

Before the
National Telecommunications and Information Administration
Washington, D.C.

In re

Initiative to Protect Youth Mental Health,
Safety, & Privacy Online

Docket No. 230926-0233

**COMMENTS OF
THE COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION (CCIA)**

In response to the request for comment (“RFC”) published in the Federal Register at 88 Fed. Reg. 67733 (Oct. 2, 2023), the Computer & Communications Industry Association (“CCIA”)¹ submits the following comments. CCIA appreciates the opportunity to provide input on these important issues and applauds the National Telecommunications and Information Administration’s (“NTIA” or the “Agency”) efforts to better understand the intersection of online platforms and youth health, safety, and privacy online.

I. Introduction

Young people increasingly rely on countless digital tools and services for daily aspects of their lives. Children and teens can use these different online platforms and services to enrich their educational experiences, foster healthy social interactions with friends, and engage with a wide range of content that is of interest to them. Such opportunities have paved the way for positive youth-led experiences and movements like the March for Our Lives. Although such online platforms and services may attract bad and malicious actors who seek to cause further division and harm, this risk is not unique to social media and exists across the digital ecosystem. Despite the array of challenges online services and platforms face in addressing these risks of harm, CCIA and its members continue to invest in tools and resources to prevent and mitigate

¹ CCIA is an international, not-for-profit trade association representing a broad cross section of communications and technology firms. For more than 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than \$100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. For more, visit www.ccianet.org.

such harms. Below, we outline some considerations for the Agency as it develops a path forward to keeping kids and teens safe online.

First, any approach must recognize and account for the inherent differences among online platforms and services. While policymakers hope an overarching solution will emerge to address all the risks associated with online services and platforms, there is no panacea for keeping young users safe across the diverse internet ecosystem. Any potential framework for youth online safety needs to have a risk-based approach that enables organizations to take the necessary actions in light of the evolving risks and dangers most relevant to their specific environment and users.

Second, any approach must account for the rights and needs of all users, especially concerning their First Amendment rights. An approach must consider the effects broad requirements like an age verification mandate would have upon all users — even more so for users from vulnerable communities. Various state and federal legislative efforts aimed at youth online safety contain provisions and requirements that would cause more harm than good. Recently, LGBT Tech and 73 other organizations and LGBTQ+ centers from around the country sent a letter to over 100 lawmakers in Congress to express concerns about the Kids Online Safety Act, particularly regarding the broad duty of care mandate.²

Lastly, any approach must be tailored to address specific, concrete harms so that online platforms and services can actually operationalize any relevant requirements. Several legislative efforts impose broad mandates that seek to address a wide range of potential harms, which only creates uncertainty and risk for businesses and users.³ As noted in the RFC, more research is needed to understand this relationship and to determine what harms there are, if any, and how to best mitigate them. Ultimately, practical solutions can only go so far, and there is a pressing need for a better overarching framework.⁴ CCIA believes an alternative to solving these complex issues is for lawmakers to work with all stakeholders, including younger users, families, and

² LGBT Tech, *LGBTQ+ Organizations and Centers Send Letter to Hill Urging Changes to Kids Online Safety Bill* (Nov. 2, 2023), <https://www.lgbttech.org/post/lgbtq-organizations-and-centers-send-letter-to-hill-urging-changes-to-kids-online-safety-bill>.

³ See Report, CCIA, *2023 State Privacy Landscape*, (Nov. 8, 2023), <https://ccianet.org/library/ccia-2023-state-privacy-landscape/>.

⁴ Daniel Castro, *The Privacy Panic Cycle: A Guide to Public Fears About New Technologies*, ITIF (Sept. 2015), <https://www2.itif.org/2015-privacy-panic.pdf>.

private businesses to promote a whole-of-community approach that ensures the internet and related mediums remain a powerful force for good for generations to come.

