and the type of bullying they faced.[283] Among U.S. high school students surveyed in a 2021 report, online bullying victimization is higher among females, White and American Indian and Alaska Native (AI/AN) youth, and youth who identify as a sexual minority.[284] Additionally, according to ED's Office of Civil Rights, students with disabilities in public schools reported being harassed or bullied at rates higher than their representation in the total school enrollment.[285, 286, 287] The accuracy of cyberbullying detection models can be affected by cultural differences.[288] Inclusion in the training of machine learning classifiers of additional contextual information from users' posts on a service (such as a given user's history of posting comments with greater than average amounts of profanity, or higher usage of pronouns indicating more messages directed at other users) could help improve the accuracy of online bullying detection.[289]

It is important that safety efforts take into account that sextortion and the non-consensual sharing or threatening to disseminate sexual images are also perpetrated by peers, including by current or former

dating partners.[290] This form of abuse is highly gendered, with girls the majority of victims targeted predominantly by boys. Other forms of technology-facilitated abuse, such as cyberstalking, can take place in the context of dating violence, with different considerations and implications for youth safety.

RECOMMENDED PRACTICES

- ✓ Implement designs that help prevent, minimize, and mitigate bullying and other forms of online harassment and abuse, including, for example:
  - Evaluate technical interventions aimed at minimizing online bullying, such as reporting and bystander support tools,[291, 292, 293] for their effects on both youth who are being bullied and those who are bullying others.
  - Use diverse, tailored approaches to help protect users from being bullied, prevent users from bullying others, and empower bystanders to stand up to bullying (e.g., by providing tools that allow users to reach out to trusted friends when they are experiencing bullying).[294]
- ✓ Share evidence-based bullying prevention resources with parents/caregivers and youth—e.g., on cyberbullying tactics;[295] preventing cyberbullying;[296] social media, apps, and sites commonly used by children and teens;[297] and cyberbullying and online gaming.[298] (For a comprehensive list of resources, visit StopBullying.gov.)
- ✓ Direct young people expressing self-harm or suicide-related behaviors to the 988 Suicide and Crisis Lifeline.[299]
- ✓ Promote access to youth-specific resources for image-based sexual abuse and dating violence, such as Love is Respect and NCMEC's Take it Down.[300]
- ✓ Allow muting/blocking of problematic users, even if the behavior does not rise to the level of violating platform policies.
- ✓ To reduce the risk of image-based sexual abuse among peers, employ image-blurring technology so that users only view images they consent to receive.
- ✓ Develop a classification framework for incorporating cultural differences to identify indicators of online bullying victimization.[301]
- ✓ Ensure equitable access to online safety resources and mechanisms for diverse user audiences (e.g., consider literacy levels, accessibility across different devices, and languages).
- ✓ Identify specific groups that have experienced more bullying to develop tailored interventions to address cyberbullying.[302, 303]
- ✓ Embed online civility norms across online spaces (e.g., onboarding, policies, design, monitoring, and resources).[304]
- ✓ Deploy and improve the use of manual and automated moderation of bullying content and activity.

9 PROVIDE AGE-APPROPRIATE PARENTAL CONTROL TOOLS THAT ARE EASY TO UNDERSTAND AND USE

Some parents and guardians would like to exercise more control over their children's online experiences.[305] Well-designed parental control tools can help accomplish this, while also preserving the benefits of Internet use for youth.[306] While parental controls are not a panacea for kids' online safety, industry can do more to create parental controls that work for parents and kids. The relationship between different layers of available parental controls (e.g., on a device versus within an app or on a website) is often not clear to parents, and controls are not equivalent on different platforms and services.[307] It is also important to note that some forms of parental controls may be invasive to young people's privacy and harmful to already vulnerable youth; platform designers should consider carefully what kinds of controls, for what age group, are appropriate for parent accounts and which should be controlled by the user directly.[308] A one-size-fits-all approach to parental controls may not be appropriate for many families.[309, 310, 311] More research is necessary to understand when, where, and which parental controls are most effective, but some steps can help parents and guardians today.

RECOMMENDED PRACTICES

- ✓ Adopt age-appropriate parental control solutions and promote their availability, which may differ by age-group and could include:
  - Supervised accounts with appropriate limitations for certain age groups.[312]
  - Limits on interactive functions such as chat.[313, 314]
  - Limiting and blocking contacts.[315, 316]
  - Limits on monetary spending.[317]
  - Time limits or scheduled breaks.[318]
  - Labels for manipulated content.[319]
  - Easy account deletion.[320]
  - Limit practices that encourage youth to circumvent parental control features.[321]
  - Limits for children to receive in-app financial transactions from adults.
- ✓ Make parental control tools easy to understand and use.
  - Make disclosures that adequately inform parents and caregivers about platforms and services[322, 323] so they understand the risks when they allow their children access to content.[324]
  - Help parents understand the content and features they are enabling children to access if they help children to circumvent age restrictions.
  - Consider developing "parental onboarding" resources to help parents and caregivers understand the available features and control tools.

- Make it easy for parents to change/configure monitoring and controls as their children age.

10 MAKE DATA ACCESSIBLE FOR VERIFIED, QUALIFIED, AND INDEPENDENT RESEARCH

A growing body of research has examined the relationship between children and online platforms with data that is available. However, researchers would significantly benefit from access to detailed platform data, which would expand and enable new areas of critical research and address the gaps in our understanding.[325] Barriers exist, for example, for academic data science research in the new realm of behavior modification by digital platforms.[326, 327] Platforms can provide tiered access to detailed online platform data under a framework that considers users' expectations of privacy.[328] Such access must be available in user-friendly formats without significant cost. Data access should protect users' privacy and respond to researchers' changing needs through context-specific consideration of the risks that different research efforts may pose. Platforms should be transparent about how users' data may be shared with researchers and aim to use privacy-enhancing technologies when possible and for the most sensitive data.

Online platform data is inherently networked and global. Youth can follow and comment on accounts from around the world and high-quality data sets will often require information on data subjects from other countries. We must collaborate with partners to respect privacy, data protection, and ethics laws that may vary. Specifically, the United States and the European Union have a shared commitment to advance data access for researchers—and this commitment has led to shared principles and transatlantic stakeholder discussions as part of the EU-U.S. Trade and Technology Council (TTC).[329] Since the launch of the TTC, the EU Digital Services Act (DSA) has gone into effect, requiring providers of Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) to provide increased transparency into the operation of their services. The DSA includes specific mandates for VLOPs/VLOSEs to share data with academic and civil society researchers in a way that is consistent with privacy protections and research ethics. The new law has encouraged platforms to launch new programs and create infrastructures that have the potential to benefit researchers globally. During the 6th Ministerial Meeting of the TTC in April 2024, Working Group 5 released a ***Status Report: Mechanisms for Researcher Access to Online Platform Data***.[330] As policymakers aim to understand the impact of the online information environment on youth development, it will be important to follow Europe's progress and offer guidance to platforms to extend access to the U.S. research community.

RECOMMENDED PRACTICES

✓ Platforms should make the following types of data available to vetted researchers, subject to privacy protections:

- Usage data, such as the number of minor users and their time spent online, including how certain features and designs increase or decrease time spent.
- Aggregate information about individuals' social network connections.
- Interaction with specific content and features of concern.

- Privacy and account settings chosen by users.
- Moderation-related data, such as user reporting, moderator decisions by type, and rate of takedowns.
- Targeted advertising that may reach children, including what data is used for ad targeting and what steps are taken to keep ads from being targeted to minors.
- Use of algorithmic and process-based recommendation systems, including actual personalized recommender systems where appropriate and the data used in the systems.

✓ Platforms should also support features that allow for data donation through comprehensive, machine-readable downloads and secure software designed for data collection through a smartphone app or browser.

Research Agenda

INTRODUCTION

The current generation of youth has grown up in an era with widespread use of digital technology. With nine in 10 youth under the age of 18 reporting use of a social media platform, the Internet is an integral part of many children's lives.[331] However, this has generated questions about the impact of digital technology on youth, and research gaps have emerged. Researchers, parents and caregivers, and policymakers have expressed significant concerns that technology has advanced without a clear understanding of its impact on youth health, safety, and privacy. Many of these concerns and questions were highlighted by the NASEM consensus study report, *Social Media and Adolescent Health* (as noted earlier in this report). Notably, one of the recommendations from the NASEM report was the need for the federal government to develop a research agenda.

This research agenda—formulated to inform independent and academic researchers, industry researchers, research funders, and the public more broadly—outlines critical questions in these areas and highlights important subjects of investigation that need to be further understood. It was put forth in consultation with subject-matter experts from across the U.S. government and informed by the numerous information-gathering exercises undertaken by the Task Force.

Given the ubiquity of digital devices, youth typically have their first online interactions before adolescence. However, the vast majority of research conducted assessing the harms and benefits of youth online focuses on adolescents. Many online platforms prohibit the use of their services by children under the age of 13 in their terms of service and purport to not allow users to indicate that they are under 13, which limits the potential data available for research involving this age group. For researchers looking to collect data about children interacting with online platforms, federal and some state privacy laws limit the collection and sharing of certain information about individuals under the age of 13; this may affect researchers' ability to collect data directly from children as well as different platforms' willingness to allow researchers to create mechanisms to collect that data.[332] Current evidence suggests that both passive and active social media use are associated with depression, anxiety,[333, 334, 335, 336] and suicide [337, 338] among specific groups of adolescents. Future studies can build on this body of research to clarify ***what*** makes social media use problematic (or not) for ***whom*** among youth.

The Task Force recommends a research agenda that identifies design features and usage patterns that contribute to harms and identifies design features that support youth well-being in the dynamic

online environment, including the quality of friendships, self-esteem, interpersonal relationships, sleep, mental health attention span, and various other outcomes of interest.

OVERARCHING GOALS AND OBJECTIVES OF THE RESEARCH AGENDA

In shaping a research agenda, it is important to acknowledge that societal concerns about the health, safety, and privacy of youth who use digital and social media encompass a broad spectrum of interests and concerns. The purpose of this research agenda is to identify where there is a critical need to build on existing literature and to facilitate new lines of inquiry that will begin to address these concerns and provide empirical evidence on which programs, practices, and policies can build.

The research agenda is arranged according to (1) research objectives, (2) domain-specific research topics, and (3) research approaches and methods. These should support the well-being of children, including their mental health, safety, privacy, self-esteem, quality friendships and relationships, and other outcomes.

OVERARCHING RECOMMENDED OBJECTIVES

1 **Develop and evaluate scalable interventions to protect children's online health, safety, and privacy.**

Future research opportunities should prioritize evaluating the efficacy of interventions that can be deployed at scale. Which parental strategies and technical controls will help ensure children's online health, safety, and privacy? Which strategies for protecting safety also protect the privacy necessary to support children's development as independent and autonomous individuals, while also maintaining trusted relationships with parents and caregivers? How do privacy violations, such as loss of control over images, affect children's mental health? How does surveillance by parents and caregivers affect children's mental health? What types of digital literacy interventions are effective, in both the short- and the long-term, and can be successfully implemented for all students across school districts? Particular attention should be paid to experimental designs that follow students throughout their development.

2 **Continue to study harms associated with children's exposure to online platforms, and intersections with risks.**

Given that online platforms are deeply integrated into the lives of youth today, future research should center on understanding harms, and the various factors that contribute to them, in both the online and physical environment, which are no longer mutually exclusive domains, rather than assuming that all harms begin and end online.

3 **Broaden access to platform data and algorithms.**

Research on how digital technologies and platforms affect youth faces significant challenges due to a lack of key information related to **how platforms are used** (e.g., patterns of usage time and forms, such as active versus passive) and **designed** (e.g., methods of procuring, applying, and securing user engagement information and behavioral data, and safety design that leverages advancements in AI and machine learning). Stated differently, data about "algorithmic design and operation should be of sufficient granularity to allow researchers to understand when, why, and how users are shown different types of content."[339]

4 **Understand child development as encompassing individual differences and contextual factors.**

Studies need to examine the differential impacts of the digital world, defining and assessing risk and protective factors. We need to better understand what is good, neutral, and/or bad for different individuals and groups of individuals (e.g., age groups, disability status, race/ethnicity, etc.). Additionally, studies need to incorporate contextual factors. These may include peer behaviors and social connections; parental digital behavior and its impacts; parental monitoring or digital restriction practices; influence of parenting styles; influence of parents' work environments; and school and community norms and influences. Research is also needed on the importance of privacy for children's development, including mental, physical, and emotional development.

RESEARCH TOPICS AND DOMAINS OF INTEREST

The Task Force identified crucial research topics and domains of interest that reflect the current trend and gaps in scholarship related to online platform use and its impact on mental and physical health, safety, and privacy. Given the evolving landscape of research and the pressing need to translate science to practical guidance for children and youth, parents, clinical providers, and policymakers, we present select areas of research that we can strategically build upon.

MENTAL AND PHYSICAL HEALTH AND WELL-BEING RESEARCH PRIORITIES

- ✓ **Multidisciplinary research that focuses on a holistic view of youth well-being.** Mental health is integrated into other health domains and therefore should not be studied in isolation. It is influenced by and influences other health outcomes like physical health, sleep health, cognitive function, and academic learning and achievement. Given the complex relationship between youth and technology, it is important that studies bring together epistemologies that include brain development, psychology, physical health, education, computer science, social interactions, social determinants of health, and societal influences.
- ✓ **Research that ensures a lifespan perspective with comparisons across different age groups, from infancy to emerging adulthood with the use of measures that are age-appropriate.** This also requires foundational research on digital and social media use and their impacts on youth mental health that addresses developmental mechanisms/processes and trajectories.
- ✓ **Longitudinal studies that consider the potential causal impact of the digital world on children and youth well-being and social, emotional, and cognitive development as well as their mental and physical health.** What is a healthy use and what is an unhealthy use, for whom and in what contexts? How do different kinds of surveillance by platforms, peers, or parents and caregivers impact youth well-being and social, emotional, and cognitive development as well as their mental and physical health? Which specific design features are harmful or beneficial, and which lead to more or less usage over time?
- ✓ **Data-informed theories and conceptual models to address how digital and social media exposure and usage impact developmental trajectories and health outcomes for youth from infancy and early childhood through adolescence and emerging adulthood.** Such research would address parenting styles and caregiving practices, economic resources, and diverse cultural backgrounds, including race and ethnicity, sex and gender, sexual

orientation and gender identity, language(s) spoken in the home, and disability status. Questions of interest include how digital and social media exposure and usage affect empathy/compassion; social or emotional competence; executive function; self-regulation; language development, early literacy, and numeracy skills; attention and memory processes; motivation; identity; creativity; gross and fine motor function; physical development and health; activity level; sleep; and weight status.

- ✓ **Core components or constructs of technology that will remain relevant as technology changes.** Research tool and metric development is needed to effectively measure youth behavior across a dynamic landscape of apps, platforms, and technologies, as well as impact on their mental health, physical health, and well-being.

- ✓ **Emerging technologies.** Since research on youth and emerging technologies tends to lag behind what youth, schools, parents, and communities have access to and are engaging with, there is an urgency to ensure that research is keeping up with the rapid pace of technological development, especially to ensure youth health, safety, and privacy. For example, recent innovations in virtual reality, voice recognition, and AI are poised to have major impacts on youth interactions with their digital ecosystem, yet research in this area is nascent.

- ✓ **The impact of varying levels of exposure.** Research on the impacts of exposure levels—such as the amount of time spent online, differences depending on the time of day for usage, benefits of breaks, passive or active engagement online, performative or exploratory use, and other factors—may help better identify and understand the impacts of exposure on sleep, mental health, and other outcomes.

SAFETY RESEARCH PRIORITIES

- ✓ **Prevalence studies of youth across development experiencing** online harassment, abuse, cyberbullying, and sexual exploitation and the nature of those harms on online platforms, including updates to key federal data sets and public health surveillance tools that measure youth well-being.

- ✓ **Clinical research** examining when, whether, and under what circumstances, an individual's engagement with computer-generated material, including CSAM, could result in harm, the nature of those harms, and the long-term impacts, including means to mitigating the harms.

- ✓ **Evaluation research on existing programs** designed to address online safety to determine which aspects of these programs yield positive outcomes and which aspects do not.

- ✓ **Experimental designs randomizing types of safety messages,** and other prevention programming, among youth populations and adults to determine the effectiveness of these messages in changing youth attitudes, behaviors, and decision-making.

- ✓ **Contextual factors that increase risk for, and fortification against, the sexual exploitation and abuse of children and youth online.** This includes assessing the impact of race, ethnicity, socio-economic status, disability status, sex, sexual orientation, and gender identity on the identification, and response to, child sexual exploitation and abuse victims and provision of services.

- ✓ **Best practices to help prevent the sexual exploitation and abuse** of youth online, with particular attention paid to the content of prevention messaging and to the individuals (e.g., law enforcement, school-based professionals, parents, youth leaders, etc.) best positioned to deliver that messaging.

PRIVACY RESEARCH PRIORITIES

- ✓ **Privacy risk profile of youth over stages of development.** Chronological age is currently used as the primary policy and technological benchmark for determining when an individual is developmentally ready for a variety of tasks, the privacy risks that children or teens face, and the best ways to tailor policies to youth development. However, is age the best metric for differentiating the risks that youth face in diverse contexts? What are alternative metrics to consider in policy-making spaces? How can protections and controls be developmentally tailored for parents?
- ✓ **Policy and practice standards on children's online usage and health.** There have been several state-level laws implemented with respect to children online. These are natural experiments being run in the laboratories of democracy, and data should be carefully collected. Researchers should study the effects of any federal policy affecting children online. More research should also be done on the uptake of standards in practice and the effectiveness of standards in supporting youth well-being. Research and evaluations on the effectiveness of laws that have been passed in other countries affecting children online (e.g., Online Safety Act in the UK, Online Safety Act in Australia, and Digital Services Act in the EU) should be conducted.
- ✓ **Long-term and systemic risks of privacy considerations.** Specific areas of inquiry include: What is the relationship between children's perception of surveillance and their mental health? Additionally, what is the impact of constant surveillance from their peers, including on the mental health and development of children and youth? Does a lack of privacy affect children's activities in the long term or does it increase the prevalence of privacy cynicism?[340] How do privacy attitudes and privacy education interventions in childhood affect identity theft rates in adulthood?
- ✓ **Efficacy and effectiveness of privacy protections for children.** No longer can Internet privacy concerns focus solely on personal interactions with a computer or phone. A variety of current and developing technologies, including smart speakers, toys, and other household objects, pose privacy threats. Common household items such as toasters, thermostats, and door locks often have the ability to gather user information and transmit it online in what is called the Internet of Things.[341, 342] Wi-Fi antennas may have the ability to sense where a person is in their home.[343] AI chatbots gather information from their users for further training.[344] Technological change is happening quickly. What distinct privacy risks do these new technologies and business models pose? What legal frameworks are necessary to ensure children's privacy in these new markets and products?
- ✓ **Effects of ubiquitous computer use in schools.** Educational technology, which became omnipresent during the COVID-19 pandemic, can pose privacy risks for children.[345, 346] What are the continued effects on children of educational technologies that were widely adopted during the pandemic? Schools are able to monitor children's online behavior, but this comes with a tradeoff in privacy. How are schools adapting to this? What are the effects on privacy, safety, and well-being?

RESEARCH APPROACHES

The Task Force identified a wide range of research approaches and methodologies that are beneficial in this domain, such as:

Including a broad spectrum of online platforms and spaces.

Research should include studies of different platforms, types of content, behaviors in the digital ecosystem, and social media, as well as but not limited to group chats, gaming, and augmented and virtual reality (AR/VR) technologies.

Focusing on causal and interpretivist research.

Future research should prioritize evaluating whether causal relationships exist between different types of online platform use/design and various health, safety, and privacy outcomes for youth. This should include use of qualitative research that emphasizes young people's subjective experiences and understandings of their use of online platforms—not just quantitative analysis of more easily observable platform usage statistics. Among the key questions to consider are: What are the complex causal linkages between social media use and mental and physical health outcomes?[347] Which interventions will improve the well-being of specific groups of youth? Which specific online behaviors and aspects of platforms (e.g., designs, features, algorithms, etc.) influence mental health outcomes, such as depression, anxiety, compulsive or problematic use, self-harm, and suicidality, or affect daily functions, such as sleep, school, or daily tasks? How is the use of social media—and the potential harm it causes—related to the beliefs, norms, and values of society broadly?

Including new methods for assessing what data are collected and with whom data are shared, including through monetization processes.

It is critical for social media platforms to provide independent researchers with access to data to assess the impact on youth health, safety, and privacy (see page 41, "Make Data Accessible for Independent Research"). For a variety of reasons, platforms do not provide what data are collected and with whom data is shared, which makes answering research questions difficult. Additionally, advancements in rapidly changing technologies, such as augmented and virtual reality, offer new avenues for engagement on digital platforms. As platforms collect new data for which the privacy implications are unclear, such as eye movements and telemetry data,[348, 349] there is a need for research cataloguing the data types[350] that are collected and their implications for health, safety, and privacy.

Engaging youth.

Technology is fully integrated into the youth experience. Adult researchers need to understand that technology is the currency of youth and that youth understand and experience digital cultures in different ways than adults do, making youth perspective essential. It is imperative to ask what youth want to know about digital behavior, the risks and benefits of social media, and the impacts of social media and the digital ecosystem on their own development and long-term outcomes. Additionally, methodologies that are participatory, such as action research and "citizen science" involving youth, may capture specific insights into their experience with health, safety, and privacy online.[351]

Next Steps for Policymakers

The Task Force brought together representatives from agencies and departments across the federal government with expertise in youth mental health, the Internet and online platforms, law enforcement, and education to identify recommendations for addressing risks to youth health, safety, and privacy online. This interagency work has been fruitful and critical to address these complex challenges. The Task Force members believe the federal government should continue convening the relevant agencies to facilitate operationalizing and implementing the report's recommendations.

In addition, the Task Force identified a number of priority areas for future work by federal policymakers to help improve young people's health, safety, and privacy online:

- ✓ **Call for Congress to enact federal legislation to protect youth health, safety, and privacy online.**

  The Biden-Harris Administration has repeatedly called on Congress to enact both comprehensive federal privacy legislation and legislation to bolster protections for young people's health, safety, and privacy online. A baseline set of data privacy protections for all users from federal legislation should include age-appropriate protections for online privacy. Platforms and other interactive digital service providers should be required to prioritize the safety and well-being of young people above profit and revenue in their product design. This entails designing technology that suits a child's developmental stage, prohibiting online platforms from collecting personal data from kids and teens, banning targeted advertising to young people, and implementing measures to protect children's mental health and safety and keep children safe from those who would use online platforms to harm, harass, and exploit them. Additionally, it includes requiring data transparency to facilitate independent research aimed at understanding and mitigating online risks faced by youth users.

- ✓ **Advance industry action to implement age-appropriate health, safety, and privacy best practices on online platforms.**

  Most existing industry efforts to promote youth online safety are voluntary and have yet to yield clear results. In addition to pursuing legislation as discussed above, policymakers should engage industry to build on existing voluntary principles[352, 353, 354] to reach additional voluntary commitments to implement specific design interventions—informed by the recommended practices for industry in this report—to protect youth health, safety, and privacy on their platforms. These commitments should come from a broad set of industry players who shape kids' online experiences, including platforms, mobile app stores, mobile app developers, self-regulatory organizations (including those that provide ratings and other information), website operators, and others. These commitments should also include agreements to provide regular public reporting on the status of their efforts and to enable transparency through independent research and evaluation of the efficacy of these interventions on their platforms.

  Complementing federal legislation that establishes health, safety, and privacy protections, areas where policymakers could bolster industry accountability by securing voluntary commitments include areas discussed in the industry recommended practices in the Task Force report, such as:

- Limiting platform design and features that materially increase engagement online or decrease online safety.
- Developing reliable, effective, privacy-preserving age assurance technology, including understanding the potential role of device-level age assurance and opportunities for simple yet meaningful parental consent.
- Improving consistency of mobile app ratings across app stores, including age ranges, features, and privacy settings of apps.
- Banning targeted advertising to children's accounts and collection of geolocation, biometric, and other personal data.
- Agreeing to common terminology for privacy and safety features, tools, and settings across services to ease the burden on parents.
- Developing consistent approaches to transparency reporting and measurement of online platforms.

✓ **Work to require access to platform data for independent researchers in privacy-preserving ways.**

Improving young people's online experiences requires more research into the effects of online platforms and other digital technologies, and the efficacy of interventions, on youth mental health and safety. Federal policymakers should identify the legal, practical, and resource barriers to independent research on online platforms and take action—including through legislation and voluntary industry commitments—to address these barriers. Congress should enact legislation to require platforms to provide vetted independent researchers with tiered access to data in privacy-preserving ways. Federal policymakers should develop guidelines for independent researchers accessing and processing data subjects' human rights, and research ethics, and offers context-specific guidance on methods for studying youth online. Policymakers should also continue to collaborate with international partners in developing mechanisms for enabling researchers to access platform data in ways that are equitable and protect users' privacy.

✓ **Provide support for research into youth health, safety, and privacy online.**

Policymakers should support research on youth online health, safety, and privacy. This support should prioritize research that incentivizes community-research collaborations that focus on emergent technology, translating the relationship between offline and online vulnerability, and effective interventions. There should be a particular focus on the impact of technology on child and adolescent development. Federal agencies that fund research should coordinate research priorities. This should complement support for prevention and education/curriculum development efforts.

✓ **Promote youth voices in solution setting.**

Young people are active participants in their own online safety and have crucial insights into their own experiences and those of their peers. Their voices should be incorporated into policymaking discussions at every level to provide feedback and input to federal policymakers.

Federal agencies should conduct self-assessments of how they are currently incorporating youth voices into policymaking and, as needed, develop and share processes and practices to better engage youth.

- ✓ **Support access to and implementation of new and updated resources tailored for youth, parents, health providers, and educators.**

  Using the best practices for parents and caregivers developed by the Task Force as a starting point, policymakers should support schools, public libraries, health providers, and other institutions in developing and implementing resources that focus on best practices for protecting children's online health, safety, and privacy; promoting benefits of using online platforms; building healthy digital habits; supporting the development of digital citizenship and media literacy skills; and mitigating the risk of harm. The Task Force supports dissemination and implementation of the 5 C's Framework, outlined in the Best Practices for Parents and Caregivers section of this report, as well as incorporating tips for parents and young people for online safety, mental health, and well-being from the Surgeon General's Advisory on Social Media and Youth Mental Health. The Task Force also recommends the educational materials and resources developed by DHS through the Know2Protect campaign, which offers tools and information to (1) empower young people, parents, and trusted adults on ways to prevent and combat exploitation and abuse both on and offline, (2) explain how to report incidents of these crimes, and (3) offer support resources for victims and survivors of online child sexual exploitation and abuse.

- ✓ **Engage in international efforts to collaborate on online safety.**

  The United States works bilaterally and multilaterally with its international government partners on online safety and security efforts. There also continues to be a growing international community of digital safety regulators, as governments around the world grapple with the need to promote young people's well-being online. The United States should join the Global Online Safety Regulators Network as an official observer or exchange best and promising practices on protecting youth privacy and safety online and continue to engage in these discussions and promote the development of effective and rights-respecting common approaches worldwide.

Conclusion

Digital technology is ubiquitous in the lives of children and youth. Their interactions with the digital landscape are embedded in a complex system involving peers, parents, schools, and the larger world. In addition, technology and digital media are changing rapidly. The ways in which youth engage with these media today may not be the way they will engage a year from now. Thus, addressing health, safety, and privacy concerns for youth online must involve an on-going, whole-of-society approach in which industry, parents and caregivers, schools, health providers, other community-based organizations, and policymakers play their roles, informed by insights from a robust research community, and from engaging with youth voices.

APPENDIX

Appendix A

INTEGRATIVE SUMMARY OF ROUNDTABLE DISCUSSION GROUPS AND SUMMARY OF INFORMATION GATHERING METHODOLOGY

The Task Force consulted with a wide array of experts and stakeholders[355] to inform the development of best practices for parents and caregivers; best practices for industry on safety-, health-, and privacy-by-design, a research agenda, and next steps for policymakers. Information from key stakeholders was primarily gathered through the following methods:

ROUNDTABLE DISCUSSION GROUPS

SAMHSA hosted six 90-minute virtual roundtable discussions with representatives from mental health professional associations, researchers, youth agencies, parents, teachers, educational organizations, and young adults between August 31, 2023, and March 6, 2024. Participants responded to a public announcement of the roundtable events and were invited based on their expertise on youth and social media. Each roundtable session addressed the following: (1) current and emerging risks of harm and potential health benefits to minors associated with online platforms; (2) measures and methods for assessing, preventing, and mitigating such harms; (3) research needs regarding online harms and health benefits to minors; and (4) best practices and technical standards for transparent reports and audits related to online harms to the health, safety, and privacy of youth.

On January 18, 2024, NTIA hosted a public listening session focused on the concrete and actionable steps that industry is taking—or can consider in the future—to improve the environment for all minors online.

Requests for Public Comments

The Department of Commerce's NTIA received over 500 written comments in response to its Kids Online Health and Safety Request for Comment (RFC), which was issued in September 2023.[356] The RFC was designed to gather information about social media and online platforms' impacts on minors, current industry practices, and ways in which current and future industry efforts could be used to mitigate harms and promote the health, safety, and well-being of minors online.[357]

Principal Listening Sessions

White House | ***Washington, DC, February 2, 2024***

- Convened a discussion with co-chairs and representatives from the Task Force and 13 representatives from youth advocacy, civil society, academia, and industry to understand the risks posed by social media and other online platforms and identify solutions to mitigate those risks.[358]

Stanford University | ***Palo Alto, CA, March 13, 2024***

- Convened an event, hosted by the Stanford Cyber Policy Center and attended by nearly 100 participants, that included high school and college-age students describing their experiences and what they and their peers would like to see changed with online platforms and services.[359] The event featured co-chairs and representatives from the Task Force, industry

experts, and child safety and civil liberties advocates.[360]

Emanuel Preparatory School for Math and Science | ***Fortson, GA, March 25, 2024***

- Convened a hybrid discussion, facilitated by the Morehouse School of Medicine and attended by co-chairs and representatives from the Task Force, with nearly 60 parents and elementary and middle school students from the Columbus, GA area to discuss their experiences with youth online safety and mental health.

SAMHSA hosted a series of six roundtable discussions with key stakeholders who have technical and experiential knowledge of youth and social media. They reported on "the status of existing industry efforts and technologies to promote the health and safety of children and teenagers vis-à-vis their online activities, particularly with respect to their engagement in social media and other online platforms."[361]

SAMHSA organized six 90-minute virtual roundtable discussions between August 31, 2023, and March 6, 2024. Participants responded to a public announcement of the roundtable events and were invited based on their expertise on youth and social media. Each roundtable session addressed the following areas: (1) current and emerging risks of harm and potential health benefits to minors associated with online platforms; (2) measures and methods for assessing, preventing, and mitigating such harms; (3) research agenda regarding online harms and health benefits to minors; and (4) best practices and technical standards for transparent reports and audits related to online harms to health, safety, and privacy of youth.

Participants responded to each focal area on ***Mural***, a virtual whiteboard platform for each topic area, followed by a 15–20-minute group discussion, during which they elaborated on their entries and answered additional discussion questions.

SESSION PARTICIPANTS	DATES
Behavioral Health Providers	8/31/23
Research Groups	9/13/23
Youth and Parent Organizations	9/20/23
Education Organizations	9/27/23
Parents of Minors	2/27/24
Young Adults Ages 18 - 25	3/6/24

Integrative Key Findings

1. Current and emerging risks of harm and potential health benefits to minors

- Framing the potential harms and benefits of social media use should consider ***developmental*** (age, brain maturation, "windows of vulnerability"—early childhood and early adolescence), ***individual*** (vulnerabilities and resilience, history of mental health concerns—most notably depressive, anxiety, and trauma/stressor-related disorders; minority status based, but not exclusively on race, physical/ cognitive ability, and sexual/ gender identities), ***social*** (peer comparison, isolation), ***family*** (guardian supervision),

and ***regional*** (urban, suburban, rural) factors, and how these factors interact with each other to affect youth engagement with online content. "Blanket, broad categories" that contribute to broad sweeping "polarized discourse" are not helpful. (Sessions 1, 2)

- Potential harms of social media broadly include (but are not limited to): (a) offline vulnerabilities of youth ("…address the issues young people have outside of their lives online because technology just makes the struggle they experience in real life more visible") (Session 2); (b) nefarious online adult actors who intend harm on youth (sex-tortion); and (c) social media platform designs that are not necessarily intended to harm youth (Session 2, 3, 5).
- Potential benefits of social media broadly provide: (a) safe alternatives to offline support and access to otherwise unavailable or less available offline information and programming; (b) opportunities to promote youth agency, activism, and self-expression; and (c) supplemental skills building (e.g., social skills for neurodivergent youth) (Session 4, 5).

2. Assessing, preventing, and mitigating such harms

- Different stakeholders have described efforts they say are intended to contribute to mitigating harm and amplifying benefits of social media use. However, these efforts have been siloed and are not always equitably distributed: (a) ***Industry.*** Prioritizing the development of accessible and simplified resources to improve digital literacy for parents and youth, transparency of how "back-end" algorithmic and user data are used (e.g., monetizing private information); (b) ***Schools***. Promote social-emotional learning, digital citizenship, and civics; encourage reporting of cyberbullying; consider burden placed on educators to integrate social media with pedagogical practices; address how social media has affected student attention capacities; and (c) ***Families***. Consistently engage children in conversations about social media use, especially when they receive their first smartphone, increase parental monitoring and supervision without being overly punitive (Sessions 1, 2, 3, 4).

3. Research agenda regarding online harms and health benefits to minors

- Challenges to advancing research are: (1) methodological (access to hard-to-reach, vulnerable populations; access to industry-held data; definitive determination of whether, how, and the degree to which specific forms of social media use harm or benefit sub-groups of youth); and (2) resource constraints (inadequate funding for larger scale studies; multi-sector collaborations) (Sessions 2, 3).
- Research focused on establishing a causal link to a certain extent between social media, harm, and benefits may be less important than understanding what makes social media platforms safer for youth. This is especially important to consider given the rapid advances in generative artificial intelligence and how this technology will likely reshape the curation of social media content for youth (e.g., altering on-line photos with exploitative intent) (Sessions 2, 3, 4).

- Broaden research across a wider developmental span – with attention on onset and prevention of vulnerabilities that place young children <10-years-old at higher risk of harm when using specific social media platforms (Sessions 1, 2, 3).
- Further clarify the relationship between on-line and off-line behavior. Consider examining, for example, how patterns of social media use and its effects "can provide valuable insights into students' lives that would otherwise remain concealed" (Sessions 2, 4).
- Address potential harms and benefits of social media use for: (a) specific groups based on primary language, social-economic class, region, sex, age, and sexual identity (Session 1); and (b) users of platforms with specific design features (Session 1, 2, 3, 5).

4. Best practices and technical standards for transparent reports and audits related to online harms to the health, safety, and privacy of children and teenagers

- Participants highlighted that recommendations to date for best practices have been polarized and siloed – underscoring the need to identify a balanced common ground that is youth-led and centered and supported by tech companies (Session 1). Different approaches to date have included: (1) policy and legislation (Kids Online Safety Act; California Age Appropriate Design Code); (2) banning or restricting minors' access to social media platforms at home and school; (3) government (federal and state) and third party (research centers) regulatory oversight – with particular attention on preventing extreme and explicit harms of online sexual exploitation; (4) social media platform design which permits more user control and promotes agency of online use; (5) prevention of early stages of "grooming" youth for victimization; (6) online and local community resources that guide parents and youth seeking to minimize harmful use of social media; and (7) exemplar global legislation and reform, most notably in the EU (Digital Services Act) and UK (Age-Appropriate Design Code Digital Services Act (Sessions 1, 2, 3, 4).

Findings from each roundtable discussion are summarized below:

Kids Online Health and Safety (KOHS)

Roundtable Discussion Summaries

SAMHSA
Substance Abuse and Mental Health Services Administration

In response to the United States Surgeon General's Advisory on Social Media and Youth Mental Health, the Substance Abuse and Mental Health Services Administration (SAMHSA) conducted a series of six roundtable discussions to gather insights from different stakeholder groups on the impact of social media on youth mental health and safety.

SAMHSA conducted 90-minute virtual listening sessions with six stakeholder groups:

- Behavioral Health Providers (held on August 31, 2023)
- Research Groups (held on September 13, 2023)
- Youth and Parent Organizations (held on September 20, 2023)
- Education Organizations (held on September 27, 2023)
- Parents of Minors (held on February 27, 2024)
- Young Adults Ages 18 - 25 (held on March 6, 2024)

The roundtable sessions were organized to support an open dialogue between facilitators and stakeholders through the use of guiding questions, thought exercises, and a real-time mural board tool to visually capture and organize ideas. Each roundtable session was transcribed to ensure that discussions were accurately documented for analysis. SAMHSA conducted a thematic analysis of the transcripts and mural boards to identify five broad topic areas within each stakeholder group.The five topic areas include:

Topic Area 1: Managing Social Media for Maximized Benefits

What are the ways that youth manage social media and online behavior to maximize the possible benefits and minimize potential harms?

Topic Area 2: Measuring, Assessing, and Preventing Harms

What are your observations with methods for measuring, assessing, and preventing potential harms of online platforms and social media?

Topic Area 3: Effective Practices for Minimizing Harms

What are useful or effective practices and/or resources aimed to prevent/ minimize the harms of online use among youth?

Topic Area 4: Further Research for Safety & Wellbeing

What research exists on this topic and what further research is needed to inform strategies for ensuring the safety and well-being of youth in online environments?

Topic Area 5: Role of the Federal Government

What role could the Federal Government play in enhancing the safety of minors who use online platforms?

Kids Online Health and Safety (KOHS)

Roundtable 1: Behavioral Health Providers & Groups | August 31, 2023

> *"There is a large interest among young people to be at the table, working to make sure that what organizations are doing is authentic and relevant."*

Roundtable Takeaways

The issue of social media and its effect on youth mental health is highly complex; addressing it necessitates bringing a diverse group of stakeholders to the table – with youth group involvement as a priority.

There is no "one size fits all" solution. An approach should not be overly broad but rather youth-focused, developmentally-centered, and sensitive to the needs of youth groups that are especially vulnerable to harm, such as LGBTQIA+ and BIPOC youth, youth with disabilities, and adolescents.

Benefits & Harms of Social Media for Youth

1. Bullying, screentime, and the potential for misinformation were the most common harms cited by participants.
2. Blanket generalizations that "all screens are bad" are common among adults. Adults do not fully appreciate how nuanced and sophisticated youth are in their understanding of social media's harms and benefits; the approach to preventing harms should be just as nuanced.
3. Social media can promote a sense of community among youth, offering a space for them to find otherwise unavailable information, acceptance, and support.
4. Certain youth groups are more vulnerable to the negative impact of social media than others.

Measuring, Assessing & Minimizing Harms

Participants suggested social media companies should be more proactive in preventing harms by enforcing their current policies and harm monitoring as well as including digital literacy tools in their platforms.

Groups more vulnerable to the negative impact of social media may need targeted support and interventions to mitigate these risks and ensure equitable access to the benefits of social media.

Educational resources and digital literacy training for youth, parents, and caregivers were endorsed as a strategy to prevent harm.

Ideas for Further Research

More research is needed to understand disparities in the negative impacts of social media and how certain youth groups are disproportionately affected.

Real-time content analysis to understand how demographic groups are impacted by content differently.

Effective strategies to inform and empower parents, healthcare providers, and trusted community sources on tools and interventions.

Suggested Actions & Policy Implications

The federal government has a role to play in helping regulate the digital ecosystem, fund research, and hold industry accountable. Engaging the youth voice and involving diverse community groups with wide representation will bring balanced perspectives and ensure cultural alignment.

Passage of the Kids Online Safety Act (KOSA) was suggested as a positive step forward.

Participants suggested requiring social media companies to make investments in research and training for those who interact with youth regarding social media use.

SAMHSA
Substance Abuse and Mental Health Services Administration

Kids Online Health and Safety (KOHS)

Roundtable 2: Research Groups | September 13, 2023

> *"Techno-deterministic rhetoric is unhelpful. The key is to focus on the broader context in which the technology fits into place."*

Roundtable Takeaways

Despite what most adults believe, a direct link between social media use and youth mental health has not been sufficiently proven by current research. Research on this issue remains challenging due to inadequate funding, lack of transparency and access to algorithmic and user data from tech companies, and a lack of diversity in sample groups.

Youth mental health is more complicated and nuanced, with root causes involving offline behaviors and environmental factors. Technology is an amplifier of issues that exist offline, not necessarily a cause.

Focus should shift from blaming technology to improving platforms for youth using a balanced, evidence-based approach.

Benefits & Harms of Social Media for Youth

1. Prevailing thought leadership making causal claims from correlative studies are flawed, misinforming, and divert attention from a substantive examination of real root causes.
2. Youth mental health is a complex and multifaceted issue. Focus on online safety should not be to the exclusion of addressing the bigger ecosystem and issues youth are facing holistically.
3. Rather than centering the tech, center the child. Youth who are more vulnerable online are more vulnerable in other contexts as well. Technology makes their vulnerability visible or augments existing issues.
4. Potential harms are not about the technology per se, but about the dynamics with peers, strangers, or content that is upsetting to them.

Measuring, Assessing & Minimizing Harms

Youth are often better than adults at navigating social media and tailoring it for their needs. In contrast to the stereotype, youth curate their online presence and do employ measures to protect privacy and minimize harm.

Social Emotional Learning (SEL) educational focus can help youth develop essential skills, cultivate empathy, teach digital literacy and citizenship, and build resiliency.

A paradigm shift is needed - away from blaming technology for harm to improving platforms to enable youth to achieve their goals.

Ideas for Further Research

How platform design features impact youth outcomes and experiences.

Research about which platform designs and educational interventions are most effective for youth at different ages and developmental stages.

Longitudinal studies exploring how external stressors are predictive of social media use and its effects.

Suggested Actions & Policy Implications

Participants suggested that legislation be mindful of the balance between protecting children from harm and enabling them to find necessary supports through social media.

Algorithmic and user data transparency, data sharing rights, and regulating data protection were suggested as a policy priority to allow researchers to have access to better data and users to control how their data is used.

Funding for the development and dissemination of social media education and digital literacy training is needed.

SAMHSA
Substance Abuse and Mental Health Services Administration

Kids Online Health and Safety (KOHS)

Roundtable 3: Youth & Parent Organizations | September 20, 2023

> *"Platforms are under no obligation to be transparent in a way that will give us the full picture. Until we have regulation, we are dealing with half-measures."*

Roundtable Takeaways

A sense of helplessness that tech companies are solely responsible and "hold all of the cards" has led to frustration that there is only so much adults can do to keep youth safe from harms online. Proactive conversations with youth lead to positive outcomes, but the burden cannot lie solely on parents to protect children online.

Commercial interests preclude child safety online. Unless social media companies are compelled to be transparent and make changes to platform design, they cannot be counted on to do so. Whether through punishment or incentive, social media companies must be involved and accountable for change.

Benefits & Harms of Social Media for Youth

1. The "Wild West" nature of the social media ecosystem has allowed companies to prioritize profit over user safety. Commercial interests supercede child welfare and safety online.
2. The complexity of online challenges faced by youth today is not fully understood. Negative experiences are inconsistently reported, either because victims are reluctant to come forward or are not aware of how to.
3. Youth have a level of awareness about the harms and have become savvy at self-regulating and detecting misinformation. However, rather than relying on their ad hoc strategies, youth should have better access to tools and resources.
4. Proactive not reactive measures are needed. Parents feel ill-equipped to take proactive measures, but if not addressed, the consequences of social media's harms can be severe.

Measuring, Assessing & Minimizing Harms

Youth who have open, proactive conversations with adults about social media tend to have more positive experiences and are more open about negative experiences.

Parent-oriented, youth-focused digital literacy education, social media best practices, and training about how to have age-appropriate conversations at every developmental stage is needed.

Social media companies, schools, peers, parents, trusted mentors, and even youth ambassadors and influencers all need to be involved in promoting online safety as a community-wide effort.

Ideas for Further Research

Long-term research on the impact of digital literacy and education efforts for parents supporting youth with safe practices online.

The development of a permanent mechanism for monitoring and sharing user data to protect from harm.

What issues would most compel social media companies to put people over profit?

Suggested Actions & Policy Implications

Federal government is an important "convener" to bring all voices together and level the playing feld - academia, parents, schools, youth, public health, tech companies and even influencers all need to have a seat at the table.

Government can play a proactive role in sharing resources, toolkits and information about existing policies or new legislation when it is passed.

Government could provide necessary funding for more research and digital literacy education programs.

SAMHSA
Substance Abuse and Mental Health Services Administration

Kids Online Health and Safety (KOHS)

Roundtable 4: Education Organizations | September 27, 2023

"The goal is to acknowledge the reality of social media's presence in everyday life and explore how it can be leveraged positively.".

Roundtable Takeaways

While online tools can be problematic for educators, students benefit from use of online platforms as an educational tool.

Digital literacy, online responsibility, and digital citizenship can be incorporated into the core curriculum, and inappropriate behavior online can be turned into "teachable moments."

The aim should be to equip students with essential skills that will equip them for a digital future. Partnerships between schools and tech companies can help build career development pathways to meet demand for digital skills in the workforce - particularly around data protection.

Benefits & Harms of Social Media for Youth

1. Online platforms can be educationally positive as a tool for research, collaboration, real-time feedback, for students with disabilities due to its flexibility, and for career networking.
2. Students struggle to manage platforms that are designed to continuously feed them content and retain their engagement. Social media impacts mental health of students and educators alike, and these concerns appear to be worsening over time.
3. Educators feel pressured to integrate online platforms into instruction, but the field lacks a clear definition of what makes a technology tool "social."
4. Concerns around data privacy, addictive algorithms, and a lack of guardrails around Artificial Intelligence (AI) and generative AI are troubling for educators who are equipping students with essential skills for a digital future.

Measuring, Assessing & Minimizing Harms

Schools need good vetting mechanisms to evaluate platforms, digital content for bias, learning progressions, and use of AI in the classroom.

Online responsibility and digital literacy can be incorporated into the core curriculum, but online safety should not be up to schools alone.

Strong school board policies developed jointly with educators are needed to establish consistent standards and safety measures. Schools, parents, and government need to be aligned and working together with the same mission.

Ideas for Further Research

Social media education practices are needed to guide effective policies at the school board level.

Methods to teach and leverage Artificial Intelligence (AI) for educaitonal benefit rather than harm.

The effectiveness of current legislation in the US and EU to make social media safer.

Suggested Actions & Policy Implications

Minimum safety standards to mandate safe storage practices as a preventative measure against cyber attacks. Regular audits for data privacy protections, safety practices, and access to data.

Convene a task force focused on AI to establish standards and guardrails with regular audits of algorithms for bias.

Recent European legislation could serve as a model for legislation that provides researchers with access needed for deeper-dive research, and for government holding social media companies accountable for safety.

SAMHSA
Substance Abuse and Mental Health Services Administration

Kids Online Health and Safety (KOHS)

Roundtable 5: Parents of Minors | February 27, 2024

"We know big brother is always listening why don't use the info they gather to inform parents of what is going on [on youth's social media] in their geographic area."

Roundtable Takeaways

Minors benefit from the opportunity to connect with family and peers outside of their local community and develop cricial thinking skills from online platforms, but time spent online, bullying, sexting and the sharing of personal information are significant concerns for parents.

Parents have developed ad hoc strategies to limit harms, but they would like access to tools and resources to support proactive measures and alert them when inappropriate or harmful activity occurs.

Benefits & Harms of Social Media for Youth

1. Social media offers youth opportunities for increased social connection to family, friends, and peers who live far away, the development of problem solving and critical thinking skills, and a sense of independence.
2. Harms such as excessive time spent on online platforms, addictive behavior patterns, sexting, and bullying are significant concerns for parents.
3. Setting boundaries around time limits for devices, online applications, and wifi access, frequent device checks, and establishing rules for using devices in shared spaces are helpful as parental controls. These strategies are most effective when paired with open conversation about why they are needed.
4. Access to tools and digital literacy resources would be beneficial for parents to inform and guide proactive safety measures and conversations.

Measuring, Assessing & Minimizing Harms

A list of red flags, warning signs to look out for, and commonly used terminology or "slang" language would be helpful to enable parents to be more proactive in preventing harm.

"Push" notifications from social media platforms alerting parents of their children's concerning or inappropriate behavior online and offering support resources could advise parents when harmful situations are developing.

Schools could provide parent education programs and student courses around use of devices/social media/gaming, the potential harms, and short- and long-term effects of online platforms.

Additional Insights

Parents noted that messaging around support information and resources could be communicated using all platforms available, not just schools, community centers, and healthcare providers, but also through podcasts, commercials, webinars, ads on the platforms themselves, and through music, art, and even TikTok dance culture.

Suggested Actions & Policy Implications

Public service announcements and public safety messaging were suggested as a strategy to make social media safer and a more positive experience for parents and youth alike.

Algorithms or SMS messaging could be leveraged to push relevent safety information to parents when concerning events happen in their local geographic areas.

Improving regulations around phone controls and settings so that they are more user friendly to parents and easier to use for restricting access to inappropriate content for youth.

SAMHSA
Substance Abuse and Mental Health Services Administration

Kids Online Health and Safety (KOHS)

Roundtable 6: Young Adults Ages 18 - 25 | March 6, 2024

"I feel like adults can dismiss the significance of social media, even if it is a positive interaction. I find that adults are quick to demonize all platforms."

Roundtable Takeaways

There is a generational divide between young adults who use social media as a tool for connection, democratized information, and self-expression and older generations who focus exclusively on the negatives of social media.

While young adults understand the potential harms of social media, the benefits outweigh the risks. Instead of imposing restrictions, parents should create a healthy environment for their child to feel safe discussing anything they experience online.

Regulation and content censoring or filtering is not the answer; instead, more resources should be available to self-check online behavior, to familiarize adults with platforms they don't trust, and to support youth in crisis using social media as a cry for help.

Benefits & Harms of Social Media for Youth

1. Young adults use social media as a tool for connection, democratized information, and entertainment, but also for self-expression - it is a key part of developing their authentic identity.
2. Adults assume that social media is solely a threat, making youth susceptible to misinformation and political bias. Young adults, however, think the abundance and immediacy of real-time decentralized information online makes them more informed and can empower broader perspectives - although algorithms can create echo-chambers by feeding content designed for engagement.
3. Parental controls and content filtering are intrusive and ineffective, denying youth information, risking free speech rights, and often resulting in youth hiding activity from parents.
4. Third party tools, self-timers, and turning off notification settings are effective tools to self-check online activity. Regulation of content is not the answer.

Measuring, Assessing & Minimizing Harms

- Clear user warnings and explicit community guidelines around the use of offensive language or content is preferable to content censoring or restrictions.
- Educational resources for parents to familiarize themselves with online platforms and normalize conversations about social media would ease discomfort, uncertainty, and distrust.
- Schools and healthcare providers who are in a position of trust should play a role in developing and disseminating youth-oriented education materials and mental health support resources.

Additional Insights

There is broad consensus that there are not enough supports or resources for youth. Barriers cited include:

- Insufficient understanding among mental health professionals of the uniquely negative aspects the medium can have on mental health.
- Not enough civil society organizations spreading awareness of available resources.
- Lack of resources tailored to youth who experience challenging circumstances offline.

Suggested Actions & Policy Implications

Hesitancy around potential regulations and policies for social media among youth stem from concerns about free speech thwarted, silencing of minority voices, and uncertainty that the internet can be regulated at all.

Government warning labels and information campaigns like there are for other potentially dangerous products like cigarettes, alcohol, vaping, etc. could be helpful in simplifying messages around potential harms.

Regulation of privacy protections may be an appropriate area for government action.