II. Identifying the Health, Safety, and Privacy Risks and Benefits for Children and Teens from the Use of Online Platforms and Services

A. Question 1

Leading online platforms want users to have a safe and enjoyable online experience.⁵ To do so, organizations must consistently invest in various tools and resources to identify and address the evolving threats facing their platforms and users. From accessing Wikipedia to learn about a solar eclipse to searching YouTube for a tutorial on how to cook the perfect scrambled eggs, “adults and children frequently use the same online platforms.”⁶ This is why any efforts to address the risks associated with online platforms and services need to be focused on preventing and mitigating specific, actual harms.

Regarding the current risks of harm, a trending claim is that social media negatively impacts an individual’s well-being, despite the lack of sufficient evidence to support this conclusion.⁷ In fact, the Oxford Internet Institute released a recent study on the impact of Facebook on well-being that found the opposite. In its August report, the researchers found “no evidence that the social media platform’s worldwide penetration is linked to widespread psychological harm.”⁸ Moreover, the frequently cited Surgeon General’s report on social media and youth mental health continues to be framed as if harm is a foregone conclusion — an assertion not supported by the evidence, which paints a much more complex picture.⁹ This stands

⁵ See Report, CCIA, *Hate Speech & Digital Ads: The Impact of Harmful Content on Brands*, (Sept. 5, 2023), <https://research.ccianet.org/reports/hate-speech-digital-ads-impact/> (research found that “online hate speech harms both the companies advertising alongside the content and the apps and websites hosting it.”)

⁶ RFC at 67734.

⁷ Aaron Brown, *The Statistically Flawed Evidence That Social Media Is Causing the Teen Mental Health Crisis*, Reason (Mar. 29, 2023), <https://reason.com/2023/03/29/the-statistically-flawed-evidence-that-social-media-is-causing-the-teen-mental-health-crisis/>.

⁸ Andrew Przybylski & Matti Vuorre, *No evidence linking Facebook adoption and negative well-being: Oxford study*, Oxford Internet Institute (Aug. 9, 2023), <https://www.oii.ox.ac.uk/news-events/news/no-evidence-linking-facebook-adoption-and-negative-well-being-oxford-study/>.

⁹ See Mike Masnick, *A Deeper Look At The Surgeon General’s Report On Kids & Social Media: It’s Not What You Heard*, Techdirt (May 30, 2023),

in contrast with the evidence put forth in a 2023 American Psychological Association “Health Advisory on Social Media Use in Adolescence”, which found that “using social media is not inherently beneficial or harmful to young people.”¹⁰

To be clear, social media and online platforms carry risks of harm to users that warrant additional protections — evidenced by leading technology companies implementing robust content moderation policies and adhering to best practices such as those outlined by the Digital Trust & Safety Partnership. But these potential concerns should not give way to the re-introduction of regressive approaches seen with past moral panics targeting comic books, television, and video games.¹¹ Otherwise, restrictive proposals such as those that seek to condition internet access upon the sharing of personal information will impose the same heavy costs seen with past moral panics — disproportionately harming individuals from vulnerable and marginalized communities.¹²

B. Question 1(c)

Technology companies continue to work with a wide range of stakeholders to advance online safety but these tools and features are ineffective if parents and children are unaware of them and more importantly, how to use them effectively. This is why CCIA’s members have invested a great deal of time and energy in public awareness campaigns to inform both parents and younger users about these beneficial features and tools. For example, Google provides a comprehensive guide for families, along with describing important steps to keeping one’s kids and teens safe online.¹³ These measures include creating a supervised account for kids, setting the right parental controls for one’s family, and finding balance with technology online.

<https://www.techdirt.com/2023/05/30/a-deeper-look-at-the-surgeon-generals-report-on-kids-social-media-its-not-wh-at-you-heard/>.

¹⁰ American Psychological Association, *Health Advisory on Social Media Use in Adolescence* (May 2023), <https://www.apa.org/topics/social-media-internet/health-advisory-adolescent-social-media-use>.