SAMHSA
Substance Abuse and Mental Health Services Administration

Appendix B

SUMMARY OF REQUEST FOR COMMENT RESPONSES

The National Telecommunications & Information Administration (NTIA) issued a Request for Comment on Kids Online Health & Safety (RFC) in September 2023 to gather information from experts, industry, and the general public about social media and online platforms' positive and negative impacts on minors; current industry practices; and ways in which the private sector, caregivers, and the U.S. government may improve young people's health and well-being online. The responses to the RFC were sought to help inform the Kids Online Health and Safety Task Force's work in developing voluntary guidance; policy recommendations; best practices on safety-, health-, and privacy-by-design for industry to apply in developing digital products and services; and questions asked in Task Force listening sessions. Below is a summary of the responses received and the entities that provided comments.

In total, NTIA received more than 500 written comments in response to its Request for Comment from a mix of industry, academic, civil society, and individual contributors. Comments have been publicly posted on Regulations.gov, under the docket NTIA-2023-0008.

In addition to comments from individuals, NTIA received comments from entities such as these below:

GOVERNMENT:

- California Privacy Protection Agency; eSafety Commissioner, Australia.

INDUSTRY AND INDUSTRY ASSOCIATIONS:

- ACT | The App Association; Association of National Advertisers, Inc. (ANA); BBB National Programs; Chamber of Progress; Computer & Communications Industry Association (CCIA); Discord Inc.; Engine (start-up association); Entertainment Software Association (ESA); Google; Information Technology Industry Council (ITI); Gaggle (student surveillance software); The LEGO Group; NetChoice; Match Group; Meta, Microsoft, Network Advertising Initiative (NAI); PBS; Pinterest, Roblox Corp.; Software & Information Industry Association (SIIA); U.S. Chamber of Commerce.

NONPROFITS/CIVIL SOCIETY:

- 5Rights Foundation; American Consumer Institute; Bipartisan Policy Center, Center for Countering Digital Hate; Center for Democracy & Technology (CDT); Common Sense Media, Center for Digital Democracy, and Fairplay (CSM et al); Electronic Privacy Information Center (EPIC); END Online Sexual Exploitation and Abuse of Children Coalition; Family Online Safety Institute (FOSI); Future of Privacy Forum (FPF); National Hispanic Media Coalition; The Phoenix Center, Public Knowledge; R Street Institute; TechFreedom; The Trevor Project (LGBTQI+ focus).

MEDICAL AND EDUCATIONAL ASSOCIATIONS:

- American Academy of Child and Adolescent Psychiatry; American Academy of Pediatrics; American Federation of Teachers; National Education Association (NEA).

ACADEMICS:

- Digital Mental Health Research Group at the University of Cambridge; Yale University – Digital Economy Project; Strategic Training Initiative for the Prevention of Eating Disorders (STRIPED) at the Harvard T. H. Chan School of Public Health and the Michigan State University College of Law; The Center for Growth and Opportunity at Utah State University; and numerous other academics in their individual capacities (from New South Wales experts on body-image issues to Cato Institute fellows).

SUMMARY OF KEY POINTS FROM COMMENTS:

1. Most commenters expressed concerns about harms to kids online and cited existing studies, often related to specific types of harms.
    - In addition to harms noted in the Surgeon General's Advisory on Youth Mental Health and Social Media, commenters included items such as:
        - The loss of time kids need for other important skill development;
        - Contribution to obesity crisis/unhealthy eating;
        - Self-harm, disruption, and danger (including a "slap a teacher" challenge);
        - Digital stress for kids, including fear of missing out and the pressure to remain online/available;
        - Distress for parents;
        - Child identity fraud;
        - Peer pressure for students—no matter the income level—to purchase items for multiplayer games.
2. Some parents and youth also detailed their personal experiences, including parents of youth who died by suicide after sextortion, from drug overdoses after exposure to online drug dealers, and eating disorders after sustained exposure to certain content.
3. Some medical and scientific experts highlighted the complexity of identifying harms and determining causality with scientific certainty.
    - This included the difficulty of disentangling online and offline factors, and comparing online consumption to eating very different types and quantities of food.
    - There were specific comments from outside the medical community, in particular, challenging causal links between youth and mental health concerns.
4. Commenters described the need for more research and the barriers to getting data.
    - This included a lack of transparency preventing understanding of scale and impact on mental health, the need for data about algorithmic practices, and the high cost to obtain data. Privacy for individuals and company proprietary data were raised as areas of concern.

- Some parties suggested different models for improving data access, such as the EU's Digital Services Act provisions or a U.S. task force on the opioid crisis.

5. Commenters provided an overview of current industry practices and technology.
    - Commenters discussed existing tools and measures to varying degrees, from general references to detailed descriptions by companies of their own efforts. Some commenters commented generally on a lack of efficacy of tools but there was little discussion of the measurement or evaluation of tools' efficacy.
    - Commenters referred to well-known tools, such as: review and age-rating of content for age-appropriateness; reporting tools; parental controls; privacy by default; CSAM and other image detection efforts; policies against targeting kids with advertising; review of chat; quiet mode and tools to limit unwanted direct messages; separate product offerings for kids; and reminders to take a break.
    - Platforms can choose not to provide support for some features on accounts for kids.
    - Other items included interventions to help users self-report and receive behavior coaching; using AI "to make everyone feel reflected and represented"; policies, teams, and technology aimed at harms such as radicalization, CSAM, and mental health harms; and a "viral circuit breaker" to minimize amplification of content.
6. The adequacy of specific tools and company efforts was questioned by experts on kids and technology as well as others. Examples include:
    - Ineffective blocking/reporting for abuse/exploitation and the failure to remove hate-related content and harassment/threats.
    - At the same time, some commenters raised concern about LGBTQI+ content, in particular, being improperly removed as sexual, leading to kids abandoning content filters altogether and, therefore, increasing risks they would otherwise have helped to avoid.
    - Some commenters expressed concern about the burden on parents/caregivers/kids to find and use tools and connected this to evidence of lower overall efficacy of those tools.
    - Another concern raised was balancing parental controls with privacy for teens, including risks of parental surveillance.
7. Some commenters provided information about existing laws.
    - Commenters discussed laws in the United States and abroad aimed at kids online generally, and privacy specifically. Some said laws protecting kids' privacy might, alone, address many of these issues.
    - California's privacy laws, which include specific measures related to kids, were noted, as were broader child-safety measures, such as in Australia, the UK (Age-Appropriate Design Code), and relevant provisions in the EU (Digital Services Act restrictions on targeted marketing, French and Italian laws).

- The global nature of online services warrants some international coordination and initiatives for consistent approaches and requirements, some noted.

8. Some suggested ways to adjust existing U.S. law to broaden coverage or spread best practices, including considering a centralized approach to child safety issues. These included:
    - Only allowing platforms to take advantage of protections from liability under Section 230 of the Communications Act if they meet a new safety-by-design requirement.
    - Considering centralized solutions, such as controls and access mediated by operating systems and devices or app stores (subject to privacy laws) or adding age-verification requirements to app stores.
    - Adopting a national safety standard (that preempts state law)
    - Requiring industry standards for ad targeting and delivery (such as limiting ad targeting to age and location).
9. There were many calls for national privacy legislation.
    - Commenters also proposed other privacy-protective approaches, including guidance and privacy by design measures. California's privacy laws, which contain special provisions for kids, were described.
10. Interventions should address specific harms yet be flexible and provide some general standards.
    - Many commenters highlighted the need for specificity in the harms to be addressed in any legislation or other measures (including adherence to voluntary frameworks). For example, incremental and small and medium-sized solutions were championed or offered.
    - Some commenters highlighted that there are different risks that exist on different platforms (e.g., direct messaging more a risk for grooming and exploitation, while cyberbullying more a risk on platforms with items like publicly visible comments).
    - Many, including those skeptical of legislative or regulatory action, urge that remedies be precise, not one-size-fits all, and include some general standards. For example, some commenters emphasized ways to tackle different risks with proportional responses and suggested to avoid being overly prescriptive and to promote interoperability.
    - The need for age-appropriate and differentiating approaches were stressed by many commentors.
11. Commenters noted both the challenges and the potential benefits associated with age verification/age assurance.
    - In addition to noting the difference that age brings to the risks of online platforms, many also highlighted the challenges of determining the age of people online. Some described the different techniques and technical challenges, while others only focused on the harms that could come from limiting access to services online by kids—or

adults who cannot or will not pass age-assurance checks—and data collection risks. Others raised concerns about state laws.

- Some proposed or reviewed risk-based approaches to age assurance to address tradeoffs and avoid unnecessary data collection.
- Some suggested the adoption of a flexible approach, such as that used in the UK Age-Appropriate Design Code implementation, and others pointed to examples of where differences in approaches are clearer, such as assuring access for adults only for pornography and gambling sites but not necessarily from general-use platforms.
- Many described existing efforts and approaches to identify users who are kids, including existing frameworks.
- Some called for the adoption of centralized age verification efforts, in part to address privacy and accuracy concerns. That included using existing infrastructure for device-level age verification such as mobile or credit card providers (for those kids who have their own devices or accounts) or app store measure; or an international certification regime with technical standards for third-party age assurance providers.
- About a dozen commenters raised general concerns about privacy risks associated with ID verification methods, and some challenged the constitutionality of age verification requirements that apply to all. A few commenters raised First Amendment concerns, including recognizing rights of older minors. Others highlighted security risks from increased collection and use of user data.
- At least one commenter raised concerns about the burdens on start-ups to implement age-verification mechanisms—including using pre-packed technology.

12. Commenters discussed existing and potential frameworks to guide interventions in favor of kids' online health and safety.

- Commenters said that companies can leverage existing privacy and data management practices to develop best practices in this area.
- Commenters discussed different general standards, such as the "best interests of the child" standard found in data privacy laws and regulations around the world, and a "duty of care standard."
- Some companies noted industry efforts to develop best practices, while others suggested their own frameworks or use of technology, arguing that self-regulatory efforts, certification programs, and safe harbors can move companies along faster than legislation mired in legal challenges.
- Commenters also highlighted the value of creating a positive environment online.

13. Commenters recommended guidance for parents, guardians, and kids.

- Some commenters recommended investment in digital literacy training and messaging, for example, highlighting Florida's new digital literacy curriculum in schools.
- Some noted the importance of different platforms streamlining words and phrases,

menus, and design/layout, including mirroring the UK Age-Appropriate Design Code (AADC) Transparency Standard.

14. Commenters proposed a variety of other solutions:

- Some noted that advertising-supported social media is not—and should not be—the only business model.
- One commenter suggested stakeholders develop databases of a) social media harms to students and schools; and (b) industry practices designed for age-appropriate content; (c) regular research and reviews; (d) accountability; and (e) funding/opportunity for long-term impact studies. Another suggested the U.S. government establish "a dedicated government office to distribute funding, conduct research, and/or oversee regulations" specific to technology, digital media, and children.

15. Regarding the role of AI and emerging technologies, a few commenters noted such technologies' role in exacerbating bullying, harassment, and other endemic challenges facing youth online.

- One commenter noted that it was important to look at specific products or service, not at AI as a distinct item, while recognizing that AI can exacerbate harms by automating and finessing problematic items.
- Commenters noted specific examples concerning uses of AI and other emerging technologies, including:
  - AI images of naked female students being circulated by their male classmates.
  - Challenges in virtual reality chats.
  - Targeted AI marketing promoting unhealthy eating.
  - AI-generated labels and applications in multiplayer games.
  - Reports of nearly 3,000 AI-generated CSAM images in the UK.
  - AI-driven content moderation, which can lead to more heavy-handed moderation than traditional content.

16. Some cautioned generally that safeguards should be weighed against benefits.

- Some warned against regulation of online platforms, often related to speech concerns. Commenters noted that:
  - Regulation could trigger legal challenges or harm innovation and free expression.
  - While harms exist, not all the problems require a regulatory or legislative solution.
  - Vagueness in requirements about safe content, in particular, could disproportionately harm the LGBTQI+ community.
  - Regulation could damage the online experience for kids by making it too sterile, interfere with teens' abilities to discuss sensitive topics, or lead to other

repressive measures.

17. Other items of note:

- Commenters raised concerns related to the lack of data about different demographic groups use of online platforms.
- One commenter challenged the traditional economic tenet that more consumption is better for consumer welfare as not accurate in the social media context and analyzed competition concepts applied to addictive aspects of technology. Another commenter suggested that competition and reputation are the surest forms of accountability for companies.
- The more than 400 comments from individuals expressed a wide array of views.
- Commenters expressed concern about the harms—including depression and anxiety—that adolescents who consistently use social media experience.
- Several commenters echoed concerns about the negative consequences that proposed safety measures in some legislation could have on free expression and, in particular, on the benefits that marginalized communities, including LGBTQI+ youth and youth of color, have derived from online platform access.
- Other comments voice concerns about, and accountability for, algorithmically promoted content and targeted advertising, as well as surveillance advertising and the loss of privacy. Some comments asked for a government database tracking algorithms and regular research on social media's effects.
- Some commenters championed the role of parental choice and control, but some noted that even with that, kids are exposed to what their friends and peers see.

Appendix C

PRINCIPAL LISTENING SESSIONS

NTIA, on behalf of the Biden-Harris Administration's Task Force on Kids Online Health and Safety, hosted a virtual listening session open to the public in January 2024, to follow up on its Request for Comment. Officials from NTIA heard from listening session attendees on the safety, health, and privacy challenges facing youth online and solutions to protect and empower them.

Participants discussed a range of topics, including:

- ✓ Centering well-being as a design goal for social media platforms.
- ✓ Calibrating privacy protections to digital services based on their risk levels.
- ✓ Addressing the addictive features inherent in the technological design and business models of online services.
- ✓ Ensuring that filtering and moderation technologies do not disproportionately harm marginalized youth.
- ✓ Supporting parents with more transparent, accessible safety features like parental controls.
- ✓ Providing researchers with the funding and data access needed to meaningfully study online platforms.
- ✓ Acknowledging the positive impacts of safe, affirming online spaces on youth mental health.

Participants at the listening session included the individuals listed below:

Listening Session Participants included:

- **Medha Tare**, Senior Director of Research, Joan Ganz Cooney Center at Sesame Workshop
- **Alexa Mooney**, Policy Counsel for Youth & Education Privacy, Future of Privacy Forum
- **Morgan Reed**, President, ACT | The App Association
- **Gaia Bernstein**, Technology, Privacy, and Policy Professor of Law, Seton Hall University School of Law
- **Aliya Bhatia**, Policy Analyst, Free Expression Project, Center for Democracy & Technology
- **David Sullivan**, Executive Director, Digital Trust & Safety Partnership
- **Maya McKenzie**, Senior Counsel, Entertainment Software Association
- **Jennifer Hanley**, Safety Policy Manager, Head of Safety Policy, North America, Meta
- **Lisa Cline**, Co-Founder, Student Data Privacy Project
- **Will Cunningham**, Senior Director, Head of Government Relations for the Americas, Match Group
- **Andrew Zack**, Policy Manager, Family Online Safety Institute
- **Kris Perry**, Executive Director, Children and Screens
- **Casey Pick**, Director of Law and Policy, The Trevor Project

COPY OF READOUT OF KIDS ONLINE HEALTH AND SAFETY TASK FORCE PRINCIPAL LISTENING SESSION

February 02, 2024

White House leaders and the co-chairs of the Biden-Harris Administration's Task Force on Kids Online Health and Safety (KOHS Task Force) hosted a listening session with academic experts, youth advocates, civil society leaders, and practitioners on advancing the health, safety, and privacy of kids online. Officials from the White House Office of Science and Technology Policy, the Domestic Policy Council, the Gender Policy Council, and the National Economic Council joined officials from the National Telecommunications and Information Administration, the Substance Abuse and Mental Health Services Administration, the Office of the Surgeon General, and the Federal Trade Commission to welcome guests and to detail the Administration's ongoing work to advance the health and safety of youth online.

Following opening remarks, participants discussed a range of topics, including:

- ✓ The harms and risks kids and teens face online.
- ✓ The necessity of digital technologies for engaging in every-day life.
- ✓ Policy and design strategies that could center children's well-being in companies' product development processes.
- ✓ The need for solutions that center the experiences and perspectives of young people, including direct youth representation in policy and design processes.
- ✓ The importance of designing digital environments that help kids thrive, while identifying and addressing risks.
- ✓ The need to balance the risks and harms of social media with the value of online platforms in building communities, particularly for historically marginalized groups including LGBTQI+, Black and Brown, and neurodiverse children.
- ✓ The risks to kids of large-scale personal data collection and advertising models of technology companies; and
- ✓ Support for President Biden's call for strong bipartisan legislation to protect children online in particular, as well as broader legislation that protects the public's privacy.

Protecting youth mental health, safety, and privacy online is a key component to delivering on President Biden's Unity Agenda – a set of priorities that Americans from every walk of life can support. This listening session will inform the Biden-Harris Administration's ongoing efforts to address the harms America's children and youth face online. More information on the Biden-Harris Administration's Task Force on Kids Online Health and Safety is available here.

LISTENING SESSION PARTICIPANTS INCLUDED:

- **Amina Fazlullah**, Head of Tech Advocacy Policy, Common Sense Media
- **Arthur C. Evans Jr.**, CEO and Executive Vice President, American Psychological Association

- **Charlotte Willner**, Executive Director, Trust and Safety Professional Association
- **Christopher Yoo**, Professor, University of Pennsylvania
- **Dan Perkel**, Partner, Media & Technology, IDEO
- **Desmond Upton Patton**, Professor, University of Pennsylvania
- **Emma Lembke**, Co-Founder, Log Off Movement
- **Jules Polonetsky**, CEO, Future of Privacy Forum
- **Kayla Bethea**, Wired Human Youth Coalition Core Leader
- **Megan Moreno**, American Academy of Pediatrics, Center of Excellence on Social Media and Youth Mental Health
- **Nora Benavidez**, Senior Counsel and Director of Digital Justice and Civil Rights, Free Press
- **Pamela Wisniewski**, Associate Professor, Vanderbilt University
- **Rebecca MacKinnon**, Vice President for Global Advocacy, Wikimedia

###

COPY OF READOUT OF KIDS ONLINE HEALTH AND SAFETY TASK FORCE PRINCIPAL LISTENING SESSION AT STANFORD UNIVERSITY

March 13, 2024

Officials from the Biden-Harris Administration's Task Force on Kids Online Health and Safety engaged with and heard from experts on the health and safety of youth online at a listening session hosted by Stanford's Internet Observatory and Social Media Lab with the Stanford Center for Youth Mental Health and Wellbeing, in collaboration with the Task Force. Officials from the White House Office of Science and Technology Policy, the National Telecommunications and Information Administration, and the Substance Abuse and Mental Health Services Administration joined with Stanford to welcome guests and to detail the Administration's ongoing work to advance the health and safety of youth online. Representatives from the US Surgeon General's Office (Director of Science and Policy), the Department of Justice's Child Exploitation and Obscenity Section, and the National Institute of Standards and Technology's Applied Cybersecurity Division were among the government attendees at the event.

In addition to fireside chats, participants discussed a range of topics, including:

- Young people are exposed to, and navigate, online communications at early ages, often with little direct help from parents, schools, or platforms themselves.
- There is a need for more transparency about what services and features involve—including using language for younger kids—well beyond when they first start to use a service.
- Better mechanisms are needed—and in some cases, already exist—to help shape kids' online experiences as they grow up. These can include increasing levels of control for kids themselves as well as tools that allow for parental oversight.
- Young people reported feeling a continued compulsion to use online services, despite negative

impacts on their lives including loss of sleep, anxiety, and depression. They attributed this compulsion to both technical design features of online services as well as social pressures (the "fear of missing out" on what their peers were doing and saying online).

- Unlike physical safety concerns for young people (such as the appropriate age to stop using a car seat), online safety issues can lack objective measures. Medical experts cannot pinpoint for parents or for companies at what precise age specific features and media are safe for the development and well-being of young people across the board.
- Most online platforms and services have been designed to take user privacy, safety, and satisfaction into account to some degree, but few of these services were designed to consider young people's well-being, specifically.
- Online methods for stopping child sexual exploitation are not adequate. There is a particular concern, given the advent of advanced image generation technology, that both platforms and law enforcement will soon be overwhelmed by AI-generated CSAM, which could further interfere with efforts to identify and intervene in cases involving the exploitation of real children. Machine-learning based image classifiers could be helpful in detecting CSAM (whether real or AI-generated) but their development is severely constrained by existing law.
- Industry and researchers lack common data formats and metrics for measuring youth well-being that would allow for better assessments of what is happening to kids online and to measure the efficacy of mitigation efforts.

This listening session will inform the Biden-Harris Administration's ongoing efforts to address the harms America's children and youth face online.

A wide variety of [nearly 100] participants, including youth advocates, experts in mental health, design, safety and privacy, parents and companies, engaged in discussion.

COPY OF READOUT OF KIDS ONLINE HEALTH AND SAFETY TASK FORCE PRINCIPAL LISTENING SESSION AT THE MOREHOUSE SCHOOL OF MEDICINE

March 25, 2024

Officials from the Biden-Harris Administration's Task Force on Kids Online Health and Safety engaged with and heard from experts on the health and safety of youth online at a listening session hosted by the Morehouse School of Medicine and Emanuel Preparatory School of Math and Science, in collaboration with the Task Force. Officials from the White House Office of Science and Technology Policy, the National Telecommunications and Information Administration, and the Substance Abuse and Mental Health Services Administration joined with the Morehouse School of Medicine to welcome guests and to detail the Administration's ongoing work to advance the health and safety of youth online. Representatives from the U.S. Surgeon General's Office, the Department of Justice's Child Exploitation and Obscenity Section, and the National Institute of Health were among the government attendees of the event.

During the two-hour listening session with parents and their children, participants discussed a range of topics, including:

- ✓ When youth experience harassment or are exposed to inappropriate content, many would rather leave the session/room/chat/game instead of using report functions on social media platforms. Leaving the session is faster than reporting negative experiences.
- ✓ During the COVID-19 pandemic, some youth used social media and video platforms to make up for lost real-world connections. These youth explained that they feel like they're talking to someone when watching videos.
- ✓ Youth see inappropriate ads online when they are looking for content that is age- appropriate for them. Parents also expressed concern that even when their children were interacting with age-appropriate content online, advertisements were often inappropriate (e.g., for alcohol, tobacco, or depicting sexual themes). In response to these experiences, some youths advocated for content moderation rules comparable to TV channels that are marketed towards children.
- ✓ Children are afraid of doom scrolling and the effects of shorts and reels on their attention spans. Some see doom scrolling and Internet addiction as potential threats to their ability to succeed offline, as they believe excessive use of certain platforms has a detrimental impact on their ability to interact with peers and teachers offline due to an inability to put devices down.
- ✓ Youth would like social media platforms to enforce timeout limits on platforms to address concerns of overuse and addiction.
- ✓ Parents employ a variety of techniques to supervise and help guide their children's use of digital technology and online platforms, including having limits on when devices can be used (e.g., not at the dinner table) and where and how certain apps can be used (e.g., streaming video apps only on the family television and not on mobile devices, certain apps only used with a parent's active participation).
- ✓ Parents also expressed a desire for devices and services that were designed to help bridge the gap between child- and adult-oriented experiences. They expressed a need to have services grow with their child and a desire for limited-functionality devices that could help tweens begin to learn how to use smartphones safely without exposing them to the entire mobile app ecosystem.

This listening session will inform the Biden-Harris Administration's ongoing efforts to address the harms America's children and youth face online.

Appendix D

BEST PRACTICES FOR PARENTS AND CAREGIVERS COMPENDIUM

The Task Force collected an extensive set of federal and non-federal best-practice resources for promoting the online health and safety of children and adolescents.

To make it easy to find resources related to social media and online platforms, the compendium has been organized into the following categories:

1. **General Information**
2. **Tools to Support Parents**
3. **Digital Citizenship**
4. **Bullying and Cyberbullying**
5. **Child Sexual Exploitation and Abuse**
6. **Teen Dating Violence and Other Forms of Gender-Based Violence**

1. GENERAL INFORMATION ABOUT YOUTH & SOCIAL MEDIA PLATFORMS

Resources in this section include the Surgeon General's Advisory on Social Media and Youth Mental Health, as well as practical tips from the Federal Trade Commission for protecting children's safety online, and NetSmartz, an online safety education program from the National Center for Missing and Exploited Children.

- ✓ **The U.S. Surgeon General's Advisory - Social Media and Youth Mental Health** - This Advisory calls attention to the growing concerns about the effects of social media on youth mental health. It explores and describes the current evidence on the positive and negative impacts of social media on children and adolescents, some of the primary areas for mental health and well-being concerns, and opportunities for additional research to help understand the full scope and scale of social media's impact. https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf
- ✓ **Protecting Kids Online** - This resource provides tips for parents from the Federal Trade Commission about protecting children's online safety**.** https://consumer.ftc.gov/articles/protecting-your-childs-privacy-online
- ✓ **NetSmartz** - NetSmartz is the National Center for Missing and Exploited Children's online safety education program that provides age-appropriate videos and activities to help teach children how to be safer online. https://www.missingkids.org/NetSmartz/home
- ✓ **Common Sense Media** - Common Sense Media gathers data and publishes articles about the impact of media and technology on kids' physical, emotional, social, and intellectual development. https://www.commonsensemedia.org/
- ✓ **Engaging, Safe, and Evidence-Based: What Science Tells Us About How to Promote Positive Development and Decrease Risk in Online Spaces** - This report provides guidelines

and recommendations for establishing healthy and developmentally considerate digital technology use for children and adolescents. https://developingadolescent.semel.ucla.edu/assets/uploads/research/resources/DigitalTechReport_FINAL_WEB_doi.pdf

2. TOOLS TO SUPPORT PARENTS NAVIGATING SOCIAL MEDIA AND ONLINE PLATFORMS

The following are a set of tools geared towards children and parents to help navigate social media and online platforms, including resources from U.S. government agencies and national non-profit national organizations that focus on specific tools to help promote online health and safety.