¹¹ Alvaro Marañón & Dalia Wrocherinsky, *Public Panics and Youth Online Safety – A Deep Dive*, Disruptive Competition Project (July 7, 2023), <https://www.project-disco.org/featured/public-panics-and-youth-online-safety-a-deep-dive/>.

¹² The public panic around comic books “resulted in the censorship of minority identities in fiction, ruined the careers of authors and illustrators, and drove many young people away from the stories that spoke to them.” Jeremy C. Young and Jonathan Friedman, *Today’s book bans echo a panic against comic books in the 1950s*, Washington Post (Oct. 17, 2022), <https://www.washingtonpost.com/made-by-history/2022/10/17/book-ban-comic-books-panic/>.

¹³ Google Families, *Empowering Your Family*, (last accessed Nov. 7, 2023), <https://families.google/>.

However, this is a shared responsibility, and public officials have already begun informing parents and teachers so they can teach children safe online behaviors. North Carolina Attorney General Josh Stein has introduced a campaign that provides tools to help parents start a conversation with their children about internet safety, and explain to parents and educators what security controls are already in place on many of these digital devices and services, and other useful tactics and tools to help parents make the best decisions regarding online use by their children.¹⁴

C. *Question 1(h)*

The development and use of artificial intelligence and similar technologies has been a tremendous benefit for users and has helped platforms alleviate a wide range of evolving challenges and risks of harm. Preventing online grooming and detecting child sexual exploitation (CSE) and child sexual abuse materials (CSAM) continues to be one of the most pressing challenges facing society today. The industry is actively researching methods and interventions to stop and prevent the creation of new CSAM. Just last week, the Tech Coalition announced the first cross-platform signal sharing program for companies to strengthen how they enforce their child safety policies and to help collaborate against “predatory actors evading detection across services.”¹⁵ Further, the number of CSAM reports and removals has increased in recent years, demonstrating that multiple industries’ investment in these technologies has helped find, remove, and report this obscene material.¹⁶ Pinterest, Google, Meta, and other responsible online platforms actively identify CSE content by leveraging their internal tools and shared industry tools such as PhotoDNA, which uses a shared industry hash database of known CSAM, and CSAI Match (an API that helps identify re-uploads of previously identified child sexual abuse

¹⁴ NCDNJ, *Protect Kids on the Internet*, (last accessed Nov. 2, 2023), <https://ncdoj.gov/internet-safety/protect-kids-on-the-internet/>.

¹⁵ Tech Coalition, *Announcing Lantern: The First Child Safety Cross-Platform Signal Sharing Program*, (Nov. 7, 2023), <https://www.technologycoalition.org/newsroom/announcing-lantern>.

¹⁶ Thorn, *New Report Shows an Increased Effort by Tech Companies to Detect CSAM on the Internet* (Mar. 18, 2022), <https://www.thorn.org/blog/new-report-shows-an-increased-effort-by-tech-companies-to-detect-csam-on-the-internet/>. (NCMEC’s recent CyberTipline report is “encouraging . . . The report shows that 230 companies across the globe are now deploying tools to detect child sexual abuse material. That’s a remarkable 21% increase since 2020. The significant uptick in the number of platforms that detect child sexual abuse material has led to more reports being filed and more CSAM hashes created, helping make the fight against the viral spread of abuse material ever more effective.”)

material in videos) to identify video content. These technology companies also work closely with the National Center for Missing and Exploited Children (NCMEC) to combat this type of activity, and report content violations as required under the law. From January to June 2022, Pinterest's team of specialists was responsible for 4,969 CyberTipline reports to NCMEC.¹⁷

AI and related technologies have been helpful in other contexts. One of CCIA's members, Pinterest, has been using AI to create a safer and healthier online environment for their users. As part of their efforts around the prevention of self-harm, Pinterest created a compassionate search function. If a user searches for terms related to suicide, self-harm, or depressive quotes, Pinterest redirects them to mental health resources like the National Suicide Prevention Hotline.¹⁸ To create a more inclusive and representative platform, Pinterest implemented a few updates to its search function. The company's changes to skin tone ranges allow users to refine and customize their searches so they will see results and other content that is representative of them. The updated hair pattern search also allows users to refine their search by six different hair patterns, along with the skin tone ranges, creating an opportunity for users to see themselves in the product.¹⁹ Lastly, Pinterest's body type technology uses shape, sizes, and form to identify various body types in over 5 billion images on the platform, leveraging its inclusive AI to increase representation across the related feeds and search results.²⁰ These are just a few of the ways leading online platforms are utilizing AI and related technologies to foster and maintain a healthier online environment for minors and teens.

The RFC also asks how the specific application of emerging technologies exacerbates certain harms or risks of harm to young people. Similar to how any proposed solution must account for the risks specific to that online platform or service, the cost and trade-offs to users and businesses need to be considered as well. For instance, states continue to propose device-level content filtering mandates despite the serious concerns around compliance,

¹⁷ Pinterest, Transparency Report (2022), <https://policy.pinterest.com/en/transparency-report>.

¹⁸ Pinterest, *Introducing a More Compassionate Search Experience for People in Distress* (July 19, 2019), <https://newsroom.pinterest.com/post/introducing-a-more-compassionate-search-experience-for-people-in-distress/>.

¹⁹ Dashia Milden, *Pinterest launches new hair pattern search for 'inclusive beauty results'*, CNET (Aug. 18, 2021), <https://www.cnet.com/tech/pinterest-launches-new-hair-pattern-search-for-inclusive-beauty-results/>.

²⁰ Newsroom, Pinterest, *Industry-first body type technology to increase body representation on platform* (Sept. 7, 2023), <https://newsroom.pinterest.com/news/pinterest-announces-industry-first-body-type-technology/>.

enforcement, and constitutionality.²¹ These concerns also extend to the rise of mandated age-verification and similar technologies. Such measures impose heavy costs upon users and businesses, yet they continue to be a common element in many online safety bills.²²

Consider an age-verification mandate that raises the age requirement to obtain verifiable parental consent before accessing any online platform from 13 to 17. Compliance would force businesses to collect even more sensitive information about users, conflicting with the data minimization principles found in many leading privacy best practices. Moreover, such proposals also require online platforms to accurately verify whether a “parent or guardian” is that specific minor’s legal parent or guardian. Many parents and legal guardians do not share the same last name as their children due to remarriage, adoption, or other cultural or family-oriented decisions. Further, some households are not proficient in English, are not technologically savvy, or work multiple jobs. This raises serious equity concerns, especially considering those households that lack the necessary government identification or other mechanisms to access an online service or platform — blocking teens from accessing helpful services and age-appropriate information.

As the Agency continues to evaluate various proposals and methods, CCIA would like to reiterate that current age verification technology still faces technical challenges and likely undermines the safety and privacy of its users. Notably, the Commission Nationale de l’Informatique et des Libertés (CNIL) analyzed several existing online age verification solutions, finding that none of these options could sufficiently meet three key standards: providing sufficiently reliable verification; allowing for complete coverage of the population; and respecting the protection of individuals’ data, privacy, and security.²³ Age verification requirements carry serious risks and concerns but less intrusive methods like age assurance could contribute to online safety if its use is limited to high-risk services such as platforms that offer

²¹ Josh Withrow, *Device-Level Content Filter Mandates Defy Common Sense and the Constitution*, R Street Institute, (June 1, 2023),

<https://www.rstreet.org/commentary/device-level-content-filter-mandates-defy-common-sense-and-the-constitution/>.

²² See Ben Sperry, *Op-Ed: State children's online safety laws fail to help parents protect their teens*, The Center Square (Apr. 21, 2023),

https://www.thecentersquare.com/opinion/article_eb34688c-e04d-11ed-810e-53be8c61726b.html.