- ✓ **Selfies, Social, And Screens: Navigating Virtual Spaces For Youth** - This toolkit provides information, tips, and resources for young people, parents and caregivers, and school personnel on how to protect youth mental health in a digital world. https://mhanational.org/sites/default/files/back-to-school/2023/downloads/2023-BTS-Toolkit.pdf
- ✓ **Net Cetera: Chatting with Kids About Being Online** - A guide for parents, teachers, and other adults, with conversation starters on how to talk to kids about being online. Offers practical advice about how to help kids make good decisions and stay safe, including socializing online, protecting their privacy, mobile devices, computer security, and dealing with cyberbullying. https://consumer.ftc.gov/articles/net-cetera-chatting-kids-about-being-online
- ✓ **Being Tech Smart, A Plug & Play Activity for Youth** - Classroom lesson designed to supplement youth-serving organizations' programming with middle and high school youth by engaging youth in pondering questions about digital technology (e.g., social media use, accepting/declining friend requests, giving out personal information) and encouraging them to think twice before using technology. https://teenpregnancy.acf.hhs.gov/resources/being-tech-smart
- ✓ **Considerations for Social Media Monitoring and Response** - Social media monitoring resources.https://www.ojp.gov/library/publications/considerations-social-media-monitoring-response
- ✓ **Family Tech Planners** - Families can use these tech planners (offered by age groups of 2–8yo, 9–12yo, and 13+) to facilitate conversations about tech use as a family. https://www.commonsensemedia.org/family-tech-planners
- ✓ **Parent Guides** - ConnectSafely provides a collection of parent guidebooks that demystify apps, services, and platforms popular with kids and teens. They also touch on topics including Cyberbullying, Parental Controls, and Teen Sextortion Scams. https://connectsafely.org/parentguides/
- ✓ **Heads Up: Stop. Think. Connect.** - Written for kids, a resource available in twelve languages to help children stand up to cyberbullying, protect their personal information, share with care, and stay safe online. https://consumer.ftc.gov/articles/heads-up
- ✓ **Early Learning and Educational Technology Policy Brief** - This guidance aims to help those who care for children from birth to age eight make wise decisions about media use

and provides four guiding principles for families and early educators on the use of technology with young children.https://tech.ed.gov/earlylearning/

3. DIGITAL CITIZENSHIP

Resources include presentations to educate children on being digital citizens, guides for parents to help their children navigate online space, and specific lessons for youth with intellectual and developmental disabilities to help them identify online risks and develop healthy online relationships.

- ✓ **Parent and Family Digital Learning Guide** - Helpful explanations, guidance, and links to additional resources developed by the Office of Educational Technology at the Department of Education to support parents and caregivers as they and their children navigate online learning and digital learning tools. This guide also addresses challenging questions related to digital learning that can come up for families, such as safety, privacy, and civil rights. Parent and Family Digital Learning Guide - Office of Educational Technology
- ✓ **Digital Citizenship Resources for Family Engagement** - Common Sense Education's Digital Citizenship Resources for Family Engagement include Tips and Activities by age on topics including Privacy and Security; Digital Footprint & Identity; and Cyberbullying, Digital Drama, and Hate Speech. https://www.commonsense.org/education/family-resources
- ✓ **Internet Keep Safe Coalition (iKeepSafe)** - The iKeepSafe mission is to provide a safe digital landscape for children, schools, and families by supporting the protection of student privacy, while advancing learning in a digital culture. https://ikeepsafe.org/resources/
- ✓ **Digital Citizenship for Youth with Intellectual and Developmental Disabilities -** Set of two interactive lessons adapted from Digital Citizenship. The lessons are designed to teach youth with intellectual and developmental disabilities (IDD) to identify online risk and develop healthy online relationships. The lessons are adapted for youth ages 10-21 with mild-to-moderate IDD. https://teenpregnancy.acf.hhs.gov/resources/digital-citizenship-youth-idd

4. BULLYING & CYBERBULLYING

Resources include materials that define these terms and list applicable laws and provide examples of court cases; training modules for teachers; scenarios for teachers on how to handle incidents of cyberbullying; lesson plans for teachers; tips and digital awareness information for families; and guidance to help schools create bullying prevention systems.

- ✓ **StopBullying.gov** - StopBullying.gov provides information from various government agencies on how to respond to and prevent bullying, including cyberbullying and how to promote digital wellbeing. https://www.stopbullying.gov/
- ✓ **Lessons from the Field Webinar Series, Preventing and Intervening in Identity-Based Bullying- National Center on Safe Supportive Learning Environments** - The U.S. Department of Education, Office of Elementary and Secondary Education's Office of Safe and Supportive Schools, and the National Center on Safe Supportive Learning Environments hosted the

Lessons from the Field Webinar on Preventing and Identity-Based Bullying. https://safesupportivelearning.ed.gov/events/webinar/lessons-field-preventing-and-intervening-identity-based-bullying

- ✓ **PACER's National Bullying Prevention Center** - PACER's National Bullying Prevention Center provides resources for students, parents, educators, and others, on topics related to bullying and cyberbullying focused on children and youth with disabilities. Additionally, "What Parents Should Know About Bullying" is that provides parents with information related to school-family partnerships, mobile and online safety, and tips for helping their child if they are a being bullied. https://www.pacer.org/bullying/ ; https://www.pacer.org/bullying/parents/definition-impact-roles.asp

- ✓ **Technology and Youth: Protecting your Child from Electronic Aggression** - **"**Youth can use electronic media to embarrass, harass, or threaten their peers. Increasing numbers of adolescents are becoming victims of this new form of violence—electronic aggression. Research suggests that 9% to 35% of young people report being victims of this type of violence." https://www.cdc.gov/violenceprevention/pdf/EA-TipSheet-a.pdf

- ✓ **Violence Prevention: School-Based Anti-Bullying Interventions** - The Community Preventive Services Task Force recommends school-based anti-bullying interventions to reduce bullying experiences and improve mental health among students. Systematic review of evidence shows that when interventions are implemented in schools, students report fewer episodes of bullying perpetration, fewer episodes of bullying victimization, and fewer mental health symptoms such as anxiety and depression.https://www.thecommunityguide.org/findings/violence-prevention-school-based-anti-bullying-interventions.html

5. CHILD SEXUAL EXPLOITATION AND ABUSE

Resources include how to protect children from online harm; national strategies to combat child sexual exploitation and abuse; videos and activities to teach kids how to be safe online; information about awareness campaigns; and a curriculum to provide youth with information and skills to make safe choices and use support systems.

- ✓ **Know2Protect** - Know2Protect: Together We Can Stop Online Child Exploitation is a national public awareness campaign sponsored by DHS to raise awareness about the rapidly escalating threat of online child sexual exploitation and abuse. Know2Protect will educate kids, parents, trusted adults, policymakers, and the broader public about online threats and empower them to help keep kids safe online; explain how to report online enticement and victimization; and offer response and support resources for victims and survivors of online child sexual exploitation. www.Know2Protect.gov

- ✓ **U.S. Department of Justice, Criminal Division, Child Exploitation and Obscenity Section: Keeping Children Safe Online** - Variety of resources for kids and parents to keep children safe online. https://www.justice.gov/criminal/criminal-ceos/keeping-children-safe-online

- ✓ **Parents, Caregivers, and Teachers: Protecting Your Kids (FBI)** - Multiple resources geared toward protecting children from online harms. https://www.fbi.gov/how-we-can-help-you/

parents-and-caregivers-protecting-your-kids

- ✓ **SchoolSafety.gov Topic Page: Child Exploitation** - Resources on SchoolSafety.gov cover a broad range of school safety topics and threats, including child exploitation. https://www.schoolsafety.gov/child-exploitation
- ✓ **Not a Number** - Not a Number is an interactive child trafficking and exploitation prevention curriculum designed to provide youth with information and skills in a manner that inspires them to make safe choices. https://love146.org/notanumber/#about
- ✓ **Sextortion Victim Resource** - Sextortion-related information and resources from the Internet Crimes Against Children (ICAC) Task Force Program. https://icactaskforce.org/resource/RS00510153
- ✓ **Sextortion resources** - Overview of extortion; questions and answers for kids and caregivers; stories and podcasts; wide array of media. https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/sextortion
- ✓ **TakeItDown** - TakeItDown is a free service that facilitates removal of intimate or explicit images or videos shared online without consent. Service aims to help survivors regain control over their privacy and prevent further harm by facilitating the removal of such content from websites and social media platforms. https://takeitdown.ncmec.org/

6. TEEN DATING VIOLENCE AND OTHER FORMS OF GENDER-BASED VIOLENCE

Resources include information about a national, toll-free telephone, text, and online chat hotline for American Indian/Alaska Native adult and youth victims; the national teen dating violence chat and helpline; the national domestic violence hotline; the national helpline for image-based abuse; and resources for taking down non-consensual intimate images (StopNCII.org) and child sexual abuse material (Take It Down website, https://takeitdown.ncmec.org/).

- ✓ **National Domestic Violence Hotline - Love is Respect** - The National Domestic Violence Love is Respect Hotline is a national resource to disrupt and prevent unhealthy relationships and intimate partner violence by empowering young people through inclusive and equitable education, support, and resources. https://www.loveisrespect.org/
- ✓ **Dating Matters®** - Dating Matters is an evidence-based teen dating violence prevention model developed by the CDC that includes prevention strategies for individuals, peers, families, schools, and neighborhoods. It focuses on teaching 11–14-year-olds healthy relationship skills before they start dating and reducing behaviors that increase the risk for dating violence, like substance abuse and sexual risk-taking. https://www.cdc.gov/violenceprevention/intimatepartnerviolence/datingmatters/index.html
- ✓ **StopNCII (Stop Non-Consensual Intimate Images)** - StopNCII is an online platform that helps individuals protect their privacy by preventing distribution of intimate images shared without consent. It uses technology to detect and remove such content from online platforms. https://stopncii.org/

- ✓ **Image Abuse Helpline and Safety Center** - The Image Abuse Helpline and Safety Center is a dedicated resource providing support and guidance to individuals affected by non-consensual sharing of intimate images. Offers confidential advice, emotional support and practical assistance to help victims navigate the process of removing abusive content online. https://cybercivilrights.org/ccri-safety-center/

- ✓ **The Safety Net Project** - National Network to End Domestic Violence provides resources on the intersection of technology and domestic and sexual violence and works to address how it impacts the safety, privacy, accessibility, and civil rights of victims. https://nnedv.org/content/technology-safety/

- ✓ **StrongHearts Native Helpline** - The StrongHearts Native Helpline 1-844-7NATIVE (762-8483) is in operation 24 hours a day. This national, toll-free telephone, text, and online chat hotline provides information and assistance to adult and youth victims of family violence, domestic violence, or dating violence; family and household members of such victims; and persons affected by the victimization, including provision to support American Indian/Alaska Native communities. https://strongheartshelpline.org/

Appendix E

BEST PRACTICES CONVERSATION CARDS

This section features conversation starter resources developed in collaboration with the Center for Excellence for Social Media and Youth Mental Health for parents and caregivers of children, including resources specifically developed to be used with younger children (2–10 years old) and tweens and adolescents (10–19 years old). These resources, which are available at the Center for Excellence webpage (available at: https://www.aap.org/en/patient-care/media-and-children/center-of-excellence-on-social-media-and-youth-mental-health/) are designed to help children build safe and healthy relationships with online platforms and media and develop their skills for doing so.

Building Healthy Relationships with Media: Essential Skills for Children 10 and Younger

Children build media habits and preferences from a very young age, so it's worthwhile to set them up for a healthy relationship with media before they grow into teens and young adults. The following practical strategies are ways to build balance, critical thinking, self-regulation, and safety skills for toddlers through elementary school-aged children.

This handout was developed in partnership with the Kids Online Health and Safety Task Force, which is co-led by the U.S. Department of Health and Human Services, through the Substance Abuse and Mental Health Services Administration, in close partnership with the U.S. Department of Commerce.

Funding for the Center of Excellence was made possible by Grant No. SM087180 from SAMHSA of the U.S. Department of Health and Human Services (HHS). The contents are those of the author(s) and do not necessarily represent the official views of, nor an endorsement by, SAMHSA/HHS or the U.S. Government.

CENTER OF EXCELLENCE
Social Media and Youth Mental Health
FROM THE AMERICAN ACADEMY OF PEDIATRICS

SAMHSA
Substance Abuse and Mental Health Services Administration

1. Make it a Low-Drama Part of the Family Conversation

Do you ever find yourself arguing with your kids about screen time?
You are not alone! Often, families' discussions about screens feel like a power struggle, full of negotiations and negatives. But they don't have to be.

Screens are all around us, and help us work, laugh, learn, and escape from stress. Therefore, like you talk about food, sleep, school, or any other part of life, it's important to find time to talk about media and technology. It can be anything from the latest movie or video game or something you hear about in the news. The key is to be open-minded, listen to our kids, and guide them without shame and blame. Even young kids can learn from conversations about online safety, how to recognize marketing, and being smart about what videos they watch. Children in elementary school may enjoy sharing their emerging opinions about technology.

Ideas for how to do it:

- ***Be an influencer detective (age 6+):*** If your child likes videos created by influencers, watch along with them and ask: "Why did they say that? Do you think someone paid them to put that in their video? Are they being real, or showing off? Do you think they get more 'likes' or earn more money that way?"
- ***Family movie night (all ages):*** Pick a movie or show to watch together. Have conversations about the characters, what happened, and what you agree with and disagree with.

2. Normalize Having Boundaries

Technology can't take up every minute of our downtime. We need a good night's sleep, time to talk to each other, and time to share food and laughs. Think about the family routines your family loves, whether it's chatting on car rides, family meals, or dancing together, and make time for it. These are the things that we need to ensure tech doesn't crowd out — for kids or parents.

Ideas for how to do it:

- ***No-phone zones (all ages):*** Together with your family, decide on rooms of your home or times of day when you don't want technology to invade, such as at the dinner table, in the car, or before bedtime.
- ***Quiet those devices (all ages):*** Set do not disturb, focus mode, or other settings on devices so that unnecessary notifications don't come through when you want quiet time.
- ***Device free meals (all ages):*** Families who decide there's "no tech at the table" can focus more on each other, having conversations, and enjoying the food they are eating.

Things you can say:

- **Ages 2-3+:**
  - Give a warning to help them transition away from screens, and help them come up with ideas for what to do next. "I'm going to set a timer for five more minutes, and then it will be time to do something else. What ideas do you have for what you want to play – maybe cars, playdoh, or stickers?"
  - "Let's do a challenge where you turn off the iPad/game console/TV by yourself, without me having to remind you. Do you think you can do that?"
  - Help kids plan so that media doesn't take up all of the day: "What's your plan for using the iPad today? " What's your plan for doing other things too?"
  - "I am going to put my phone away for the night so we can have time together."
- **Ages 5+:**
  - "It seems like you're having a hard time putting your device down, let's talk about that."
  - "What makes you want to play that game every day?"

3. Pick Good Content

There is so much content out there for kids! It's your right to be choosy about what your kids watch and learn from. Pick videos, games, and movies with good storytelling and minimal marketing or ads. If you want something educational, go with shows that are proven to help kids learn, like Sesame Street or PBS KIDS. This helps kids understand that their minds can really engage with media — not just zone out.

Ideas for how to do it:

- ***Look it up (all ages):*** **Common Sense Media** rates thousands of movies, shows, apps, games, and books to let you know whether they are worth your child's attention, are too mature, or contain themes you'd rather not introduce yet.
- ***Peek in on what they are watching (all ages):*** Part of monitoring kids' media use is watching along — even for just a few minutes. If you don't like what they are watching, talk about it and find alternatives.

Things you can say:

- **Ages 2-3+:**
  - When you see them watching something new, ask: "What do you like about this? What happens on this show/game?"
  - "Can you show me your favorite channel?"
  - "I'm not crazy about what that character just did. I thought it was rude. What do you think?"

4. Teach Non-Screen Ways to Manage Emotions and Boredom

During the COVID-19 pandemic, we all used media a little more to manage stress and boredom. But those habits don't need to stick around. It's a really important part of mental health to learn how to manage strong emotions and channel boredom into other activities that make us feel human. Many kids need to unwind and burn off a little steam when they come home from school, but make a time limit around technology so that this doesn't take up the whole afternoon. Remember, managing emotions and boredom are skills that don't come easily to all kids, so they need practice and help from caregivers.

Ideas for how to do it/What to say:

- **(Age 2+) Talk about emotions:** "When you feel these big emotions, it's okay. Emotions come and go. Let's stretch our bodies reeeeeaaaaalllly big and take 5 deep slow breaths. When we're done, let's see how we feel."
- **(Age 4+) Help build insight into how technology makes us feel.** "How does your brain and body feel after playing that game?"
- **(All ages) Find alternatives:** "Let's try listening to some calm relaxing music" or "Instead of watching tv to go to bed, we are going to try reading a book. How about you pick out two books for us to read tonight?"
- **(All ages) Recognize when your family is all sitting around looking at your own devices.** "I've noticed that our family has been using our screens to help us calm down. Let's talk about other ways we could calm down when we are stressed out."

5. Build Digital Smarts and Kindness

We all see weird or upsetting stuff online sometimes. Talk about it in a non-judgmental way, so that your child knows it's not their fault and they can come to you to process it. When they do see something upsetting, empower them to pause, think about it, block it, and report it. Kids should know that kindness and respect is the expectation online, and rudeness or violence is not.

Ideas for how to do it/What to say:

- **(Ages 6+):**
  - "I saw something rude in my social media feed today, and it made me upset. Does that ever happen to you?"
  - "Do you ever see other kids being mean online/in your game? Why do you think they do that?"

6. Teach Safety Skills

When kids are young, we talk to them about street safety, swimming safety, and other rules that come with exploring the world.
Safety rules for the digital world should include:

1) privacy about names, addresses, phone numbers, and passwords,
2) not chatting with strangers (who can sometimes pose as kids),
3) not clicking links or downloading things that can carry viruses, and
4) unsafe websites that can show sexy or violent things. Kids can be impulsive and curious, so it's important to teach them these rules ahead of time, before they stumble into trouble. Having kid-safe filters and protections on devices or Wi-Fi also helps.

Ideas for how to do it/What to say:

- **(Ages 3+):**
  - "Just like I teach you how to be safe crossing the street, it's my job to teach you how to be safe when using your tablet."
- **(Ages 5+):**
  - "You wouldn't post your name and address on a billboard, right? That's why we don't share private information on a chat or game that anyone can see."
  - "Computer viruses can make our laptop/tablet crash and not work. That's why I help you decide what websites to visit and games to download."
  - "If people online try to give you things, ask you for pictures or private information, or otherwise are making you feel weird, let me know and I can help you block them."

7. "Sharenting:" Thinking Before You Share

Since the invention of social media, parents have shared billions of photos of their children online — often without kids' permission.
While these photos can share joy, parents say they also can lead to negative social comparisons about picture-perfect parenting. These photos also contain a lot of data about children's faces and locations. Experts recommend asking for your kids' permission before posting photos or stories about them online. This helps teach children about consent and privacy, which may help them be a more responsible social media user as a teen.

Ideas for how to do it/What to say:

- **(Ages 5+):** If your child doesn't like what you've posted, ask them why. Sometimes children are embarrassed or might want more of a say in what pictures you decide to post.
- **(All ages):** If you post pictures of your child(ren) on social media, show them. Younger children may not understand who else can see these posts, so you might need to explain it, like "My account is public, so anyone can see this." or "I only share pictures with my good friends and people like grandma."

Suggested Activities

Print and try some of these fun skill-building activities with your kids!

Setting Up for Us Time

Family Movie Night

Technology That's Hard to Put Down

YouTube Together Time

CENTER OF EXCELLENCE
Social Media and Youth Mental Health
FROM THE AMERICAN ACADEMY OF PEDIATRICS

SAMHSA
Substance Abuse and Mental Health Services Administration

Suggested Activities

Print and try some of these fun skill-building activities with your kids!

Family Movie Night

Plan a family movie night. You can have your child pick something or watch something you loved from your childhood. Or, if your child likes to watch a streaming series, ask to join them for an episode or two. Resist picking up your phone! Ask your child 1) what they like about the movie/show and characters. 2) What they think is going to happen next in the plot. 3) How does the movie/show make them feel (happy/sad/excited/nervous/etc.)

Setting Up for Us Time

Set up device free dinners or device free zones and designate a basket or box where devices go to be quiet for a while. If you feel like being crafty, make the bag or box and have your child help make or decorate it. When your devices are in there, communicate that you are doing this so you can focus just on them and the things you want to do or play together.

YouTube Together Time

Watch a YouTube video together (can be anything you find appropriate or perhaps your child's favorite channel). Talk about the ads that pop up and what they mean. Talk about the recommended videos that show up, encourage appropriate choices, and see what your child wants to click on. Talk to them about what you think is appropriate video content, and what is not.

Technology That's Hard to Put Down

Take turns looking at your 'screen time' output and talk about what you usually do on your device and whether it brings you joy or stress. Ask kids which apps and games are hardest to put down, and which ones let them have boundaries or allow them to feel like they are easily in control.

Suggested Activities

How We Manage Emotions

Our Non-Tech Favorites

How Technology Makes Us Feel

Choosing the Good Stuff

Suggested Activities

Our Non-Tech Favorites

Pick a board game you want to play, song you want to dance to, art activity that makes you feel good, outdoor place you want to visit, or pet you want to snuggle. Each family's non-tech favorites are different, so find a few that work for you and make them a regular routine. Write them down here:

How We Manage Emotions

What's your family's emotion coping plan? How do you each like to deal with stress or upsetting feelings? Find healthy ways to cope that feel right for your family, like movement (stretching, taking a walk), using your senses (music, hugging, stress putty), deep breathing, or talking about your feelings without yelling. Write down your coping plan here:

Choosing the Good Stuff

Talk with your child about what type of channels/shows they watch or what digital games they play. Play a quiz game where you rate each video or game on a scale of 1 to 5 on qualities like:

- I use my brain when I watch this (vs. My brain turns off when I watch this)
- The people are kind (vs. The people are rude)
- I feel good about myself when I watch this (vs. I feel worse about myself when I watch this)
- This feels like our family (vs. This feels unrealistic)

How Technology Makes Us Feel

Both parents and kids, think about what apps or games you use the most. How do they make you feel during and after using them? Good? Cranky? Riled up? Worried? Maybe take a break from the ones that don't make you feel good.

Suggested Activities

Scam Finder

Digital Disengage Challenge

Pop-up Ad Whackamole

Weird or Creepy Content

Suggested Activities

Digital Disengage Challenge

This is a family challenge to put your devices down! It's hard to pull your attention away, but make a plan to turn it off, hand over the device, or put it away when it's time to do something else. Count up points when family members can put their device down the first time someone asks them. The person with the most self-control points at the end of the week wins!

Scam Finder

Talk about the types of scams you've seen lately. Spam phone calls? Too-good-to-be-true advertisements? An influencer saying something outlandish? This helps your child build a critical eye.

Weird or Creepy Content

Ask your child to tell you about the weirdest or creepiest thing that they've seen online lately. Don't overreact! Help them understand what it was, why it showed up, and how to avoid it next time.

Pop-up Ad Whackamole

If your child is watching videos or playing a mobile game, teach them to close, "X" or "skip" the ad, and to let you know when they did it! Have them help you figure out which apps or games have the most annoying pop-ups, uninstall them, and find fun alternatives.

Suggested Activities

To Post or Not to Post

Private vs. Shareable

Offline Family Photo Album

Chat Etiquette

Suggested Activities

Private vs. Shareable

Quiz your child on what is private versus what is OK to be shared. Their last name? Address? School name? Phone number? Home town? Password? All private! Their high score? Favorite game? OK to share!

To Post or Not to Post

Do you regularly post photos of your children? If so, sit down with them on the couch and go through your social media feed with them. Ask them to rate your posts — from recent to when they were just babies — with one of three responses:

- I love that you shared it!
- Meh, don't really care.
- I kinda wish you hadn't....

You don't need to necessarily take photos down but listen to your kids with an open mind about why they wish those photos stayed on your phone, and not on the internet.

Chat Etiquette

If your child uses a video game or video platform that allows chatting and comments, have them show you what it looks like. Look at the chat together and talk about: who is being respectful and positive? Who isn't? How do they know that other players are really kids? Help them restrict their chat to "friends" online, or try turning off the chat for a week or 2 — some kids don't miss it.

Offline Family Photo Album

Instead of posting photos online, select a few that are special to your family to print out and put in an album in your home. Have your children help pick out the ones that give them the best memories and help arrange their order in the album. Keep the album in an easy-to-reach place so that kids can look through it during downtime (rather than grabbing a device!).

Conversation Starters for Families of Tweens and Teens

Having conversations with tweens and teens about technology and digital media can be challenging. For busy families, it can feel hard to find the right moment, or to say the right things. This resource provides ideas and examples that you, as parents and guardians, can use to frame conversations with your tweens and teens around common scenarios involving technology, social media, and video games. It is intended for use with tweens and teens who already are engaged with technology and digital media.

Below are questions and prompts that you can use with your child to get their input, make decisions together, and have conversations rather than lectures. It's normal for parents to feel stressed during these conversations, so it is ok to pause or take some breaths if you need to, and remember not to jump in and try to control things. Having conversations "early and often" is preferable to planning and structuring one long talk. While there is no perfect time to have these discussions the table below gives some ideas for timing to consider and timing to avoid.

Potential times for conversations	Times to avoid these conversations
• When driving your child to or from activities and you have some alone time with them in the car • During a family dinner so other family members can be part of the discussion • During downtime at home • After your child shared something that happened at school or with peers related to these topics	• When there is a tight timeline or limited time for the conversations (e.g. When you have 10 minutes before the dentist appointment starts) • During or just after a conflict related to technology and digital media • When your child's friends are around

CENTER OF EXCELLENCE Social Media and Youth Mental Health
FROM THE AMERICAN ACADEMY OF PEDIATRICS

SAMHSA
Substance Abuse and Mental Health Services Administration

Setting initial boundaries around technology and digital media use

"I'd like us to talk about our family's approach for setting some boundaries around technology and media use. I was thinking that this is something we could work on together as I'd like to include your input in these decisions."

Possible Follow-Up Prompts

"Are there times of the day that you think we should not use devices or phones? One example may be during family dinner."

"Are there times that are important to you for *me* to be present and not on a device or phone?"

"Digital media is fun and a learning opportunity, but it can also be a lot to handle. You and I are both learning about this together. I want you to know I'm here to help you through any situation that may come up. I'd like to keep an eye on a few things for now, like your sleep and whether you are seeing things or having experiences that stress you out."