²³ CNIL, *Online age verification: balancing privacy and the protection of minors* (Sept. 22, 2022),

<https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors>.

gambling, pornography, or alcohol, and the requirements adhere to other important considerations and safeguards.²⁴

D. Question 3

Recent headlines have largely fixated on the potential risks of harm associated with social media and online platforms, however, the documented and growing benefits provided by such technologies continue to receive little to no attention. A unique strength of the internet is that it opens so many doors for countless people with different socio-economic backgrounds. Future innovation and social progress rest on these generations, and while all the benefits may not be immediately known, the return in the long run for allowing the younger generation to learn about new topics or get involved in local social causes is immeasurable.

Social media has been found to encourage collaborative learning that teaches children and teens about the importance of appreciating different perspectives and views to better understand the world. This in turn helps spark their curiosity and discover areas of interest to them. Social media has also played an important role in digital media literacy. Importantly, Boston Children’s Digital Wellness lab found that it is critical to help kids learn to navigate digital spaces on their own.²⁵ Social-emotional skills like empathy, kindness, and personal responsibility, which are crucial for offline interactions, can also be taught to enhance online interactions. Even for younger children, character education through digital citizenship is gaining traction in practice. According to a study on school children in the United States, 62% of K-2 teachers and 69% of grade 3-5 teachers report using some digital citizenship curriculum, with competencies related to developing positive character features being most common, such as understanding cyberbullying and hate speech.²⁶

Social media and online platforms also provide important tools and resources for youth mental health and well-being, especially those teens from vulnerable communities. The Surgeon

²⁴ See 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.

²⁵ Elizabeth Hunt, *Research brief: Digital Citizenship and Media Literacy*, The Digital Wellness Lab, <https://digitalwellnesslab.org/research/research-brief-digital-citizenship-and-media-literacy/> (last accessed Sept. 5, 2023).

²⁶ Alexis Lauricella, Jenna Herdzina, Michael Robb, *Early childhood educators’ teaching of Digital Citizenship Competencies*, *Computers & Education* (Dec. 2020), <https://www.sciencedirect.com/science/article/abs/pii/S0360131520301871>.

General’s Report notes that social media has profoundly positive effects on LGBTQ and minority female youths in particular, “enabling peer connection, identity development and management, and social support.” Further, “a majority of adolescents report that social media helps them feel more accepted (58%), like they have people who can support them through tough times (67%), like they have a place to show their creative side (71%), and more connected to what’s going on in their friends’ lives (80%).”

As mentioned in the RFC, social media is an important safe space for many young people, allowing them to have a space for self-expression, develop social skills, and education. Online spaces have been found to play a crucial role in the identity formation and resilience of LGBT, racial and ethnic minority adolescents.²⁷ Further, it has been found that LGBT teenagers are more likely than non-LGBT teenagers to search online for information about sexuality or sexual attraction (62% vs. 12%), health and medical information (81% vs. 46%), and sexual health information (19% vs. 5%).²⁸ Despite the evidence of social media’s benefits and importance to teens, recent legislative proposals aimed at vague harms could jeopardize the safe spaces and important connections social media creates for these young people. For example, it could extend to the efforts of the Trevor Project, which created an online, moderated community for LGBTQ young people to help them explore their identity, get advice and help, find support, make friends, and more.²⁹

E. Question 5

As previously mentioned, a whole-of-community framework is needed to create safer online environments for all. Children and teens need to be involved in this important process as their experiences with current efforts and “solutions”, both positive and negative, need to be heard.

²⁷ See Linda Charmaraman, J. Maya Hernandez, Rachel Hodes, *Marginalized and Understudied Populations Using Digital Media* in Handbook of Adolescent Digital Media Use and Mental Health (2022), <https://www.cambridge.org/core/books/handbook-of-adolescent-digital-media-use-and-mental-health/marginalized-and-understudied-populations-using-digital-media/11A8E212846491FFEA02A32EAFDC401E>.