"I'd like for us to talk about your device and internet use regularly; that way we can check in with each other and see how it's working for you and for us. I'm thinking for now let's touch base every other month or so, what do you think? When would be a good time to check in?"

"Since a lot of the time when you're on your phone, you're doing it by yourself, I'll be checking in with you about how it's going. It's important for you to feel comfortable talking to me in honest ways about this."

"I'd like to be sure that any discussions we have about rules or guidelines also apply to me and my own tech use. We can use the Family Media Plan tool from the AAP to get some ideas for approaches and guidelines for both/all of us. Let's take a look and see if it is helpful to us."

Initial check-ins after setting guidelines and boundaries

"It's been about a month since we set our guidelines around technology and digital media. I wanted to check in on how things are going."

Possible Follow-Up Prompts

"What's working well?"

"What is not going as well as you hoped?"

"What could I be doing better in role modeling technology use?"

"Let's take a look at the guidelines we set up in the Family Media Plan, and we can discuss if anything needs to be changed at this point. You can also give me feedback on how I'm doing with these rules."

Social media specific check-ins

"I know that social media is important to you. I wanted to check in about it; how do you think things are going with your social media use?"

Possible Follow-Up Prompts

"What are some of the things you've enjoyed about having this social media account? What are the downsides? Is there anything you want to change? Why?"

"I don't know much about this social media platform. Can you show me a little bit about how it works, or what you like to look at on this one?"

"I understand that what you follow has a big impact on what you see when you are on that app. How do you decide who or what to follow on your profile? Do you ever think about unfollowing accounts when you don't like the content they show you? Why or why not?"

"Have you noticed whether you feel drawn to using social media during the day or at night? Anything stand out to you?"

"Have you noticed times when it's harder to get off social media. Why do you think so? What helps you get off it?"

"What's something that's surprised you about using social media so far? Was it good or bad? How about something you expected to experience — has it been what you thought it would be? Why?"

"Have you experienced any unexpected or unpleasant situations since you've gotten your account? What was that like for you?"

"It sounds like you made a great decision with how to handle that. Did anything surprise you about what happened? Would you do something similar if this happens again? Or, would you do something different?"

Checking in on unwanted contact

"One aspect of social media use that is really important is protecting our privacy. Have you looked at the privacy settings on all of your accounts? How are things going with those settings? "

Possible Follow-Up Prompts

"Have people tried to contact you who you didn't know?"

"Do you know how to block someone online if they contact you or make you feel uncomfortable? Can we look together and figure out how?"

"It is unfortunately common that people online can pretend to be people they are not. This happens online and on social media or gaming platforms. Sometimes adults pretend to be teens to try to get something from them, like a sexy picture. I want you to know if anything like that ever happened to you, I would want to support you. I would be there to help you figure out a solution. I want you to be really careful with your privacy and who you share information with, but most importantly I want you to know we are here to support you no matter how bad a situation may be. "

"I am guessing that you probably know about this, but there are some people who use online platforms to bully or harass others. Has anything like that ever happened to you? How did you handle it? How can I support you?"

Checking in on unwanted content

"As you probably know, your social media platforms track your search and viewing patterns. They try to get to know you, and an algorithm (a set of rules that rank content across the platform) decides what to put in your feed. How is the algorithm working for you at this point? Is there content you don't want to see? Can we look at ways to reset your algorithm?"

Possible Follow-Up Prompts

"It's really normal to see some content that is creepy, upsetting, or that you don't want to see online, or via social media or gaming. Have you had any of these experiences that you are comfortable sharing? In thinking back on these situations, are there ways that you handled them that you feel good about? Things you would do differently? How can I support you?"

Struggles with meeting family expectations around digital media use

"I feel like it's a good time for us to check in on how our family media expectations are going. How are we all doing with using our devices? I've noticed a few times that I've needed to remind you about our agreement to not have devices at the dinner table so we can spend time together *(or other area that is a struggle)*. What ideas do you have to make that rule work better for you? What would work about that plan and what wouldn't?"

Possible Follow-Up Prompts

"What is that like for you?"

"How am I doing with role-modeling that boundary?"

"How do you feel like you're doing role-modeling for your siblings?"

"How can we support you following that rule?"

"What should our next steps be?"

Tween/teen gaming too much

"Let's talk about gaming. I'd like to share a few things I've noticed about your gaming behaviors, and then hear from you. My goal is for us to get on the same page about this."

Possible Follow-Up Prompts

"You seem to get upset when I try to get you to stop playing video games and [come to dinner/go to bed/do homework/do chores/etc]. What's going on in those moments for you?"

"What sort of things make it hard to stop gaming?" — *explore wanting to be on at the same time as friends, designs of games, wanting to de-stress, avoidance of homework or family chores.*

"It sometimes feels like gaming is a distraction from some things stressing you out at school. That makes sense. I also sometimes find after a hard day at work that scrolling on my phone can feel good in the moment/distract me from work I have to do/etc. While gaming sometimes is one way to help, as your parent, I want to help you figure out other ways you can deal with stress or relax. Let's see if, together, we can come up with any ideas."

Media and technology interfering with sleep

"Sleep is really important for everyone. I know you aren't able to show up to [x] activity/have the energy to do all the things you want to do/etc. when you don't get enough sleep. Let's talk about some ideas for how to help you get better sleep."

Possible Follow-Up Prompts

"I've heard you say you're feeling really tired this week. How is it going with putting your phone away at [x] time?"

"Let's come up with a plan that would help you feel more rested."

"What about keeping your phone away from your bed since it can interfere with sleeping? What other ideas do you have to calm down before you go to sleep?"

"I know that you use a calming app to go to sleep at night, so your phone is near where you sleep. Can we look at some settings to make sure your phone doesn't send notifications that wake you up?"

"What makes your phone so easy to use at night? What makes it hard to put down?"

Overheard conversation about social media

"When I was driving you and your friends today, I heard you talk about something you saw on social media last week. I'm interested in what's going on for you, so I'd like to hear a little more from you about what happened."

Possible Follow-Up Prompts

"How did you feel about that?"

"What are ways that this happening on social media helped or hurt this situation compared to if it happened offline?"

"Who can you talk to when things like that happen?"

"Are there ways I could have supported you better during that situation?"

Prompts to encourage reflection around relationships with media

"Do you feel like people are being real on social media? How can you tell if they are being authentic?"

"When you left your phone at home by accident the other day, how did that feel? Why?"

"How do you wish [your phone/favorite social media platform] was designed better? What would you change?

"What does it feel like when you've lost track of time in your phone, versus [other favorite activities like a book, doing art work, playing basketball]?"

"What do you think [platform] knows about you? How do you feel about that?"

"Have you ever given attention to how you feel immediately after using your favorite social media app for a while? If you aren't sure, try to check in next time right after — do you feel good or bad? Why do you think so?"

Reflecting on other peoples' tech use

"I know that you've seen classmates spend time on their phones, what do you think is good about it? What is annoying? Why?"

"When you're hanging out with friends, and they are all on their phones and not paying attention to each other, how does that feel?"

"When you're on [platform], how do you know who is nice and who's not? How do you decide who to block, or who is a grown up or a teen?"

"Have you noticed any of your friends change as a result of spending a lot of time on their phones? How do they change?

"What's the cringiest thing you have seen other kids do online? How did you feel about it?"

"What's the most hilarious thing you've seen other kids do online?"

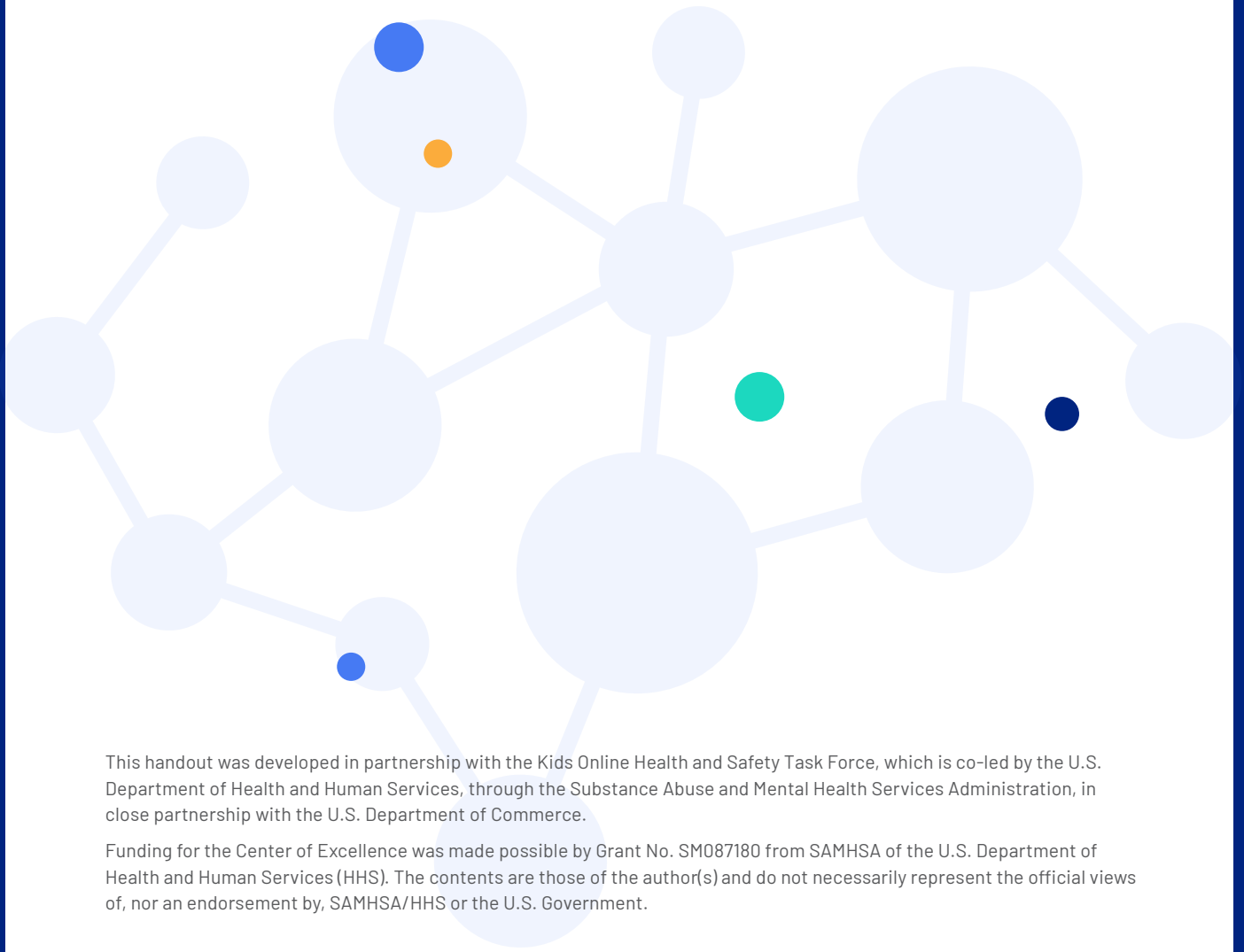
"When you're trying to talk to someone, and they're looking at their phone, how does that feel?"

Parents talking about their own media use

"I'm feeling overwhelmed with all the technology in our day. Can we think about ways to put it down and spend quality time together?"

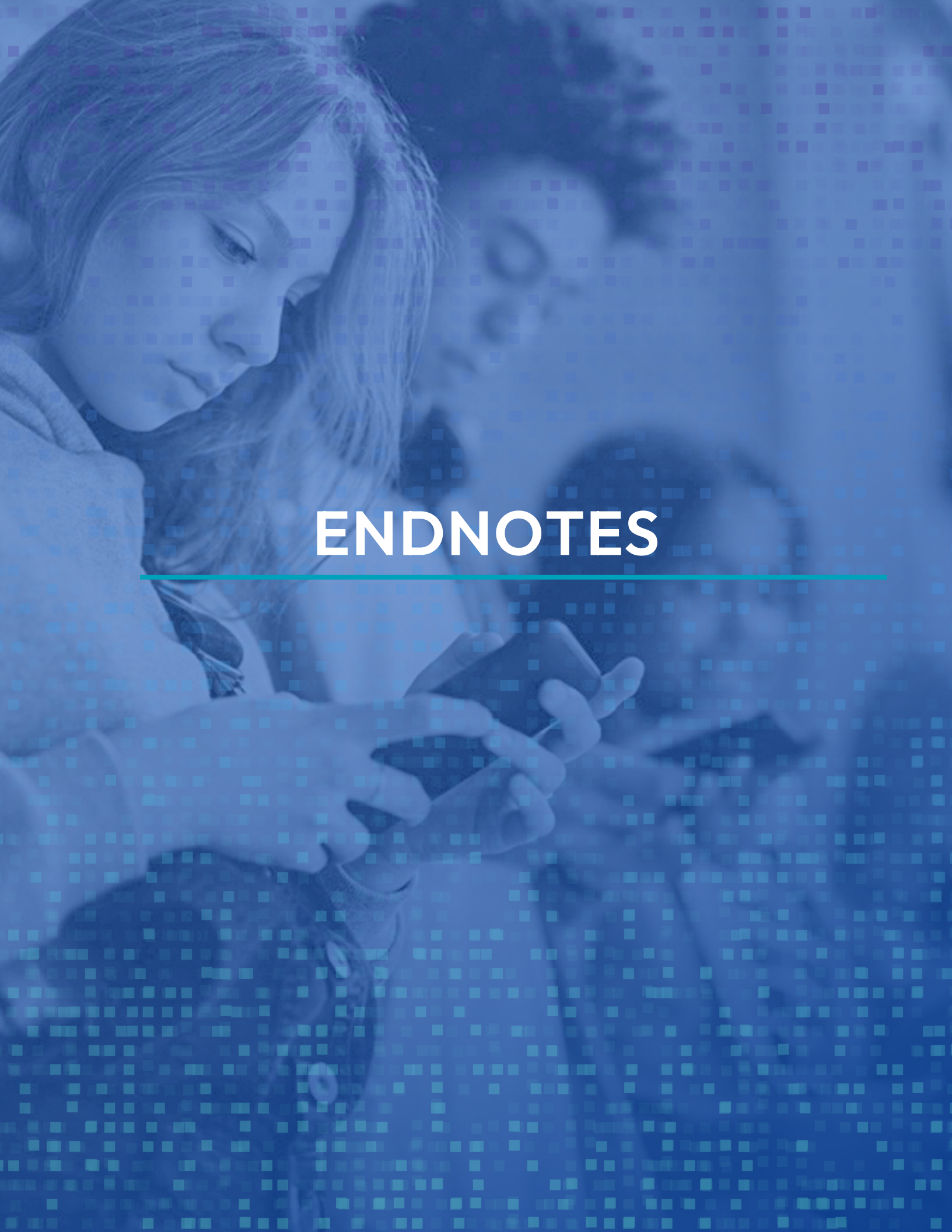
"I sometimes have a hard time not checking my phone or feeling the need to respond to texts or emails. I'm working on how to be better about my own boundaries. Let's help each other find a good balance."

"What do you think of my phone use habits? What could I do better?"



This handout was developed in partnership with the Kids Online Health and Safety Task Force, which is co-led by the U.S. Department of Health and Human Services, through the Substance Abuse and Mental Health Services Administration, in close partnership with the U.S. Department of Commerce.

Funding for the Center of Excellence was made possible by Grant No. SM087180 from SAMHSA of the U.S. Department of Health and Human Services (HHS). The contents are those of the author(s) and do not necessarily represent the official views of, nor an endorsement by, SAMHSA/HHS or the U.S. Government.



ENDNOTES

Endnotes

1 C. Carr, and R. Hayes, "Social Media: Defining, Developing, and Divining." *Atlantic Journal of Communication*, (2015): 23:1, 46-65. https://doi.org/10.1080/15456870.2015.972282.

2 See also Harvard Medical School and Boston Children's Hospital that estimated youth use based on market research data and public sources: A. Raffoul, Z. Ward, M. Santoso, J. Kavanaugh, and S. Austin, "Social media platforms generate billions of dollars in revenue from U.S. youth: Findings from a simulated revenue model." (2023): PLoS ONE 18(12): e0295337. https://doi.org/10.1371/journal.pone.0295337.

3 Office of the Surgeon General (OSG). *Social Media and Youth Mental Health: The U.S. Surgeon General's Advisory*. (2023)

4 Office of the Surgeon General (OSG). *Protecting Youth Mental Health: The U.S. Surgeon General's Advisory.* (2021)

5 A. Giovanelli, E. Ozer, and R. Dahl, "Leveraging technology to improve health in adolescence: A developmental science perspective," *Journal of Adolescent Health*, (2023): 67(2).

6 J. Nesi, S. Choukas-Bradley, and M. Prinstein, "Transformation of adolescent peer relations in the social media context: Part 1—A theoretical framework and application to dyadic peer relationships." *Clinical Child and Family Psychology Review* (2018): 21, 267-294.

7 M. Álvarez-Jiménez, J. Gleeson, S. Rice, C. Gonzalez-Blanch, and S. Bendall, "Online peer-to-peer support in youth mental health: seizing the opportunity." *Epidemiology and Psychiatric Sciences* (2016): 25(2), 123-126.

8 F. Angelini, C. Marino, and G. Gini, "Friendship quality in adolescence: the role of social media features, online social support and e-motions." *Current Psychology* (2023): 42(30), 26016-26032.

9 J. Nagata, H. Abdel Magid, and K. Gabriel, "Screen Time for children and adolescents during the coronavirus disease 2019 pandemic." *Obesity* (2020): 28(9), 1582–1583. https://doi.org/10.1002/oby.22917.

10 J. Naslund, K. Aschbrenner, L. Marsch, and S. Bartels, "The future of mental health care: peer-to-peer support and social media." *Epidemiology and Psychiatric Sciences*, (2016): 25(2), 113-122.

11 J. Nesi, T. Burke, A. Bettis, A. Kudinova, E. Thompson, H. MacPherson, and R. Liu, "Social media use and self-injurious thoughts and behaviors: A systematic review and meta-analysis." *Clinical Psychology Review* (2021): 87, 102038.

12 K. Riehm, K. Feder, K. Tormohlen, R. Crum, A. Young, K. Green, and R. Mojtabai, "Associations between time spent using social media and internalizing and externalizing problems among US youth." *JAMA Psychiatry* (2019): 76(12), 1266-1273.

13 J. Twenge, T. Joiner, M. Rogers, and G. Martin, "Increases in depressive symptoms, suicide-related outcomes, and suicide rates among US adolescents after 2010 and links to increased new media screen time." *Clinical Psychological Science* (2018): 6(1), 3-17.

14 M. Gámez-Guadix, E. Mateos-Pérez, S. Wachs, M. Wright, J. Martínez, and D. Íncera, "Assessing image-based sexual abuse: Measurement, prevalence, and temporal stability of sextortion and nonconsensual sexting ("revenge porn") among adolescents. *Journal of Adolescence* (2022): 94(5), 789-799.

15 B. Sciacca, A. Mazzone, M. Loftsson, J. O'Higgins Norman, and M. Foody, "Nonconsensual dissemination of sexual images among adolescents: associations with depression and self-esteem." Journal of Interpersonal Violence, (2023): 38(15-16), 9438-9464.

16 E. Vogels, Pew Research Center, "Teens and Cyberbullying 2022" (December 2022): https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/.

17 K. Greškovičová et al. "Superlatives, clickbaits, appeals to authority, poor grammar, or boldface: Is editorial style related to the credibility of online health messages?" *Front. Psychol.*, (August 2022): *Sec. Health Psychology* Volume 13 - 2022 | https://doi.org/10.3389/fpsyg.2022.940903.

18 The White House "FACT SHEET: Biden-Harris Administration Announces Actions to Protect Youth Mental Health, Safety & Privacy" (May 23, 2023).

19 The White House "Readout of White House Listening Session on Tech Platform Accountability" (Sept. 08, 2022): https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/08/readout-of-white-house-listening-session-on-tech-platform-accountability/.

20 Office of the Surgeon General (OSG). "Social Media and Youth Mental Health: The U.S. Surgeon General's Advisory." (2023)

21 White House Task Force to Address Online Harassment and Abuse, "Final Report and Blueprint" (May 2024): https://www.whitehouse.gov/wp-content/uploads/2024/05/White-House-Task-Force-to-Address-Online-Harassment-and-Abuse_FINAL.pdf.

22 Congressional Research Service "Defining and Regulating Online Platforms" (Aug. 25, 2023): https://crsreports.congress.gov/product/pdf/R/R47662.

23 OECD "An Introduction to Online Platforms and Their Role in the Digital Transformation" (2019): https://read.oecd-ilibrary.org/science-and-technology/an-introduction-to-online-platforms-and-their-role-in-the-digital-transformation_19e6a0f0-en#page1.

24 Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505 Children's Privacy.

25 California regulations protecting data about minors under the age of 16, ARTICLE 6. https://cppa.ca.gov/regulations/pdf/cppa_regs.pdf

26 National Academies of Sciences, Engineering, and Medicine "Social media and adolescent health." *The National Academies Press*. (2023): https://doi.org/10.17226/27396.

27 Cingel et al, "Social media and adolescent health, at 97" *National Academies of Sciences, Engineering, and Medicine* (2022).

28 K. Regehr, C. Shaughnessy, M. Zhao, N. Shaughnessy, UCL IOE, "SAFER SCROLLING How algorithms popularise and gamify online hate and misogyny for young people," *University of Kent* (Feb 2, 2024).

29 R. van den Eijnden et al., "Social Media Use and Adolescents' Sleep: A Longitudinal Study on the Protective Role of Parental Rules Regarding Internet Use before Sleep." I*nt J Environ Res Public Health*. 2021 Feb; 18(3): 1346. https://www.mdpi.com/1660-4601/18/3/1346.

30 D. Yu et al., "The Impact of Social Media Use on Sleep and Mental Health in Youth: a Scoping Review." *Curr Psychiatry Rep*. 2024; 26(3): 104–119.

31 A. Khan et al., "Intense and problematic social media use and sleep difficulties of adolescents in 40 countries." *Journal of Adolescence* (preprint). (2024)

32 Social Media and Adolescent Health, "Comm. on the Impact of Social Media on Adol. Health" *Board on Pop. Health and Public Health Prac.; Health and Med. Div*.

33 A. Orben, and A. Przybylski, "The association between adolescent well-being and digital technology use," *Nature Human Behaviour* (February 2019): 177-178, https://doi.org/10.1038/s41562-018-0506-1.

34 P. Valkenburg, A. Meier, and I. Beyens, "Social media use and its impact on adolescent mental health: An umbrella review of the evidence." *Curr Opin Psychol.* (2022): 44:58-68. doi: 10.1016/j.copsyc.2021.08.017. Epub 2021 Aug 18. PMID: 34563980.

35 H. Shannon, K. Bush, P. Villeneuve, K. Hellemans, and S. Guimond, "Problematic Social Media Use in Adolescents and Young Adults: Systematic Review and Meta-analysis." *JMIR Ment Health*. (2022): 9(4):e33450. doi: 10.2196/33450. PMID: 35436240; PMCID: PMC9052033.

36 Office of the Surgeon General (OSG). "Social Media and Youth Mental Health: The U.S. Surgeon General's Advisory. Washington (DC): US Department of Health and Human Services" (2023): https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf.

37 Office of the Surgeon General (OSG). "Social Media and Youth Mental Health: The U.S. Surgeon General's Advisory. Washington (DC): US Department of Health and Human Services" (2023): https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf.

38 V. Murthy, Surgeon General, "Why I'm Calling for a Warning Label on Social Media," *New York Times*.

39 S. Prasad, S. Souabni, G. Anugwom, K. Aneni, A. Anand, A. Urhi, and F. Oladunjoye, "Anxiety and depression amongst youth as adverse effects of using social media: A Review." *Annals of Medicine and Surgery*, (2023): 85(8), 3974-3981.

40 B. Keles, N. McCrae, and A. Grealish, "A systematic review: the influence of social media on depression, anxiety and psychological distress in adolescents." *International journal of adolescence and youth*, (2020): 25(1), 79-93.

41 M. Selfhout, S. Branje, M. Delsing, T. ter Bogt, and W. Meeus, "Different types of Internet use, depression, and social anxiety: The role of perceived friendship quality," *Journal of Adolescence*, (2009): 32(4), 819-833.

42 J. Nesi, and M. J. Prinstein, "Using social media for social comparison and feedback-seeking: Gender and popularity moderate associations with depressive symptoms." *Journal of Abnormal Child Psychology*, (2015): 43, 1427-1438.

43 E. Swedo, J. Beauregard, S. de Fijter, L. Werhan, K. Norris, M. Montgomery, and S. Sumner, "Associations between social media and suicidal behaviors during a youth suicide cluster in Ohio," *Journal of Adolescent Health*, (2021): 68(2), 308-316.

44 N. Macrynikola, E. Auad, J. Menjivar, and R. Miranda, "Does social media use confer suicide risk? A systematic review of the evidence," *Computers in Human Behavior Reports*, (2021): 3, 100094.

45 J. Nesi, E. Telzer, and M. Prinstein, "Adolescent Development in the Digital Media Context," *Psychological Inquiry* (2020): 31, no. 3, 230, https://doi.org/10.1080/1047840x.2020.1820219.

46 E. Galinsky, "The Breakthrough Years," *Flatiron Books*, (2024)

47 G. Wells, J. Horwitz, and D. Seetharaman, "Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show," *The Wall Street Journal,* (Sep. 14, 2022), https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739.

48 D. Elkind, and R. Bowen, "Imaginary Audience Behavior in Children and Adolescents," *Developmental Psychology* (1979): 15, no. 1, 38-44, https://doi.org/10.1037/0012-1649.15.1.38.

49 J. Nesi, Eva H. Telzer, and Mitchell J. Prinstein, "Adolescent Development in the Digital Media Context," *Psychological Inquiry,* (2020): 31, no. 3, 230, https://doi.org/10.1080/1047840x.2020.1820219.

50 E. Vogels, R. Gelles-Watnick, and N. Massarat, "Teens, Social Media and Technology 2022," *Pew Research Center*, (August 10, 2022), https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-tech-

nology-2022/.