²⁸ Gay, Lesbian & Straight Education Network, *Out Online: The Experiences of Lesbian, Gay, Bisexual and Transgender Youth on the Internet* (July 10, 2013), https://www.glsen.org/sites/default/files/2020-01/Out_Online_Full_Report_2013.pdf.

²⁹ Since its creation, the Trevor Project has become an essential ally in the efforts around suicide prevention among LGBTQ youth, fielding hundreds of thousands of calls from young people in crisis. Trevor Project, *Visit Trevorspace*, (2023), <https://www.thetrevorproject.org/visit-trevorspace/>.

For example, consider addressing these risks and challenges facing young users in the educational context. The use and deployment of third-party tracking services appeared to some to be a potential solution to remote learning, promising a better way to help teachers and parents protect students from bullying, engaging in dangerous acts, and more. Despite its popular appeal, the student experience has not aligned with this vision. Last October, a high school student described their experience with a popular monitoring service being used in over 2,300 school districts. The student highlighted the various shortcomings and costs associated with the monitoring software, “... it functions at the cost of struggling students being prohibited from accessing the information they need online. The desire for convenience and control over students seem to overshadow the importance of privacy in classrooms.”³⁰

However, not every approach needs to impose such high costs. This is why CCIA supports the implementation of a digital citizenship curriculum in schools, which would both educate children on proper social media use and empower parents by informing them of what mechanisms are already out there that they can use now to protect their children the way they see fit and based on their family’s lived experiences.³¹ Given the complexity of tackling this critical issue, existing industry efforts coupled with educational curricula focused on how to be a good citizen online can have positive impacts. Offering such education to children would provide a more holistic approach to fostering children’s online safety. Enabling young people to properly identify and respond to such behavior would promote safer online habits.

III. Information on the Status of Industry Efforts and Technologies

A. Question 6

As discussions of child online safety and privacy continue, responsible social media companies and online platforms are working jointly and independently to advance online safety.

³⁰ Genie Tang, *Opinion: Bark Technologies, the dangers of third-party trackers for children*, Los Angeles Times, (Oct. 12, 2022), <https://highschool.latimes.com/troy-high-school/opinion-bark-technologies-the-dangers-of-third-party-trackers-for-children/>.

³¹ Edward Longe & Will Flanders, *A better way to protect teenagers online*, Wisconsin State Journal (Aug. 25, 2023), https://madison.com/opinion/column/a-better-way-to-protect-teenagers-online---will-flanders-and-edward-longe/article_683a2b94-42f2-11ee-9a79-a32fcbd2fedb.html.

These timely undertakings include joint work in organizations such as the Technology Coalition, and the Family Online Safety Institute, among others, whose collective efforts promote child safety online and provide resources for parents to foster safer digital experiences for young persons. Any proposal for youth online safety must consider the inherent differences and challenges between each online service and platform. A risk-based approach would ensure that the efforts each company takes, including developing products and tools specifically tailored to their organization, are not unnecessarily undermined. To highlight the myriad of approaches taken by different online platforms and services, below we describe a few of the mechanisms implemented by digital services and other social media websites that minors may use.³²

Discord. This online service added a channel setting that allows the user to designate one or more text channels in their server as age-restricted. Anyone who opens the channel will be greeted with a notification informing them that it might contain age-restricted material and asking them to confirm that they are over 18. Any content that cannot be placed in an age-gated channel, such as avatars, server banners, and invites splashes, cannot also contain age-restricted content. Discord also has a safety center dedicated to parents and educators detailing how to approach online safety with children and what resources the service has to offer to keep them safe when using Discord.

YouTube. This digital service has created YouTube Kids, which is a separate app with tools for parents and caregivers to guide their child's online activity. The app is a filtered version of YouTube and has a much smaller set of content available than YouTube's main app and website. Moreover, the data from anyone watching content identified as 'made for kids' on YouTube is treated as coming from a child, regardless of the age of the user, limiting data collection and use while also restricting or disabling some product features native to YouTube. This includes not serving personalized ads on content 'made for kids' and disabling features like comments and notifications. YouTube also has a Youth and Families Advisory Committee composed of experts in children's media, child development, digital learning, and citizenship from a range of academic, non-profit, and clinical backgrounds. This committee weighs in on products, policies, and services YouTube offers to young people.

³² CCIA, *What Tools are Available to Families and Young People Online* (2023), https://ccianet.org/wp-content/uploads/2023/02/General-Child-Safety-Mechanisms_Fact-Sheet.pdf.

Instagram. This online service also has a multifaceted approach to child safety online. Their Parent’s Guide and Family Center include resources for parents and allow for a tailored approach for parents to make sure their teens are exploring the app safely. Parents and guardians or teens can also send requests to initiate supervision to help build positive online habits together. Instagram has also recently launched two new features to combat the possibility of “social media addiction” — Take a Break and Daily Limit. Take a Break will remind users to stop using the app if it has been open for a long time without closing it. The Daily Limit feature reminds users to close Instagram once they have used it to their personally set standard of “too much” in a single day.

Amazon. This digital service created Amazon Kids, a separate service that helps parents manage their children’s interaction with technology and provides kids with a safe place to enjoy age-appropriate content. This dedicated service also includes various strict guidelines that include requiring parental consent from all customers before enabling Amazon Kids on Alexa, prohibiting all kid skills in Amazon Kids+ from collecting personal information, and multiple mechanisms to delete a child’s profile and recording. Amazon also provides the free Parent Dashboard which makes it easy for adults to manage a child’s screen time and digital content in one central place.³³ Parents can log in at any time to control and track what children are doing online on up to four individual child profiles across multiple devices. Usage information – including books, videos, skills, and apps – is displayed for at-a-glance review.

Apple. This technology company employs expanded efforts across many different facets of its technology to ensure child safety. Mechanisms like communication safety in their Messages app and expanded guidance in Siri and Safari search have most recently been implemented. Communication safety in Messages is only available for accounts set up as families in iCloud. Parent or guardian accounts must opt-in to turn on the feature for their family group, and notifications can be enabled by parents or guardians for child accounts aged 12 or younger. Apple also uses different age-based presets that help parents from the start such as preventing the 11-year-old from watching a PG-13 movie.³⁴ Content and Privacy Restrictions in

³³ Blog, Amazon, *Discover entertainment and education parents can trust with Alexa*, (June 15, 2022), <https://www.aboutamazon.com/news/devices/discover-entertainment-and-education-parents-can-trust-with-alexa>.

³⁴ Support, Apple, *Use parental controls on your child's iPhone, iPad, and iPod touch*, (last accessed Nov. 3, 2023), <https://support.apple.com/en-us/HT201304>.

Screen Time also allow parents to block or limit specific apps and features on their child's device. Users can also restrict the settings on their iPhone, iPad, or iPod touch for explicit content, purchases and downloads, and privacy.

B. Question 10

Online platform services are diverse, playing varying roles and functions. Any approach needs to take into account the diverse roles played by online platforms and services, tailoring the requirements to what is appropriate and technically feasible. Therefore, a risk-based approach is needed that accounts for differences in each platform and online services.

Design elements will vary with each company as well, as the needs and risks differ greatly. If a service allows the spread of unfiltered content, it can create dangerous environments for disinformation campaigns that help spread bias and fear. But such risks of harm are not isolated to only social media, other platforms like video games also present various risks of harm to young users. The Federal Trade Commission's recent complaint against Epic Games, creator of the popular video game Fortnite, illustrates the reality of such dangers. The FTC alleged that the company's settings enabled "live on by-default text and voice communication for users", which coupled with the random matchmaking function of the game, meant children and teens were meeting and interacting with strangers of all ages — children and teen users reported bullying, threats, harassment, and exposure to traumatizing issues while playing the game.³⁵ Any proposed solution needs to be tailored to the potential underlying risk to children and teens posed by a particular platform or service.