51 C. Bryan, D. Yeager, and C. Hinojosa, "A values-alignment intervention protects adolescents from the effects of food marketing," *Nature Human Behaviour,* (2019): 3 no. 6, 596-603, https://doi.org/10.1038/s41562-019-0586-6.

52 N. Vijayakumar et al., "Getting to know me better: An fMRI study of intimate and superficial self-disclosure to friends during adolescence," *Journal of Personality and Social Psychology, (2020):* 118, no. 5, 885–899, https://doi.org/10.1037/pspa0000182.

53 N. Vijayakumar, and J. Pfeifer, "Self-disclosure during adolescence: Exploring the means, targets, and types of personal exchanges," *Current Opinions Psychology* (2020): 31, 135-140, https://doi.org/10.1016/j.copsyc.2019.08.005.

54 A. Marwick, and D. Boyd, "I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience." *New Media & Society*, (2011): 13(1), 114-133.

55 N. Lapidot-Lefler, and A. Barak, "Effects of anonymity, invisibility, and lack of eye-contact on toxic online disinhibition." *Comput. Hum. Behav*. (2012): 28, 434-443.

56 D. Yeager, R. Dahl, and C. Dweck, "Why interventions to influence adolescent behavior often fail but could succeed," *Perspectives on Psychological Science : a Journal of the Association for Psychological Science,* no. 1 (2018): 13, 101-122, https://doi.org/ 10.1177/1745691617722620.

57 L. Sherman, A. Payton, L. Hernandez, P. Greenfield, and M. Dapretto, "The power of the like in adolescence: Effects of peer influence on neural and behavioral responses to social media," *Psychological science*, 27(7), 1027-1035.

58 H. Lee, J. Jamieson, H. Reis, C. Beevers, R. Josephs, M. Mullarkey, and D. Yeager, "Getting fewer "likes" than others on social media elicits emotional distress among victimized adolescents," *Child Development*, (2020): 91(6), 2141-2159.

59 M. Prinstein, J. Nesi, and E. Telzer, "Commentary: An updated agenda for the study of digital media use and adolescent development - future directions following Odgers & Jensen (2020)," *Journal of Child Psychology and Psychiatry, and Allied Disciplines* 61, no. 3 (2020): 350, https://doi.org/10.1111/jcpp.13219.

60 C. Hoffmann, and C. Lutz, "Spiral of silence 2.0: Political self-censorship among young Facebook users," *In Proceedings of the 8th international conference on social media & society* (July, 2017): 1-12.

61 D. Patton, "There Is One Major Element Missing From the Debate on Kids and Social Media," *Newsweek*, (Apr 30, 2024).

62 S. Moskalenko, J. González, N. Kates, and J. Morton, "Incel Ideology, Radicalization and Mental Health: A Survey Study," *The Journal of Intelligence Conflict and Warfare*. 4, (2022): 1-29. 10.21810/jicw.v4i3.3817.

63 J. Rothwell, "Teens Spend Average of 4.8 Hours on Social Media Per Day," *Gallup* (Oct. 13, 2023): https://news.gallup.com/poll/512576/teens-spend-average-hours-social-media-per-day.aspx.

64 J. Rothwell, "Teens Spend Average of 4.8 Hours on Social Media Per Day," *Gallup* (Oct. 13, 2023): https://news.gallup.com/poll/512576/teens-spend-average-hours-social-media-per-day.aspx.

65 J. Rothwell, "How Parenting and Self-Control Mediate the Link between Social Media Use and Youth Mental Health," Institute for Family Studies (Oct. 11, 2023) https://ifstudies.org/ifs-admin/resources/briefs/ifs-gallup-parentingsocialmediascreentime-october2023-1.pdf.

66 Y. Kelly, A. Zilanawala, C. Booker, and A. Sacker, "Social Media Use and Adolescent Mental Health: Findings From the UK Millennium Cohort Study," *EClinicalMedicine,* 6 (2018) 59–68, https://doi.org/10.1016/j.eclinm.2018.12.005

67 H. Shannon, K. Bush, P. Villeneuve, K. Hellemans, S. Guimond, "Problematic Social Media Use in Adolescents and Young Adults: Systematic Review and Meta-analysis," *JMIR Ment Health* (2022): 9(4):e33450.

68 "Attention Deficit Hyperactivity Disorder-Symptoms, Social Media Use Intensity, and Social Media Use Problems in Adolescents: Investigating Directionality," *Child Dev*. Vol. https://doi.org/10.1111/cdev.13334.

69 V. Franchina, M. Abeele, A. Van Rooij, G. Coco, and L. De Marez, "Fear of Missing Out as a Predictor of Problematic Social Media Use and Phubbing Behavior among Flemish Adolescents," *International Journal of Environmental Research and Public Health,* 15, (2018): no. 10: 2319. https://doi.org/10.3390/ijerph15102319.

70 E. Telzer, D. Goldenberg, A. Fuligni, M. Lieberman, and A. Gálvan, "Sleep variability in adolescence is associated with altered brain development." *Developmental Cognitive Neuroscience*, 14, (2015): 16–22. https://doi.org/10.1016/j.dcn.2015.05.007.

71 T. Shochat, M. Cohen-Zion, and O. Tzischinsky, "Functional consequences of inadequate sleep in adolescents: A systematic review." *Sleep Medicine Reviews*, 18(1), (2014): 75–87. https://doi.org/10.1016/j.smrv.2013.03.005.

72 R. Liu, S. Steele, J. Hamilton, Q. Do, K. Furbish, T. Burke, A. Martinez, and N. Gerlus, "Sleep and suicide: A systematic review and meta-analysis of longitudinal studies," *Clinical Psychology Review*, 81, (2020): 101895. https://doi.org/10.1016/j.cpr.2020.101895.

73 V. Rideout, VJR Consulting, M. Robb, Common Sense, " SOCIAL MEDIA, SOCIAL LIFE: Teens Reveal Their Experiences," *Common Sense* (2018): https://www.commonsensemedia.org/sites/default/files/research/report/2018-social-media-social-life-executive-summary-web.pdf.

74 APA, "Health advisory on social media use in adolescence," *APA*, (May, 2023): https://www.apa.org/topics/social-media-internet/health-advisory-adolescent-social-media-use.

75 "Petition for Rulemaking to Prohibit the Use on Children of Design Features that Maximize for Engagement" (Fairplay/CDD Petition), 67 (Nov. 17, 2022): https://www.regulations.gov/document/FTC-2022-0073-0002.

76 FTC Workshop https://www.ftc.gov/news-events/events/2021/04/bringing-dark-patterns-light-ftc-workshop.

77 FTC Report https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf.

78 FTC Bureau of Consumer Protection, Staff Report, "Bringing Dark Patterns to Light", (September 2022): https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf

79 Ofcom, "Understanding Pathways to Online Violent Content Among Children," (2024): https://www.ofcom.org.uk/__data/assets/pdf_file/0026/280655/Understanding-Pathways-to-Online-Violent-Content-Among-Children.pdf.

80 Pew Research Center, "Teens and Cyberbullying 2022" (December, 2022): https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/.

81 H. Clayton, G. Kilmer, S. DeGue, L. Estefan, V. Le, N. Suarez, B. Lyons, and J. Thornton, "Dating Violence, Sexual Violence, and Bullying Victimization among High School Students – Youth Risk Behavior Survey," *United States*, (2021): MMWR supp. 2023:72(1).

82 Emily A. Vogels, Pew Research Center, December 2022, "Teens and Cyberbullying," (2022): https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/.

83 S. Galea et al., "Social Media and Adolescent Health (Comm. on the Impact of Social Media on Adol. Health," *Board on Pop. Health and Public Health Prac.; Health and Med. Div.; Nat'l Acad. of Sci., Eng'g, and Med.)*.

84 See also Comment of #ShePersisted on NTIA KOHS RFC at 4 (noting intersectional impact-based research indicating LGBTQIA users and users of color may face greater cyberbullying, for example); and Combined Comment of Common Sense Media, Center for Digital Democracy, Fairplay on NTIA KOHS RFC at 6-9.

85 Ruderman Family Foundation, "The Ruderman White Paper on Social Media, Cyberbullying, and Mental Health: A Comparison of Adolescents With and Without Disabilities." https://rudermanfoundation.org/white_papers/ruderman-white-paper-reveals-students-with-disabilities-are-almost-twice-as-likely-to-be-victims-of-cyberbullying /.

86 Ruderman Family Foundation, "The Ruderman White Paper on Social Media, Cyberbullying, and Mental Health: A Comparison of Adolescents With and Without Disabilities," https://rudermanfoundation.org/white_papers/ruderman-white-paper-reveals-students-with-disabilities-are-almost-twice-as-likely-to-be-victims-of-cyberbullying/

87 R. Gladden, A. Vivolo-Kantor, M. Hamburger, and C. Lumpkin, "Bullying Surveillance Among Youths: Uniform Definitions for Public Health and Recommended Data Elements, Version 1.0," *Atlanta, GA: National Center for Injury Prevention and Control, CDC*; (2014).

88 CDC, "Fast Facts: Preventing Bullying. National Center for Injury Prevention and Control," *CDC*; (September 28, 2023): https://www.cdc.gov/violenceprevention/youthviolence/bullyingresearch/fastfact.html.

89 StopBullying.gov. "Effects of Bullying. U.S. Department of Health and Human Services," (May 21, 2021): https://www.stopbullying.gov/bullying/effects.

90 S. Sumner, B. Ferguson, B. Bason, J. Dink, E. Yard, M. Hertz, B. Hilkert, K. Holland, M. Mercado-Crespo, S. Tang, and C. Jones, "Association of Online Risk Factors with Subsequent Youth Suicide-Related Behaviors in the US," *JAMA Network Open*, 4(9):e2125860. doi: 10.1001/jamanetworkopen.2021.25860.

91 R. Gladden, A. Vivolo-Kantor, M. Hamburger, and C. Lumpkin, "Bullying Surveillance Among Youths: Uniform Definitions for Public Health and Recommended Data Elements, Version 1.0.," *Atlanta, GA: National Center for Injury Prevention and Control, CDC*, (2014)

92 N. Wilkins, B. Tsao, M. Hertz, R. Davis, J. Klevens, "Connecting the Dots: An Overview of the Links Among Multiple Forms of Violence," *Atlanta, GA: National Center for Injury Prevention and Control, CDC and Oakland, CA: Prevention Institute*, (2014).

93 D. Espelage, S. Swearer, "Addressing research gaps in the intersection between homophobia and bullying," *School Psychology Review*, 37(2), (2008):155-159.

94 H. Clayton, G. Kilmer, S. DeGue, L. Estefan, V. Le, N. Suarez, B. Lyons, and J. Thornton, "Dating Violence, Sexual Violence, and Bullying Victimization among High School Students – Youth Risk Behavior Survey," *United States,* (2021): MMWR supp. 2023:72(1).

95 N. Wilkins, B. Tsao, M. Hertz, R. Davis, and J. Klevens, "Connecting the Dots: An Overview of the Links Among Multiple Forms of Violence," *Atlanta, GA: National Center for Injury Prevention and Control, CDC and Oakland, CA: Prevention Institute*, (2014).

96 N. Wilkins, B. Tsao, M. Hertz, R. Davis, and J. Klevens, "Connecting the Dots: An Overview of the Links Among Multiple Forms of Violence," Atlanta, GA: National Center for Injury Prevention and Control, CDC and Oakland, CA: Prevention Institute, (2014)

97 J. Hong, and D. Espelage, "A review of research on bullying and peer victimization in school: An ecological system analysis," *Aggression and Violent Behavior,* 17(4) (2012): 311-322.

98 J. Hong, and D. Espelage, "A review of research on bullying and peer victimization in school: An ecological system analysis," *Aggression and Violent Behavior,* 17(4) (2012): 311-322.

99 N. Wilkins, B. Tsao, M. Hertz, R. Davis, and J. Klevens, "Connecting the Dots: An Overview of the Links Among Multiple Forms of Violence," *Atlanta, GA: National Center for Injury Prevention and Control, CDC and Oakland, CA: Prevention Institute*, (2014)

100 N. Wilkins, B. Tsao, M. Hertz, R. Davis, and J. Klevens, "Connecting the Dots: An Overview of the Links Among Multiple Forms of Violence," *Atlanta, GA: National Center for Injury Prevention and Control, CDC and Oakland, CA: Prevention Institute*, (2014)

101 T. Nansel, M. Overpeck, D. Haynie, W. Ruan, and P. Scheidt, "Relationships between bullying and violence among US youth," *Archives of Pediatrics & Adolescent Medicine*, 157(4), (2003):348-353.

102 N. Wilkins, B. Tsao, M. Hertz, R. Davis, and J. Klevens, "Connecting the Dots: An Overview of the Links Among Multiple Forms of Violence," *Atlanta, GA: National Center for Injury Prevention and Control, CDC and Oakland, CA: Prevention Institute*, (2014)

103 Pichel et. al., "Analysis of the relationship between school bullying, cyberbullying, and substance use," *Children and Youth Services* Rev. Vol. 134, at 7.

104 CDC, "Suicide Prevention Resource for Action: A Compilation of the Best Available Evidence," *Atlanta, GA: National Center for Injury Prevention and Control, Centers for Disease Control and Prevention*.

105 S. Sumner, B. Ferguson, B. Bason, J. Dink, E. Yard, M. Hertz, B. Hilkert, K. Holland, M. Mercado-Crespo, S. Tang, and C. Jones, "Association of Online Risk Factors with Subsequent Youth Suicide-Related Behaviors in the US," *JAMA Network Open*, 4(9):e2125860. doi: 10.1001/jamanetworkopen.2021.25860.

106 N. Wilkins, B. Tsao, M. Hertz, R. Davis, and J. Klevens, "Connecting the Dots: An Overview of the Links Among Multiple Forms of Violence," *Atlanta, GA: National Center for Injury Prevention and Control, CDC and Oakland, CA: Prevention Institute*, (2014)

107 D. Espelage, and S. Swearer, "Addressing research gaps in the intersection between homophobia and bullying," *School Psychology Review,* 37(2), (2008):155-159.

108 A. Vivolo-Kantor, P. Niolon, L. Estefan, V. Le, A. Tracy, N. Latzman, T. Little, K. Lang, S. DeGue, and A. Tharp, "Middle School Effects of the Dating Matters ® Comprehensive Teen Dating Violence Prevention Model on Physical Violence, Bullying, and Cyberbullying: A Cluster-Randomized Controlled Trial," *Prevention Science,* 22, 151-161.

109 Community Preventive Services Task Force. "Violence Prevention: School-based Anti-Bullying Interventions – Findings and Rationale Statement," (December, 2021): https://www.thecommunityguide.org/pages/tf-frs-violence-prevention-school-based-anti-bullying-interventions.html.

110 National Academies of Sciences, Engineering, and Medicine, "Preventing Bullying Through Science, Policy, and Practice," *The National Academies Press*. https://doi.org/10.17226/23482.

111 H. Gaffney, M. Ttofi, and D. Farrington, "Evaluating the effectiveness of school-bullying prevention programs: An updated meta-analytical review," *Aggression and Violent Behavior*, 45, (2019): 111-133.

112 M. Hensums, B. De Mooij, S. Kuijper, M. Fekkes, and G. Overbeek, "What works for whom in school-based anti-bullying interventions? An individual participant data meta-analysis." *Prevention Science*, 24(8), (2023): 1435-1446.

113 Office of the U.S. Surgeon General, "Social Medqia and Youth Mental Health: The U.S. Surgeon General's Advisory." *U.S. Department of Health and Human Services*, https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf

114q S. Schoenebeck, C. Scott, E. Hurley, T. Chang, and E. Selkie, "Youth trust in social media companies and expectations of justice: Accountability and repair after online harassment," *Proceedings of the ACM on Human-Computer Interaction*, 5, (2021): 1–18. https://doi.org/10.1145/3449076.

115 Pew Research Center, "Teens and Cyberbullying," (December, 2022): https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/.

116 Family Online Safety Institute, "Managing the Narrative: Young People's Use of Online Safety Tools" (2021): https://www.fosi.org/policy-research/managing-the-narrative.

117 Family Online Safety Institute, "Managing the Narrative: Young People's Use of Online Safety Tools" (2021): https://www.fosi.org/policy-research/managing-the-narrative.

118 N. Wilkins, B. Tsao, M. Hertz, R. Davis, and J. Klevens, "Connecting the Dots: An Overview of the Links Among Multiple Forms of Violence," *Atlanta, GA: National Center for Injury Prevention and Control, CDC and Oakland, CA: Prevention Institute*, (2014).

119 C. Salmivalli, A. Huttunen, K. M. Lagerspetz, "Peer networks and bullying in schools," *Scandinavian Journal of Psychology*, ;38(4), (1997):305-312.

120 C. David-Ferdon, A. Vivolo-Kantor, L. Dahlberg, K. Marshall, N. Rainford, and J. Hall, "A comprehensive technical package for the prevention of youth violence and associated risk behaviors," *Atlanta, GA: National Center for Injury Prevention and Control, Centers for Disease Control and Prevention,* (2016).

121 CDC, "Suicide Prevention Resource for Action: A Compilation of the Best Available Evidence," *Atlanta, GA: National Center for Injury Prevention and Control, Centers for Disease Control and Prevention,* (2022).

122 C. David-Ferdon, A. Vivolo-Kantor, L. Dahlberg, K. Marshall, N. Rainford, and J. Hall, "A comprehensive technical package for the prevention of youth violence and associated risk behaviors," *Atlanta, GA: National Center for Injury Prevention and Control, Centers for Disease Control and Prevention,* (2016).

123 Centers for Disease Control and Prevention, "Adverse Childhood Experiences (ACEs) Prevention Resource for Action: A Compilation of the Best Available Evidence," *Atlanta, GA: National Center for Injury Prevention and Control, Centers for Disease Control and Prevention,* (2019).

124 K. Basile, S. DeGue, K. Jones, K. Freire, J. Dills, S. Smith, and J. Raiford, "Sexual Violence Prevention Resource for Action: A Compilation of the Best Available Evidence," *Atlanta, GA: National Center for Injury Prevention and Control, Centers for Disease Control and Prevention,* (2016)

125 CDC, "Suicide Prevention Resource for Action: A Compilation of the Best Available Evidence," *Atlanta, GA: National Center for Injury Prevention and Control, Centers for Disease Control and Prevention,* (2022)

126 S. Kairam, M. Mercado, and S. Sumner, "A Socio-Ecological Approach to Modeling Sense of Virtual Community (SOVC) in Livestreaming Communities," *Proc. ACM Hum.-Comput.* Interact., 6, (2022): CSCW2, Article 356, https://dl.acm.org/doi/10.1145/3555081

127 Digital Wellness Lab at Boston Children's Hospital, "Creating a Positive Foundation for Greater Civility in the Digital World," *Boston, MA: Boston Children's Hospital*, (2023): https://digitalwellnesslab.org

128 National Survey on LGBTQ Youth Mental Health, "The Trevor Project, at 14," (2021): https://www.thetrevorproject.org/wp-content/uploads/2021/05/The-Trevor-Project-National-Survey-Results-2021.pdf.

129 Sandro Galea et al., "Social Media and Adolescent Health," *Comm. on the Impact of Social Media on*

Adol. Health; Board on Pop. Health and Public Health Prac.; Health and Med. Div.; Nat'l Acad. of Sci., Eng'g, and Med.

130 A. McDaniel, "Women in Gaming: A Study of Female Players' Experiences in Online FPS Games," Honors Theses. 427, 28, (2016)

131 See also Comment of #ShePersisted on NTIA KOHS RFC at 4 (noting intersectional impact-based research indicating LGBTQIA users and users of color may face greater cyberbullying, for example); and Combined Comment of Common Sense Media, Center for Digital Democracy, Fairplay on NTIA KOHS RFC at 6-9.

132 See Comment from 5 Rights to NTIA KOHS RFC, 2023 (screen time with a parent or caregiver can be beneficial).

133 Kowalski et. al., "Cyberbullying among college students with disabilities," *Comp. in Human Behavior,* 57 (2016) 416-427 at 417. https://www.myovm.com/media/1046/cyberbullyingstudentsdisabilities.pdf.

134 J. Huynh, J. Chien, A. Nguyen, D. Honda, E. Cho, M. Xiong, T. Doan, and T. Ngo, "The mental health of Asian American adolescents and young adults amid the rise of anti-Asian racism," *Front Public Health*, (Jan, 2023): 10:958517. doi: 10.3389/fpubh.2022.958517. PMID: 36711363; PMCID: PMC9880072

135 "Online and ICT facilitated violence against women and girls during COVID-19," *UN Women* (2020): Brief-Online-and-ICT-facilitated-violence-against-women-and-girls-during-COVID-19-en.pdf (unwomen.org).

136 Ofcom, "Protecting children from harms online," Volume 3, (May 8, 2024): The causes and impacts of online harms to children, pp39-, https://www.ofcom.org.uk/__data/assets/pdf_file/0030/284484/vol3-causes-impacts-of-harms-to-children.pdf.

137 "Teens and Mental Health: How Girls Really Feel About Social Medi, Common Sense," at 46 (Mar. 30, 2023). how-girls-really-feel-about-social-media-researchreport_final_1.pdf (commonsensemedia.org) (among adolescent girls of color, one-third or more report exposure to racist content or language on social media platforms at least monthly).

138 M. Anderson, M. Faverio, and J. Gottfried, "Teens, Social Media and Technology," *Pew Research Center,* 2023.

139 Ofcom, "Protecting children from harms online," Volume 3: The causes and impacts of online harms to children, pp39-, (May 8, 2024): https://www.ofcom.org.uk/__data/assets/pdf_file/0030/284484/vol3-causes-impacts-of-harms-to-children.pdf.

140 O. Lopez-Fernandez et al., "Female Gaming, Gaming Addiction, and the Role of Women Within Gaming Culture: A Narrative Literature Review," *Frontiers in Psych*. Vol. 10 454, 6.

141 O. Lopez-Fernandez et al., "Female Gaming, Gaming Addiction, and the Role of Women Within Gaming Culture: A Narrative Literature Review," *Frontiers in Psych*. Vol. 10 454, 6.

142 J. Stoever, "Title IX, Esports, and #EToo," (July 27, 2021). 89 GEO. WASH. L. REV. 857 (2021), UC Irvine School of Law Research Paper No. 2021-42,at 8810896, https://ssrn.com/abstract=3894496.

143 Protecting children from harms online Volume 3: The causes and impacts of online harms to children, pp 113-116, (May 8, 2024), https://www.ofcom.org.uk/__data/assets/pdf_file/0030/284484/vol3-causes-impacts-of-harms-to-children.pdf.

144 "Young people's experiences of online misogyny and image-based abuse," *Internetmatters.org*, (September, 2023): https://www.internetmatters.org/wp-content/uploads/2023/09/Internet-Matters-Online-misogyny-and-image-based-abuse-report-Sep-2023-2.pdf.

145 D. English, S. Lambert, B. Tynes, L. Bowleg, M. Zea, and L. Howard, "Daily multidimensional racial

discrimination among Black U.S. American adolescents," *J Appl Dev Psychol.* at 6. (2020): Jan-Feb;66:101068. doi: 10.1016/j.appdev.2019.101068. Epub 2019 Dec 11. PMID: 33994610; PMCID: PMC8117402.

146 "A Double-Edged Sword: How Diverse Communities of Young People Think About the Multifaceted Relationship Between Social Media and Mental Health, Common Sense Media," at 7 2024-double-edged-sword-hopelab-report_final-release-for-web-v2.pdf (commonsensemedia.org).

147 S. Galea et al., "Social Media and Adolescent Health," *Comm. on the Impact of Social Media on Adol. Health; Board on Pop. Health and Public Health Prac.; Health and Med. Div.; Nat'l Acad. of Sci., Eng'g, and Med*.

148 A. Bliuc et al, "Online networks of racial hate: A systematic review of 10 years of research on cyber-racism, Computers in Human Behavior" 87, (2018): 75-86

149 J. Huynh, J. Chien, A. Nguyen, D. Honda, E. Cho, M. Xiong, T. Doan, T. Ngo, "The mental health of Asian American adolescents and young adults amid the rise of anti-Asian racism," *Front Public Health*. (2023): Jan 13;10:958517. doi: 10.3389/fpubh.2022.958517. PMID: 36711363; PMCID: PMC9880072.

150 A. Umaña-Taylor, B. Tynes, R. Toomey, D. Williams, K. Mitchell, "Latino adolescents' perceived discrimination in online and offline settings: an examination of cultural risk and protective factors," *Dev Psychol*. 51(1), (2015 Jan): 87-100. doi: 10.1037/a0038432. PMID: 25546597; PMCID: PMC4752111.

151 B. Tynes et, al., "Online Racial Discrimination, Suicidal Ideation, and Traumatic Stress in a National Sample of Black Adolescents," 315 (Mar, 2024).

152 B. Tynes, A. Maxie-Moreman, T. Hoang, H. Willis, D. English, "Online Racial Discrimination, Suicidal Ideation, and Traumatic Stress in a National Sample of Black Adolescents," *JAMA Psychiatry*. 81(3), (2024): 312–316. doi:10.1001/jamapsychiatry.2023.4961.

153 J. Cubbage, and L. Adams, "Still Ringing the Alarm, An Enduring Call to Action for Black Youth Suicide Prevention," Johns Hopkins Center for Gun Violence Solutions and Johns Hopkins Bloomberg School of Public Health, Department of Mental Health, 4 (2023).

154 K. Calhoun, and A. Fawcett, "They Edited Out her Nip Nops: Linguistic Innovation as Textual Censorship Avoidance on TikTok" *Language@ Internet,* 21: art. 1. (2023): https://www.languageatinternet.org/articles/2023/calhoun.

155 K. Rosenblatt, "Months after TikTok apologized to Black creators, many say little has changed." *NBC News*, (Feb. 29, 2021): https://www.nbcnews.com/pop-culture/pop-culture-news/months-after-tiktok-apologized-black-creators-many-say-little-has-n1256726.

156 See G. Birchall et al., "Chinese Users Claim iPhone X Face Recognition Can't Tell Them Apart," *NYPOST*, (Dec. 21, 2017) https://nypost.com/2017/12/21/chinese-users-claim-iphone-x-face-recognition-cant-tell-them-apart/ (stating that Apple was accused of racism in 2017 when a child using the iPhone X was able to unlock the phone with his face rather than his mother's).