C. Question 12

Creating a workable approach to address the online safety of children and teens is a dynamic challenge. A successful approach needs to avoid being overly prescriptive so it can respond to new and emerging risks of harm and must respect the inherent differences between children and teens to avoid imposing new and future harms. As noted in the Surgeon General report, "[i]n most cases, the effects of social media are dependent on adolescents' own personal

³⁵ Press Release, FTC, *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>.

and psychological characteristics and social circumstances...the effects of social media likely depend on what teens can do and see online, teens' pre-existing strengths or vulnerabilities, and the contexts in which they grow up." Below, CCIA outlines some principles to help online services and platforms as they develop their approach to keeping kids and teens safe online.

First, online services and platforms should respect the development stages of children and teens, ensuring the offered protections reflect the differences in maturity, capacity, and risk of harm between children and teens. Second, online services and platforms should provide age-appropriate features and controls. For children, this could include default uploading settings, having autoplay off by default, and break and bedtime reminders. But as users get older, the protections and controls may no longer be appropriate for teens. Auto-scroll limits may be more disruptive than helpful to a teen studying for an upcoming exam or the SAT. This also goes beyond the technical safeguards and extends to the health and wellness resources available to children and teens such as relating to issues around bullying or self-harm. Lastly, any proposal needs to encourage harmonization and interoperability so that kids and teens, regardless of their physical location, continue to receive the benefits of innovative technologies. A growing patchwork of inconsistent and often conflicting requirements at the state and local levels creates serious liability risks for business and confusion for users.

IV. Conclusion

The RFC asks what policy actions could be taken, by Congress or others, to advance minors' online health, safety, and/or privacy. A few options come to mind.

Passing federal comprehensive privacy legislation with strong preemption to end the patchwork of state laws that contain confusing and conflicting obligations. This would create clearer expectations for businesses and clarity and consistency for individuals of all ages and avoid infringing or restricting access to important resources and tools. Further, it would help put an end to the concerning trend of foreign officials importing foreign legislation that is ignorant of the rights and protections granted under the U.S. legal system, especially regarding the freedom of speech.³⁶ The recent and successful challenge to the California Age-Appropriate Design Code

³⁶ Mike Masnick, *Why Is A British Baroness Drafting California Censorship Laws?*, Techdirt (Aug. 25, 2022), <https://www.techdirt.com/2022/08/25/why-is-a-british-baroness-drafting-california-censorship-laws/>.

Act reaffirmed this notion, where the court held that all ten of the Act’s provisions likely violated the First Amendment.³⁷

Another opportunity lies in addressing the problems that contribute to the lack of prosecutions around CSAM — the industry makes tens of millions of CSAM reports to authorities every year, yet fewer than 1500 prosecutions have occurred annually.³⁸ A narrowly tailored legislative effort could be of immediate help to address the ongoing and serious harm to the victims of such heinous crimes.

CCIA appreciates the opportunity to comment on these important issues and would be happy to provide any additional assistance that might be useful to the Agency as it prepares its report.

Respectfully submitted,

Alvaro Marañon
Privacy Policy Counsel
Computer & Communications Industry Association

November 16, 2023

³⁷ Alvaro Marañon, *NetChoice v. Bonta: First Amendment Challenges to Age-Gating Mandates*, (Oct. 16, 2023), <https://www.project-disco.org/privacy/netchoice-v-bonta-first-amendment-challenges-to-age-gating-mandates/>.

³⁸ See Table D-2—U.S. District Courts—Criminal Federal Judicial Caseload Statistics (Mar. 31, 2023), <https://www.uscourts.gov/statistics/table/d-2/federal-judicial-caseload-statistics/2023/03/31>.