157 K. Hill, "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match," *New York Times*, (Dec. 29, 2020).

158 See H. Chang, et al., "Targeted Ads and/as Racial Discrimination: Exploring Trends in New York City Ads for College Scholarships," (2021).

159 C. Gilliard, "Prepared testimony and statement for the record of Christopher Gilliard PhD," *Hearing on Banking on your Data the Role of Big Data in Your Financial Services, Before the House Financial Services Committee Task Force on Financial Technology,* (2019).

160 H. Chang et al., "Targeted Ads and/as Racial Discrimination: Exploring Trends in New York City Ads for College Scholarships," (2021)

161 G. Birchall et al., "Chinese Users Claim iPhone X Face Recognition Can't Tell Them Apart", *NY Post*, (Dec 21, 2017): https://nypost.com/2017/12/21/chinese-users-claim-iphone-x-face-recognition-cant-tell-them-apart/.

162 K. Hill, "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match," *NY Times*, (Dec. 29, 2020).

163 FTC complaint against Fortnite, paragraph 40 ("All the while, kids have been bullied, threatened, and harassed, including sexually, through Fortnite. Numerous news stories chronicle reports of predators blackmailing, extorting, or coercing children and teens they met through Fortnite into sharing explicit images or meeting offline for sexual activity. Such issues are also the subject of numerous player support tickets submitted to Epic by distressed parents and players.") See https://www.ftc.gov/system/files/ftc_gov/pdf/2223087EpicGames-Complaint.pdf.

164 J. Campbell, and J. Kravarik, "A 17-year-old boy died by suicide hours after being scammed. The FBI says it's part of a troubling increase in 'sextortion' cases," *CNN,* (May 23, 2022).

165 NTIA KOHS RFC, Comment from END Online Sexual Exploitation and Abuse of Children Coalition.

166 Western District of Washington | FBI and Partners Issue National Public Safety Alert on Financial Sextortion Schemes | United States Department of Justice https://www.justice.gov/usao-wdwa/pr/fbi-and-partners-issue-national-public-safety-alert-financial-sextortion-schemes; WeProtect Global Alliance, Global-Threat-Assessment-2023-English.pdf (weprotect.org) at 20.

167 In the typical sextortion scheme, the offender (i) makes contact with the targeted minor on social media and pretends to be a peer of the targeted minor; (ii) persuades the targeted minor to send sexually explicit images or videos of him- or herself to the offender (or creates such images himself through the use of AI); and then (iii) threatens to widely distribute the sexually explicit images and videos of the targeted minor (for example, to the minor's parents, coaches, religious leaders, school, etc.) unless the minor sends money or additional imagery to the offender.

168 See FTC complaint against Fortnite, paragraph 40 ("All the while, kids have been bullied, threatened, and harassed, including sexually, through Fortnite. Numerous news stories chronicle reports of predators blackmailing, extorting, or coercing children and teens they met through Fortnite into sharing explicit images or meeting offline for sexual activity. Such issues are also the subject of numerous player support tickets submitted to Epic by distressed parents and players.") See https://www.ftc.gov/system/files/ftc_gov/pdf/2223087EpicGames-Complaint.pdf. For a much more robust assessment of the risks of online child sexual exploitation and abuse, please see the Department of Justice's 2023 "National Strategy for Child Exploitation Prevention & Interdiction," and the associated subject matter expert working group reports, available at https://www.justice.gov/psc/national-strategy-child-exploitation-prevention-and-interdiction.

169 For a more robust discussion of sextortion, see Department of Justice, "National Strategy for Child Exploitation Prevention and Interdiction," Subject-Matter Expert Report on "Sextortion, Crowdsourcing, Enticement, and Coercion" (2023).

170 2023 CyberTipline Data (missingkids.org) (2023): https://www.missingkids.org/content/dam/missingkids/pdfs/2023-CyberTipline-Report.pdf.

171 NCMEC, "Sextortion." Unsurprisingly, the problem is international in scope. See, e.g., Internet Watch Foundation, "Hotline reports 'shocking' rise in the sextortion of boys" (Sept. 18, 2023) ("The Internet Watch Foundation (IWF) has found that in the first six months of 2023 reports of confirmed child sexual abuse involving 'sextortion' surged by 257% compared with the whole of 2022."); WeProtect Global Alliance, "Global Threat Assessment 2023" at 20 ("Of known cases, many schemes orchestrated by offshore criminal syndicates reportedly originate from countries such as Nigeria, Côte d'Ivoire, and the Philippines, and target children from more affluent countries.").

172 See, e.g., FBI Sacramento, "Sextortion: A Growing Threat Preying Upon Our Nation's Teens" (Jan. 17, 2024) https://www.fbi.gov/contact-us/field-offices/sacramento/news/sextortion-a-growing-threat-preying-upon-our-nations-teens.

173 J. Campbell, and J. Kravarik, "A 17-year-old boy died by suicide hours after being scammed. The FBI says it's part of a troubling increase in 'sextortion' cases," *CNN* (May 23, 2022).

174 WeProtect Global Alliance, "Global Threat Assessment 2023"

175 D. Citron, "Sexual Privacy," *128 Yale L.J.* 1870, 1926 (2019).

176 H. Turner, D. Finkelhor, D. Colburn, "Contexts and Characteristics of Imaged-BasedSexual Exploitation and Abuse of Children: Incident Dynamics in a National Sample," *Child Maltreat*. 20 (Feb, 2024):10775595241233970. doi: 10.1177/10775595241233970. Epub ahead of print. PMID: 38378143.

177 D. Finkelhor, H. Turner, and D. Colburn, "Prevalence of Online Sexual Offenses Against Children in the US.," *JAMA* (Oct, 2022): Netw Open. 3;5(10):e2234471. doi: 10.1001/jamanetworkopen.2022.34471. PMID: 36239942; PMCID: PMC9568794.

178 N. Hanacek, "Face Analysis Technology Evaluation (FATE) Age Estimation & Verification," *NIST*, (May 28, 2024): https://pages.nist.gov/frvt/html/frvt_age_estimation.html.

179 One effort to address questions of media content provenance (history/source) issues is the technical standard developed by the Coalition for Content Provenance and Authenticity. https://c2pa.org/.

180 V. Strasburger, H. Zimmerman, J. Temple, and S. Madigan, "Teenagers, sexting, and the law," *Pediatrics*, 143(5).

181 J. Temple, V. Le, P. van den Berg, Y. Ling, J. Paul, and B. Temple, "Brief report: Teen sexting and psychosocial health," *Journal of Adolescence*, 37(1), (2014): 33-36.

182 J. Rose, K. Regehr, B. Milne, "Understanding and Combatting Youth Experiences of Image-Based Sexual Harassment and Abuse," *Department of Education, Practice and Society, UCL Institute of Education*, (2021): https://discovery.ucl.ac.uk/id/eprint/10139669.

183 J. Wolak, D. Finkelhor, W. Walsh, and W. Treitman, "Sextortion of Minors: Characteristics and Dynamics," *Journal of Adolescent Health* no. 62, (2018): 72–79 https://www.unh.edu/ccrc/sites/default/files/media/2022-02/sextortion-of-minors-characteristics-and-dynamics.pdf

184 NTIA KOHS RFC, Comment from Internet Safety Labs. Nov. 16, 2023. https://www.regulations.gov/comment/NTIA-2023-0008-0491.

185 S. Livingstone, M. Stoilova, R. Nandagiri, "Children's data and privacy online: Growing up in a digital age. An evidence review."

186 V. Steeves, and C. Webster, "Closing the Barn Door: The Effect of Parental Supervision on Canadian Children's Online Privacy." *Bulletin of Science, Technology & Society*, 28(1), (2008): 4–19. https://doi.org/10.1177/0270467607311488.

187 N. Alomar, and S. Egelman, "Developers Say the Darnedest Things: Privacy Compliance Processes Followed by Developers of Child-Directed Apps." *Proceedings on Privacy Enhancing Technologies Symposium*, (4), (2022): 250–273. https://doi.org/10.56553/popets-2022-0108.

188 R. Balebako, A. Marsh, J. Lin, J. Hong, and L. Cranor, "The Privacy and Security Behaviors of Smartphone App Developers." USEC '14. Network and Distributed System Security (NDSS) Symposium USEC '14. 10.14722/usec.2014.23006.

189 S. Spiekermann, J. Korunovska, and M. Langheinrich, "Inside the Organization: Why Privacy and Security Engineering Is a Challenge for Engineers," Proceedings of the IEEE, 107(3), (2019): 600–615. https://ssrn.com/abstract=3598930.

190 L. Yu, H. Li, W. He, F. Wang, and S. Jiao, "A meta-analysis to explore privacy cognition and information disclosure of Internet users," *International Journal of Information Management*, 51, (2020): 102015. https://www.sciencedirect.com/science/article/abs/pii/S026840121831137X?via%3Dihub.

191 "Kids & Screen Time: How to Use the 5 C's of Media Guidance," *HealthyChidren.org*, (April 30, 2024): https://www.healthychildren.org/English/family-life/Media/Pages/kids-and-screen-time-how-to-use-the-5-cs-of-media-guidance.aspx.

192 For more on this topic, see, for example, Comment from 5 Rights Foundation to NTIA KOHS RFC at 4 (2023) https://www.regulations.gov/comment/NTIA-2023-0008-0384.

193 According to International Organization for Standardization (ISO) standard 9241-210:2019 ISO 9241-210, human-centered design is "an approach to interactive systems development that aims to make systems usable and useful by focusing on the users, their needs and requirements, and by applying human factors/ergonomics, and usability knowledge and techniques." ISO 9241-210:2019 Ergonomics of human-system interaction — Part 210: Human-centered design for interactive systems.

194 B. Friedman, D. Hendry, and A. Borning, "A survey of value sensitive design methods. Foundations and Trends® in Human–Computer Interaction," 11(2), (2017): 63-125.; Knobel, C., & Bowker, G. C. (2011). Values in design. Communications of the ACM, 54(7), 26-28.

195 General comment No. 25 (2021) on children's rights in relation to the digital environment | OHCHR, paras 19-21, p4; see, also, Digital Childhood – Addressing Childhood Development Milestones in the Digital Environment. Baroness Beeban Kidron, Founder 5Rights, and Dr. Angharad Rudkin, University of Southampton. Dec. 2017 ("In broad terms, childhood development moves from a state of high dependency on carers for security and guidance (infancy to 5 years), towards a move to school that increases independence and self-care (6-11 years), through to adolescence which is a time of increasing autonomy and growing reliance on peers for approval and support (12-18 years) and the final step in the move towards fully independent adult living (18-25). ").

196 Comment on NTIA KOHS RFC, American Academy of Pediatrics (noting also differences by gender….).

197 In the typical sextortion scheme, the offender (i) makes contact with the targeted minor on social media and pretends to be a peer of the targeted minor; (ii) persuades the targeted minor to send sexually explicit images or videos of him- or herself to the offender (or creates such images himself through the use of AI); and then (iii) threatens to widely distribute the sexually explicit images and videos of the targeted minor (for example, to the minor's parents, coaches, religious leaders, school, etc.) unless the minor sends money or additional imagery to the offender.

198 J. Nesi, E. Telzer, and M. Prinstein, "Adolescent Development in the Digital Media Context," *Psychological Inquiry* 31, no. 3 (2020): 230, https://doi.org/10.1080/1047840x.2020.1820219.

199 General comment No. 25 (2021) on children's rights in relation to the digital environment | OHCHR, paras 19-21, p4.

200 Digital Childhood – Addressing Childhood Development Milestones in the Digital Environment. Baroness Beeban Kidron, Founder 5Rights, and Dr. Angharad Rudkin, University of Southampton. Dec. 2017 ("In broad terms, childhood development moves from a state of high dependency on carers for security and guidance (infancy to 5 years), towards a move to school that increases independence and self-care (6-11 years), through to adolescence which is a time of increasing autonomy and growing reliance on peers for approval and support (12-18 years) and the final step in the move towards fully independent adult living (18-25). ").

201 Comment on NTIA KOHS RFC, American Academy of Pediatrics, Nov. 30, 2023 (noting also differences by gender….).

202 Comment on NTIA KOHS RFC , BBB National Programs at 5-6, Nov. 30, 2023 (noting needs of 17, 13 and 7 year olds differ).

203 Comment from 5 Rights to NTIA KOHS RFC at 13, 2023 ("Some of the most commonly used EdTech products are commercially provided, highly data extractive and use the same persuasive design strategies found on social media, such as gamification and personalization").

204 Services that are directed to minors may have specific obligations under state law. Services that are directed to children under 13 must obtain verified parental consent before collecting personal information from their users, as required by the Children's Online Privacy Protection Act.

205 The Australian eSafety Commission, which has studied the topic particularly with regard to limiting minors' access to pornography, concluded in early 2023 that mandating age assurance methods was not yet possible as "each type of age verification or age assurance technology comes with its own privacy, security, effectiveness and implementation issues." (Australia) "Roadmap for age verification and complementary measures to prevent and mitigate harms to children from online pornography, eSafety (March 2023) (concluding "that a decision to mandate age assurance is not ready to be taken."); See, also, Online age verification: balancing privacy and the protection of minors, French CNIL (Sep. 22, 2022). https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors.

206 E.g., comment of ITI to NTIA Kids Online Health and Safety (KOHS) Request for Comment (RFC) (these come with tradeoffs, involving more data collection/use or restricted access for adults so age assurance should be risk-based and not mandated for all, citing to UK AADC principles, providing guidance and flexibility for companies).

207 E.g., comment on NTIA KOHS RFC, Microsoft, Nov. 30, 2023 (noting legislation should allow for "risk-based, proportionate application of age assurance mechanisms").

208 E.g., comment on NTIA KOHS RFC, TechNet, Nov. 30, 2023.

209 E.g., comment on NTIA KOHS RFC, R Street Nov. 30, 2023 (noting age assurance makes sense for pornography and gambling sites, but not for general-use platforms).

210 See, e.g., Measurement of Age Assurance Technologies | DRCF and Home - Age Check Certification Scheme (accscheme.com).

211 See, e.g., Families' attitudes towards age assurance, Research commissioned by the United Kingdom's Information Commissioner's Office and Ofcom (Oct. 11, 2022), at 19, available at https://www.gov.uk/government/publications/families-attitudes-towards-age-assurance-researchcommissioned-by-the-ico-and-ofcom (cited in the Children's Online…. Rulemaking doc, FTC, N177). In addition, parents and guardians sometimes assist in setting up adult accounts for minors, as a way to exercise their rights to decide where their kids can go online. See, e.g., (UK) Families Attitudes Towards Age Assurance, Digital Regulation Cooperative Forum, 2021 (research commissioned by the ICO and Ofcom), pp6-7.

212 Face Analysis Technology Evaluation (FATE) Age Estimation & Verification, NIST (May 2024) https://doi.org/10.6028/NIST.IR.8525.

213 Comment on NTIA KOHS RFC, Match to NTIA KOHS RFC (describing how it uses additional sources).

214 See, e.g., Comment on NTIA KOHS RFC, Access Now, (privacy, surveillance, disproportionate risk to LGBTQ youth).

215 See comment on NTIA KOHS RFC from CDT (privacy concerns).

216 See comment on NTIA KOHS RFC from CCIA (citing CNIL (French) study of age-verification solutions).

217 See comment on NTIA KOHS RFC from Future of Privacy Forum (privacy risks, limits legitimate access to services).

218 See comment on NTIA KOHS RFC from Huddleston (requiring age verification "will result in companies having access to IDs or biometrics of all [I]nternet users").

219 See comment on NTIA KOHS RFC from NetChoice and Comment from Taxpayers Protection Alliance (saying age and users ID can't be separated).

220 See comment on NTIA KOHS RFC from Public Knowledge (significant privacy risks, including loss of anonymity).

221 See, e.g., Centre for Information Policy Leadership, Protecting Children's Data Privacy POLICY PAPER I, International Issues And Compliance Challenges at 31 (Oct. 20, 2022) (filed as a comment to NTIA, https://www.regulations.gov/comment/NTIA-2023-0008-0391).

222 International Organization for Standardization/International Electrotechnical Commission, ISO/IEC 27566-1 (under development) Information security, cybersecurity and privacy protection — Age assurance systems — Framework — Part 1: Framework, https://www.iso.org/standard/88143.html.

223 Digital Trust & Safety Partnership, Age Assurance: Guiding Principles and Best Practices (Sept. 2023), https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf.

224 We use "age assurance" to refer to the range of techniques that can be used to estimate or verify the age of an individual online.

225 The Australian eSafety Commission, which has studied the topic particularly with regard to limiting minors' access to pornography, concluded in early 2023 that mandating age assurance methods was not yet possible as "each type of age verification or age assurance technology comes with its own privacy, security, effectiveness and implementation issues." (Australia) Roadmap for age verification and complementary measures to prevent and mitigate harms to children from online pornography, eSafety (March 2023) (concluding "that a decision to mandate age assurance is not ready to be taken.").

226 See Online age verification: balancing privacy and the protection of minors, French CNIL (Sep. 22, 2022) https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors.

227 For example, UK Information Commissioner's Office, Age Assurance Opinion, (Jan. 18, 2014) (3. Age assurance methods); https://ico.org.uk/about-the-ico/what-we-do/information-commissioners-opinions/age-assurance-for-the-children-s-code/3-age-assurance-methods/. See also Ofcom, "Consultation: Guidance for service providers publishing pornographic content (Dec. 5, 2023), https://www.ofcom.org.uk/__data/assets/pdf_file/0017/272600/consultation-part-5-guidance.pdf 4.12-13 (Noting it does "not have sufficient evidence as to the effectiveness and potential risks of different age assurance methods to recommend specific metrics for assessing whether or not any given age assurance method or process should be considered highly effective" and that "it would not be appropriate at this time to set a base level or score which service providers must ensure their age assurance method or process meets for each of the criteria.").

228 COPPA applies to data about children under 13. It includes collection, use, and retention limitations, as well as data security requirements. Use limits prevent children's data collected with permission for one purpose from ending up as part of some other score, algorithm, profile, or for another commercial use (for instance A/B testing or supposedly "anonymous" or "aggregate" audience models that parents did not consent to). COPPA also includes retention limits to prevent companies, once they collect a child's data, from keeping it for speculative future uses. The COPPA Rule is currently under review to ensure it meets the needs of modern technological advances. See https://www.ftc.gov/news-events/news/press-releases/2023/12/ftc-proposes-strengthening-childrens-privacy-rule-further-limit-companies-ability-monetize-childrens.

229 The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. FERPA applies here to the extent that the technology is an online educational service provided by a third-party or school district and used as a part of a school activity. For more information about FERPA, please visit the U.S. Department of Education's Student Privacy Policy Office's Web site at https://studentprivacy.ed.gov.

230 CA Civ Code § 1798.99.28-40 (2022) (currently under preliminary injunction, NetChoice v. Bonta, Case No. 22-cv-08861-BLF, N.D. Cal., Sep. 18, 2023, on appeal in Bonta v. NetChoice, Case No. 23-2969, 9th Cir., oral arguments scheduled for Jul. 17, 2024).

231 The White House, "State of the Union," (2024): https://www.whitehouse.gov/state-of-the-union-2024/.

232 The White House, "Readout of White House Listening Session on Tech Platform Accountability," (Sept. 08, 2022): https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/08/read-out-of-white-house-listening-session-on-tech-platform-accountability/.

233 COPPA NPR, 89 Fed. Reg. at 2059-62.

234 The Children's Online Privacy Protection Act prohibits collecting more personal information from a child than is reasonably necessary for a child to participate in a game, offering of a prize, or another activity. See 15 U.S.C. § 6502(b)(1)(c); 16 C.F.R. § 312.7; COPPA NPR, 89 Fed. Reg. at 2059-60.

235 The COPPA Rule specifically states that operators should retain personal information collected online from a child for only as long as is reasonably necessary to fulfill the purpose for which the information was collected. See 16 C.F.R. § 312.10.

236 COPPA NPRM, 89 Fed. Reg. at 2062 (proposing these measures).

237 Epic Games' settlement with the FTC in 2022 requires the company to have strong privacy default settings for children and teen users of products, including Fortnite, ensuring that voice and text communications are turned off by default. See Fed. Trade Comm'n, Fortnite Video Game Maker Epic Games to Pay More Than Half a Billion Dollars over FTC Allegations of Privacy Violations and Unwanted Charges (Dec. 19, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/12/fortnite-video-game-maker-epic-games-pay-more-half-billion-dollars-over-ftc-allegations.

238 See also Children's Online Privacy Protection Rule Notice of Proposed Rulemaking, 89 Fed. Reg. 2034 (Jan. 11, 2024) [hereinafter COPPA NPR] (The FTC's recent proposed changes to the COPPA Rule include a proposal making more rigorous the ban on sharing children's information with third parties by default and making more explicit within the Rule that operators are prohibited from conditioning access to the service on the parent agreeing to the sharing of information.).

239 See Complaint, United States v. Amazon.com, Inc., 2:23-cv-811 (W.D. Wash 2023), available at https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever (allegation that data deletion requests were not honored due to undisclosed retention of transcripts of children's voice recordings).

240 See also Complaint, In re: Epic Games, Inc., FTC Docket No. C-4790 (Mar. 14, 2023) at https://www.ftc.gov/system/files/ftc_gov/pdf/1923203epicgamesfinalconsent.pdf (alleging that operators failed to delete children's personal information at parents' requests).

241 Design it For Us Policy Platform, Section V(D), https://designitforus.org/resource/policy-platform.

242 U.S. Surgeon General, "Social Media and Youth Mental Health: The U.S. Surgeon General's Advisory," 16 (2023): https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf ("Surgeon General's Advisory") ("Ensure default settings for children are set to highest safety and privacy standards.").

243 Center for Digital Democracy, Fairplay, et al., "Petition for Rulemaking to Prohibit the Use on Children of Design Features that Maximize for Engagement" ("Fairplay/CDD Petition"), 67 (Nov. 17, 2022), https://www.regulations.gov/document/FTC-2022-0073-0002.

244 See also US v. Epic Games, Inc. (E.D.N.C. 2023) (FTC settlement in which Epic Games agreed to set minors' strong privacy settings for minors using Fortnite at their highest levels by default), https://www.ftc.gov/news-events/news/press-releases/2022/12/fortnite-video-game-maker-epic-games-pay-more-half-billion-dollars-over-ftc-allegations.

245 Design It For Us recommends eliminating targeted advertising to minors and young adults. See Design It For Us Policy Platform, Section II(A). The FTC has brought numerous cases against companies that collected from children, or caused to be collected from children on their behalf, persistent identifiers and/or other personal information and used such information to deliver targeted ads without complying with the Children's Online Privacy Protection Act's verifiable parental consent requirement.

246 See, e.g., Complaint, US v. OpenX Techs., Inc., 2:21-cv-09693 (C.D. Cal. Dec. 15, 2021); Complaint, US v. Hyperbeard, Inc., 3:20-cv-03683 (N.D. Cal. June 3, 2020); Complaint, FTC and State of NY v. Google, LLC and YouTube, LLC, 1:19-cv-02642 (D.D.C. Sept. 4, 2019).

247 See also Complaint, US v. Edmodo, LLC, 3:23-cv-02495 (N.D. Cal. May 23, 2023) (alleging that ed tech provider violated COPPA by failing to obtain verifiable parental consent for collection and use of persistent identifiers for contextual advertising)., and engagement.

248 J. Pfeifer et. al, "What Science Tells Us About How to Promote Positive Development and Decrease Risk in Online Spaces for Early Adolescents," *UCLA*. https://developingadolescent.semel.ucla.edu/assets/uploads/research/resources/DigitalTechReport_FINAL_WEB_doi.pdf.

249 An August 2023 European Union (EU) Parliament Committee Report on addictive design recommends turning off all notifications by default. European Parliament Committee on the Internal Market and Consumer Protection, Report on Addictive Design of Online Services and Consumer Protection in the EU Single Market ("EU Report") (Aug. 23, 2023), https://www.europarl.europa.eu/doceo/document/A-9-2023-0340_EN.pdf. American Federation of Teachers ("AFT") President Randi Weingarten also suggested at an October 2023 Safe Tech, Safe Kids conference that notifications could be muted while children are in school. Alternatively, lower-priority notifications might be muted by default (e.g., passive or less direct interactions such as reactive emojis to the minor's post). or even notifications unrelated to the minor's own such as posts by, accounts the minor follows, or a notification that the minor has not interacted with a certain user in a while).

250 A. Hern, "TikTok acts on teen safety with 'bedtime' block on app alerts," The Guardian (Aug. 12, 2021) https://www.theguardian.com/technology/2021/aug/12/tiktok-acts-on-teen-safety-with-bedtime-block-on-app-alerts#:~:text=The%20company%20will%20no%20longer,not%20be%20sent%20after%2010pm.

251 An August 2023 European Union (EU) Parliament Committee Report on addictive design recommends turning off all notifications by default. European Parliament Committee on the Internal Market and Consumer Protection, Report on Addictive Design of Online Services and Consumer Protection in the EU Single Market ("EU Report") (Aug. 23, 2023), https://www.europarl.europa.eu/doceo/document/A-9-2023-0340_EN.pdf. American Federation of Teachers ("AFT") President Randi Weingarten also suggested at an October 2023 Safe Tech, Safe Kids conference that notifications could be muted while children are in school. Alternatively, lower-priority notifications might be muted by default (e.g., notifications about passive or less direct interactions like reactive emojis to the minor's post, or notifications unrelated to the minor's own posts, such as posts by accounts the minor follows, or a notification that the minor has not interacted with a certain user in a while).

252 A. Hern, "TikTok acts on teen safety with 'bedtime' block on app alerts," The Guardian (Aug. 12, 2021) https://www.theguardian.com/technology/2021/aug/12/tiktok-acts-on-teen-safety-with-bedtime-block-on-app-alerts#:~:text=The%20company%20will%20no%20longer,not%20be%20sent%20after%2010pm.

253 C. Odgers, N. Allen, J. Pfeifer, R. Dahl, J. Nesi, S. Schueller, J. Williams, and the National Scientific Council on Adolescence, "Engaging, safe, and evidence-based: What science tells us about how to promote positive development and decrease risk in online spaces," *Council Report No 2*, (2022): https://developingadolescent.semel.ucla.edu/assets/uploads/research/resources/DigitalTechReport_FINAL_WEB_doi.pdf. The FTC recently proposed amendments that would clarify that an operator's online notice must indicate the use of children's personal information to encourage or prompt use of the operator's website or online service, such as through a push notification (89 Fed. Reg. at 2050) and to exclude from the internal operations and multiple contacts exceptions to COPPA's VPC requirement the use of persistent identifiers to encourage or prompt use of a website or online service. (89 Fed. Reg. at 2053. 2059, 2074).

254 Yolanda Reid et al., "Media and Young Minds," Pediatrics Vol. 138 , iss. 5 https://publications.aap.org/pediatrics/article/138/5/e20162591/60503/Media-and-Young-Minds?autologincheck=redirected.

255 "Blue Blocker Glasses as a Countermeasure for Alerting Effects of Evening Light-Emitting Diode Screen Exposure in Male Teenagers," at 114 https://www.jahonline.org/article/S1054-139X(14)00324-3/fulltext (explaining that excessive blue light exposure can negatively affect circadian physiology in male youth).

256 An August 2023 European Union (EU) Parliament Committee Report on addictive design recommends turning off all notifications by default. European Parliament Committee on the Internal Market and Consumer Protection, Report on Addictive Design of Online Services and Consumer Protection in the EU Single Market ("EU Report") (Aug. 23, 2023), https://www.europarl.europa.eu/doceo/document/A-9-2023-0340_EN.pdf. American Federation of Teachers ("AFT") President Randi Weingarten also suggested at an October 2023 Safe Tech, Safe Kids conference that notifications could be muted while children are in school. Alternatively, lower-priority notifications might be muted by default (e.g., passive or less direct interactions such as reactive emojis to the minor's post). or even notifications unrelated to the minor's own such as posts by, accounts the minor follows, or a notification that the minor has not interacted with a certain user in a while).

257 Alex Hern, "TikTok acts on teen safety with 'bedtime' block on app alerts," *The Guardian* (Aug. 12, 2021) https://www.theguardian.com/technology/2021/aug/12/tiktok-acts-on-teen-safety-with-bedtime-block-on-app-alerts#:~:text=The%20company%20will%20no%20longer,not%20be%20sent%20after%2010pm.

258 FTC Video Game Loot Box Workshop, Staff Perspective (Aug. 2020) at 1, https://www.ftc.gov/system/files/documents/reports/staff-perspective-paper-loot-box-workshop/loot_box_workshop_staff_perspective.pdf ("Broadly speaking, a loot box is a video game microtransaction in which the consumer purchases a reward containing one or more virtual items of differing value or rarity assigned at random.").

259 D. Yeager, R. Dahl, and C. Dweck, "Why interventions to influence adolescent behavior often fail but could succeed," *Perspectives on Psychological Science : a Journal of the Association for Psychological Science* 13, no. 1, (2018): 101-122, https://doi.org/ 10.1177/1745691617722620; see also J. Nesi, E. Telzer and M. Prinstein, "Adolescent Development in the Digital Media Context," *Psychological Inquiry 31*, no. 3 (2020): 230, https://doi.org/10.1080/1047840x.2020.1820219.

260 "Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show," *The Wall Street Journal*, accessed September 12, 2022, https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739.

261 E.g., comment of APA to NTIA KOHS RFC at 5 ("platforms are more apt to motivate users towards one's metrics than people themselves, which has led many youths to upload curated or filtered content to portray themselves most favorably. Note that these features of social media, and the resulting behaviors of those who use social media create the exact opposite qualities needed for successful and adaptive relationships (i.e., disingenuous, anonymous, depersonalized). In other words, social media offers the 'empty calories of social interaction,' that appear to help satiate our biological and psychological needs, but do not contain any of the healthy ingredients necessary to reap benefits.").

262 See In Re: Social Media Adolescent Addiction/Personal Injury Products Liability Litigation, at 135.

263 Courts and Tribunals Judiciary, Molly Russell: Prevention of Future Deaths Report, (13 October 2022), https://www.judiciary.uk/prevention-of-future-death-reports/molly-russell-prevention-of-future-deaths-report/.

264 Fairplay/CDD Petition, at 66-67.

265 Id. Design it For Us generally supports eliminating or hiding by default public displays of engagement and engagement metrics, such as likes, views, etc. Design it For Us, Policy Platform, Section I(A), Appendix (last visited Dec. 11, 2023), https://designitforus.org/resource/policy-platform/.

266 Take It Down website, National Center for Missing & Exploited Children,https://takeitdown.ncmec.org/

267 Cyber Tip Line, https://www.missingkids.org/gethelpnow/cybertipline.

268 See, e.g., U.S. Dep't of Justice, 2023 National Strategy for Child Exploitation Prevention & Interdiction, Unique Resource and Enforcement Issues Subject Matter Expert Working Group Report, at 7 ("Law enforcement also has difficulties when companies fail to provide any information in response to a valid search warrant, when tech companies provide the requested information in an unreadable format, when there is a significant delay in receiving information in response to a search warrant, ...").

269 For example, see the Technology Coalition's "Project Lantern," https://www.technologycoalition.org/newsroom/announcing-lantern.

270 Know 2 Protect, Department of Homeland Security, https://www.dhs.gov/know2protect

271 In this context, red-teaming refers to the process by which a company (1) tests its generative AI platform to determine whether and how the platform can be used to generate CSEA material, and (2) uses that information to implement remedial measures to prevent further creation of such material.

272 See, e.g., National Strategy for Child Exploitation Prevention and Interdiction, A Report to Congress, Dept. of Justicep21, https://www.justice.gov/d9/2023-06/2023_national_strategy_for_child_exploitation_prevention_interdiction_-_a_report_to_congress.pdf; See also Subject Matter Expert Working Group Report on Livestreaming and Virtual Child Sex Trafficking at 9, https://www.justice.gov/d9/2023-06/livestreaming_and_virtual_child_sex_trafficking_2.pdf ("Livestreaming platforms should pursue, and federal agencies support the development of, new technological services to detect initial captures and redistributions of livestreamed child sexual abuse online").

273 See, e.g., Apple, https://www.apple.com/newsroom/2023/05/developers-generated-one-point-one-trillion-in-the-app-store-ecosystem-in-2022/ (May 31, 2023) (as of May 31, 2023, Apple's app store had "nearly 1.8 million" apps available for download).

274 See, e.g., Minnesota Attorney General's Report on Emerging Technology and Its Effects on Youth Well-Being, at 26 (Feb. 2024), https://www.ag.state.mn.us/Office/Reports/EmergingTechnology.pdf.

275 D.. Patton, R. Eschmann, and D. Butler, "Internet banging: New trends in social media, gang violence, masculinity and hip hop." *Computers in Human Behavior*, 29(5), A54-A59.

276 "Hate Is No Game: Hate and Harassment in Online Games," *ADL* (2022): (explaining that gamers age 10-17 may experience acts of discrimination that traditional chat moderation tools may not catch such as being excluded from joining a game/chat or being "griefed" or "trolled").

277 M. Popa-Wyatt, "Reclamation: Taking Back Control of Words," (2020) (defining reclamation as "taking back control by targets of words used to attack them" and explaining that a reclaimed speech-act may be empowering rather than harmful as it strives to remove the harmful context of the initial use).

278 N. Duarte et al., "Mixed Messages? The Limits of Automated Social Media Content Analysis," at 19 (explaining how algorithms that struggle to identify socio-ethnic dialects have lower accuracy rates for those communities).

279 R. Kowert, and L. Moderation, "Challenges in digital gaming spaces: Prevalence of offensive behaviors in voice chat," *Take This* (Aug. 16, 2023): at 6 (defining the types of discriminatory speech moderated by "Tox-Mod" a resource that preemptively works to moderate chat so that users do not need to do the moderation themselves).

280 M. Al-Garadi, M. Hussain, N. Khan, G. Murtaza, H. Nweke, I. Ali, G. Mujtaba, H. Chiroma, H. Khattak, and A. Gani, "Predicting Cyberbullying on Social Media in the Big Data Era Using Machine Learning Algorithms," *Review of Literature and Open Challenges*, (2019): IEEE Access, 7, 70701–70718.

281 M. Hasan, M. Hossain, M. Mukta, A. Akter, M. Ahmed, and S. Islam, "Review on Deep-Learning-Based Cyberbullying Detection," *Future Internet, 15,* (2023): 179. https://doi.org/10.3390/fi15050179.

282 M. Dadvar, D. Trieschnigg, R. Ordelman, and F. de Jong, "Improving cyberbullying detection with user context. In Advances in Information Retrieval," Berlin, Germany: Springer, 2013, pp. 693–696.

283 National Academies of Sciences, Engineering, and Medicine, "Preventing Bullying Through Science, Policy, and Practice," *The National Academies Press*. https://doi.org/10.17226/23482.

284 H. Clayton, G. Kilmer, S. DeGue, L. Estefan, V. Le, N. Suarez, B. Lyons, and J. Thornton, "Dating Violence, Sexual Violence, and Bullying Victimization among High School Students – Youth Risk Behavior Survey," *United States*, (2021): MMWR supp. 2023:72(1).

285 U.S. Department of Education, Office of Civil Rights, "Student Discipline and School Climate in U.S. Public Schools," *ed.gov* (page 16); Last reviewed, May 16, 2024.

286 "Student Discipline and School Climate in U.S. Public Schools," *Civil Rights Data Collection, Office for Civil Rights, Department of Education*, (Nov. 2023) at 16, https://www2.ed.gov/about/offices/list/ocr/docs/crdc-discipline-school-climate-report.pdf.

287 "The Ruderman White Paper Reveals: Students with Disabilities are Almost Twice as Likely to Be Victims of Cyberbullying," *Ruderman Family Foundation* (rudermanfoundation.org) (June 2019): https://rudermanfoundation.org/white_papers/ruderman-white-paper-reveals-students-with-disabilities-are-almost-twice-as-likely-to-be-victims-of-cyberbullying/.

288 M. Al-Garadi, M. Hussain, N. Khan, G. Murtaza, H. Nweke, I. Ali, G. Mujtaba, H. Chiroma, H. Khattak, and A. Gani, "Predicting Cyberbullying on Social Media in the Big Data Era Using Machine Learning Algorithms," *Review of Literature and Open Challenges*. IEEE Access 2019, 7, 70701–70718.

289 M. Dadvar, D. Trieschnigg, R. Ordelman R, and F. de Jong, "Improving cyberbullying detection with user context." *Advances in Information Retrieval*. *Springer*, (2013): 693–696.

290 D. Finkelhor, H. Turner, and D. Colburn, "Which dynamics make online child sexual abuse and cyber-stalking more emotionally impactful: Perpetrator identity and images?," *Child Abuse & Neglect*, Volume 137, (2023): (noting the emotional impact from sexual image misuse by peers, who made up a majority of offenders in this study, was just as great as with adult offenders), https://doi.org/10.1016/j.chiabu.2023.106020

291 M. Hasan, M. Hossain, M. Mukta, A. Akter, M. Ahmed, and S. Islam, "Review on Deep-Learning-Based Cyberbullying Detection," *Future Internet,* 15, (2023): 2, 179. https://doi.org/10.3390/fi15050179 (recommending Deep learning based cyberbullying detection systems, to detect cyberbullying).

292 M. Dadvar, D. Trieschnigg, R. Ordelman, And F. de Jong, "Improving cyberbullying detection with user context. In Advances in Information Retrieval," *Springer*, (2013), pp. 693–696 (recommending the inclusion of

cyberbully specific features and terminology to detection tools to improve their capabilities).

293 N.A. Samee, U. Khan, S. Khan, M. Jamjoom, M. Sharif, D. Kim, "Safeguarding Online Spaces: A Powerful Fusion of Federated Learning, Word Embeddings, and Emotional Features for Cyberbullying Detection," In IEEE Access, vol. 11, pp. 124524-124541, 2023, doi: 10.1109/ACCESS.2023.3329347 (recommending the use of NLPs with to address cyberbullying concerns while preserving data privacy).

294 StopBullying.gov, "Bystanders to Bullying. U.S. Department of Health and Human Services," Last reviewed October 23, 2018. https://www.stopbullying.gov/bullying/effects. https://www.stopbullying.gov/prevention/bystanders-to-bullying

295 StopBullying.gov, "Cyberbullying Tactics. U.S. Department of Health and Human Services," Last reviewed May 10, 2018. https://www.stopbullying.gov/cyberbullying/cyberbullying-tactics.

296 U.S. Department of Health and Human Services, "Preventing Cyberbullying," *StopBullying.gov*. Last reviewed November 10, 2021. https://www.stopbullying.gov/cyberbullying/prevention.

297 U.S. Department of Health and Human Services, "Social Media, Apps, and Sites Commonly Used by Children and Teens," *StopBullying.gov* https://www.stopbullying.gov/cyberbullying/social-media-apps-sites-commonly-used-children-teens.

298 U.S. Department of Health and Human Services, "Cyberbullying and Online Gaming," *StopBullying.gov*. https://www.stopbullying.gov/cyberbullying/cyberbullying-online-gaminghttps://www.stopbullying.gov/cyberbullying/cyberbullying-tactics.

299 988 Suicide and Crisis Lifeline, https://988lifeline.org/. Other resources include Know2Protect hotline, NCMEC CyberTipline reporting link.

300 Take It Down website, National Center for Missing & Exploited Children, https://takeitdown.ncmec.org/

301 Pichel et. al., "Analysis of the relationship between school bullying, cyberbullying, and substance use," *Children and Youth Services* Rev. Vol. 134.

302 Pichel et. al., "Analysis of the relationship between school bullying, cyberbullying, and substance use," *Children and Youth Services* Rev. Vol. 134.

303 Kowalski et. al, "Racial Differences in Cyberbullying From the Perspective of Victims and Perpetrators," *Amer. Jour. Of Ortho*. (Identifying racial and gender differences in who perpetrates and experiences bullying).

304 Digital Wellness Lab at Boston Children's Hospital, "Creating a Positive Foundation for Greater Civility in the Digital World," *Boston Children's Hospital*. https://digitalwellnesslab.org

305 See comment on NTIA KOHS RFC from CIPLat 64 (stating services providers are recommended to "promote parental controls that respect the child's privacy and best interests), and The James Madison Institute comment at 7.

306 D. Schiano, and C. Burg, "Parental Controls: Oxymoron and Design Opportunity," *International Conference on Human-Computer Interaction*, (2017): https://link.springer.com/chapter/10.1007/978-3-319-58753-0_91.

307 Comment on NTIA KOHS RFC from FOSI ("Parents are overwhelmed by the many different types of parental controls, where to find them, how to use them, and what the tools do."), Comment of ESA (stating that video game platforms and video games have their own parental control tools.)

308 L. Clark, "Digital Media and the Generation Gap: Qualitative research on U.S. teens and their parents," Information, Communication, and Society, 12(3), 388-407, and Rasi, P.R., Vuojärvi, H., and Ruokamo, H., "Media

Literacy Education for All Ages," Journal of Media Literacy Education, 11(2) 1-19, 2019, and LGBT Tech comment (noting "parental control requirements that strip youth of any autonomy in their online experiences and therefore isolate or out LGBTQ+ youth").

309 See comment on NTIA KOHS RFC from American Academy of Pediatrics (stating "the effects of social media on well-being are nested within family relationships and household dynamics, and one size-fits all mandatory parental control over teen media use is not developmentally appropriate for many families.").

310 See comment on NTIA KOHS RFC from American Academy of Pediatrics.

311 See comment on NTIA KOHS RFC from 5 Rights at 2. (noting parental controls do not adequately address the problem as they are unable to address issues related to the interactivity of digital products and services).

312 See generally Google Families | Empowering kids to safely connect, play, and learn online, and Tips for Parents on Helping Your Teen Stay Safe on Discord

313 See, e.g., comment on NTIA KOHS RFC from Future of Privacy Forum (FPF)(pointing to some options where kids under age 13 have strict default settings, which can include "the disabling of purchasing, email marketing or push notifications, custom display names, communications with players using voice chat or free text chat, and recommendations based on past activity").

314 Comment on NTIA KOHS RFC from Entertainment Software Association ("ESA") at 8 (re in-game communications). For other measures, see, Tips for Parents on Helping Your Teen Stay Safe on Discord.

315 See, e.g., comment on NTIA KOHS RFC from Future of Privacy Forum (FPF)Comment of American Academy of Pediatrics on NTIA KOHS RFC and Tips for Parents on Helping Your Teen Stay Safe on Discord

316 Comment on NTIA KOHS RFC from American Academy of Pediatrics.

317 Comment on NTIA KOHS RFC from Roblox at 11.

318 Comment on NTIA KOHS RFC from #Shepersistedat 3 ("Platform design choices that impact minors specifically, such as ineffective parental control mechanisms, photo filters that alter a user's physical appearance, a lack of mechanisms for restricting time spent on platforms, not providing labels for filtered content, weak systems for age verification, ineffective reporting systems for predatory accounts, and difficulties surrounding account deletion are examples of fair territory for oversight.)"

319 See Comment on NTIA KOHS RFC from #Shepersisted at 3.

320 See Comment on NTIA KOHS RFC from #Shepersisted at 3.

321 105-2 Hearing: S. 2326, Children's Online Privacy Protection Act Of 1998 comment from then FTC Chairman Robert Pitofsky (stating "the practice of collecting personal identifying information directly from children without parental consent is clearly troubling, since its [sic] teaches children to reveal their personal information to strangers and circumvents parental controls over their family's information."). While the circumstances have changed since COPPA has passed, the sentiment remains the same: where parental controls are used, requests for access to youth data should go through parental control platforms.

322 See comment on NTIA KOHS RFC from Future of Privacy Forum (FPF).

323 See NTIA KOHS RFC ESA comment (stating "Understanding a game's features and its age appropriateness begins before a caregiver purchases or downloads a game.) I.e. Social media and online platforms should learn from video games and provide proactive, easy to understand information about their features and age appropriateness.

324 See NTIA KOHS RFC App Association comment at 5 (stating "enabl[e] parental control settings on

their children's devices to make sure they do not have access to inappropriate information and reading privacy policies that the child likely does not understand due to their age.").

325 C. Vogus, T. Greene, D. Martens, and G. Shmueli, "Improving Researcher Access to Digital Data: A Workshop Report," *Center for Democracy & Technology*, (2021)

326 T. Greene, D. Martens, and G. Shmueli, "Barriers for Academic Data Science Research in the New Realm of Behavior Modification by Digital Platforms," (October 20, 2021).

327 National Academies of Sciences, Engineering, and Medicine, "Social Media and Adolescent Health," *The National Academies Press.* https://doi.org/10.17226/27396.

328 "Edmo Releases Report on Researcher Access to Platform Data." EDMO. Accessed July 19, 2024. https://edmo.eu/edmo-news/edmo-releases-report-on-researcher-access-to-platform-data/

329 Transparent and accountable online platforms | Shaping Europe's digital future (europa.eu).

330 Status Report: Mechanisms for Researcher Access to Online Platform Data | Shaping Europe's digital future (europa.eu)

331 Pew Research Center, "Teens, Social Media and Technology," 2023, https://www.pewresearch.org/internet/2023/12/11/teens-social-media-and-technology-2023/.

332 See, e.g., https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa. See also state laws, such as California regulations protecting data about minors under the age of 16, ARTICLE 6. https://cppa.ca.gov/regulations/pdf/cppa_regs.pdf

333 S. Prasad, S. Souabni, G. Anugwom, K. Aneni, A. Anand, A. Urhi, and F. Oladunjoye, "Anxiety and depression amongst youth as adverse effects of using social media: A Review," *Annals of Medicine and Surgery*, 85(8), (2023), 3974-3981.

334 B. Keles, N. McCrae, and A. Grealish, "A systematic review: the influence of social media on depression, anxiety and psychological distress in adolescents," *International journal of adolescence and youth*, 25(1), (2020): 79-93

335 M. Selfhout, S. Branje, M. Delsing, T. ter Bogt, and W. Meeus, "Different types of Internet use, depression, and social anxiety: The role of perceived friendship quality," *Journal of Adolescence*, 32(4), (2009): 819-833.

336 J. Nesi, and M. Prinstein, "Using social media for social comparison and feedback-seeking: Gender and popularity moderate associations with depressive symptoms," *Journal of Abnormal Child Psychology*, 43, (2015): 1427-1438.

337 E. Swedo, J. Beauregard, S. de Fijter, L. Werhan, K. Norris, M. Montgomery, and S. Sumner, "Associations between social media and suicidal behaviors during a youth suicide cluster in Ohio," *Journal of Adolescent Health*, 68(2), (2021): 308-316.

338 N. Macrynikola, E. Auad, J. Menjivar, and R. Miranda, "Does social media use confer suicide risk? A systematic review of the evidence," *Computers in Human Behavior Reports*, 3, (2021): 100094.

339 Office of the Surgeon General (OSG), "Protecting Youth Mental Health: The U.S. Surgeon General's Advisory," *US Department of Health and Human Services*; 2021 at 27.

340 C. Hoffmann, C. Lutz, C., and G. Ranzini, "Privacy cynicism: A new approach to the privacy paradox," *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 10(4), (2016): https://doi.org/10.5817/CP2016-4-7

341 O. Albuquerque, M. Fantinato, J. Kelner, and A. de Albuquerque, "Privacy in smart toys: Risks and proposed solutions," *Electronic Commerce Research and Applications*, 39, (2020): 100922. https://doi.org/10.1016/j.elerap.2019.100922.

342 A. Sunyaev, "The Internet of Things," *Internet Computing,* (2020): pp. 301–337. Springer International Publishing. https://doi.org/10.1007/978-3-030-34957-8_10.

343 J. Geng, D. Huang, and F. De la Torre, (2022) DensePose From WiFi. http://arxiv.org/abs/2301.00250.

344 Terms of Use, OpenAi, (Jan. 31, 2024) https://openai.com/policies/terms-of-use/.

345 T. West, "Children's Privacy: An Evaluation of EdTech Privacy Policie," *Proceedings of the Conference on Information Systems Applied Research*, (2022): 1–12.

346 See V. Zhong, S. McGregor, and R. Greenstadt, (2023). I'm going to trust this until it burns me" Parents' Privacy Concerns and Delegation of Trust in K-8 Educational Technology. 32nd USENIX Security Symposium, USENIX Security 2023, 5073–5090, and The Federal Trade Commission 2023 Privacy and Data Security Update Fed. Trade Comm., 2023, at 30 (affirming previous guidance that ed tech providers that rely upon a school's authorization to collect children's personal information are permitted to use the information only for the school-authorized educational purpose and not for other commercial purposes, including marketing or advertising. The COPPA NPR, among other things, proposes to codify that guidance and to require schools to have written agreements with ed tech providers in accord with the COPPA).

347 Social media and adolescent mental health: A consensus report of the National Academies of Sciences, Engineering, and Medicine PNAS Nexus, 2024, 3, 1–3. https://doi.org/10.1093/pnasnexus/pgae037 Advance access publication 27 February 2024

348 S. Landau, and P. Leon, "Reversing Privacy Risks: Strict Limitations on the Use of Communications Metadata and Telemetry Information," *Colo. Tech*. (2023): LJ, 21, p.225.

349 E. Dick, "Balancing user privacy and innovation in augmented and virtual reality," *Information Technology and Innovation Foundation* (2021).

350 Y. Fan, S. Lehmann, and A. Blok, "New methodologies for the digital age? How methods (re-)organize research using social media data," *Quantitative Science Studies* (2023); 4 (4): 976–996. doi: https://doi.org/10.1162/qss_a_00271

351 T. Katapally, "The SMART framework: Integration of citizen science, community-based participatory research, and systems science for population health science in the digital age," *JMIRmHealth and uHealth*, 7, (2019): e14056

352 For example, the "Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse", We-Protect Global Alliance (Mar. 5, 2020): https://www.weprotect.org/library/voluntary-principles-to-counter-online-child-sexual-exploitation-and-abuse/.

353 "Safety by Design for Generative AI: Preventing Child Sexual Abuse", *Thorn* (2024), https://info.thorn.org/hubfs/thorn-safety-by-design-for-generative-AI.pdf.

354 "Best Practices Framework," *Digital Trust & Safety Partnership* (2021): https://dtspartnership.org/best-practices/.

355 Health professionals, including specialists in child development; child advocacy center professionals; privacy, civil liberties, and civil rights experts; parents, children and teenagers; scholars, civil society, and technologists and engineers with expertise in mental health and the prevention of harms to minors, behavioral economics and harm avoidance, teens use of social media, and persuasive design; elementary and secondary school educators and administrators; representatives of online platforms, including product designers, and

other industry as appropriate; state attorneys general; representatives of communities of socially disadvantaged individuals; and U.S. international partners.

356 Initiative To Protect Youth Mental Health, Safety & Privacy Online," Federal Register 88, no. 189 (October 2, 2023): 67733 https://www.regulations.gov/document/NTIA-2023-0008-0001

357 National Telecommunications and Information Administration. "NTIA Receives More Than 500 Comments on Protecting Kids Online." Press Release, November 30, 2023. https://www.ntia.gov/press-release/2023/ntia-receives-more-500-comments-protecting-kids-online.

358 National Telecommunications and Information Administration. "Statement of Assistant Secretary Davidson on the White House Kids Online Health & Safety Listening Session." Press Release, January 30, 2024. https://www.ntia.gov/press-release/2024/statement-assistant-secretary-davidson-white-house-kids-online-health-safety.

359 See GoodforMEdia https://www.goodformedia.org/learn/events/whitehouse-kids-online-safety-task-force-sessionand Unwiring https://www.unwiring.org/.

360 National Telecommunications and Information Administration. "NTIA Joins Stanford University to Advance Kids' Online Safety." Press Release, March 13, 2024. https://www.ntia.gov/press-release/2024/ntia-joins-stanford-university-advance-kids-online-safety.

361 The White House, "FACT SHEET: Biden-Harris Administration Announces Actions to Protect Youth Mental Health, Safety & Privacy," (May 23, 2023): https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/23/fact-sheet-biden-harris-administration-announces-actions-to-protect-youth-mental-health-ine/.

Page intentionally left blank.