Comments of Common Sense Media, the Center for Digital Democracy, and Fairplay
Docket No. NTIA-2023-0008
RIN 0660-XC059
November 15, 2023

Common Sense Media ("Common Sense"), the Center for Digital Democracy ("CDD"), and Fairplay are pleased to submit these comments in response to the National Telecommunications and Information Administration's ("NTIA's") Request for Comment re its Initiative to Protect Youth Mental Health, Safety & Privacy Online. Common Sense is a national, independent, and nonpartisan resource for America's children, dedicated to improving the lives of kids and families by providing the trustworthy information, education, and independent voice they need to thrive in the 21st century. The Center for Digital Democracy is a public interest research and advocacy organization which works on behalf of citizens, consumers, communities, and youth to protect and expand privacy, other digital rights, and data justice. Its research-led initiatives focus on commercial and marketing practices, including youth and health, and are designed to educate policymakers, the news media, civil society, and the public, and to hold corporations accountable. Fairplay is a nonprofit organization committed to helping children thrive in an increasingly commercialized, screen-obsessed culture, and the only organization dedicated to ending marketing to children. We support the goals of the Kids Online Health and Safety Task Force ("Task Force") and offer below our input and recommendations for Task Force priorities.

The digital world offers enormous opportunities and benefits for young people. It connects them to previously unimaginable knowledge; it helps young people to find community; and it offers the potential for positive feedback and support. At the same time, it can leave young people feeling exposed and vulnerable. There are numerous risks of harm, including: privacy risks, misuses of information, inappropriate content, sexual exploitation, the inability to disconnect (so-called "addictive" tech), and childhood obesity. These risks and harms are exacerbated by children's and teen's developmental capacities and developing brains. Big tech's business models enable these risks and harm, with products and profits that depend on "engagement," eyeballs, and targeted advertisements. Children and teens in different groups can be disproportionately affected by their experiences online, and no one set of policy recommendations will fit all youth. Companies can and should prioritize youth well-being and be more transparent with kids and families. In addition, Congress must pass new laws–including updates to the Children's Online Privacy Protection Act (COPPA 2.0) and the Kids Online Safety Act (KOSA)–that protect children's online privacy and safety. Federal agencies should continue their important work, and the Federal Trade Commission especially should continue offering expert guidance and strong enforcement of privacy laws.

Q1. Youth face numerous risks of harm online.

Today's youth are almost never alone–they are constantly connected to their phones, the internet, and the technology companies that power popular social media and other platforms. While this opens young people up to many opportunities, it also leaves them vulnerable to many risks and harms, including but not limited to privacy harms and behavioral tracking and

targeting; inappropriate content; sexual exploitation; addictive design features; and unhealthy product marketing. Youth are vulnerable to these harms in large part because of their unique developmental needs and vulnerabilities.

Privacy

Privacy risks are rampant on social media and other platforms. Tracking and targeting minors is very common, even when laws purport to restrict it. One study found ad tech companies have gathered at least 72 million data points on children by the age of 13 (precisely when the Children's Online Privacy Protection Act (COPPA) is supposed to limit collection).[1] Partly, companies avoid complying with COPPA because they avoid having knowledge of children under 13, as narrowly defined under the 25-year-old children's privacy law. According to Common Sense privacy research, half of all companies in 2021 likely avoided obtaining actual knowledge of whether a user is a child under 13 years of age through the product's experience with an age-gate or required birth date, which can lead to inadvertently exposing children using these products to data monetization practices that are intended to only apply to teen and adult users.[2] Indeed, of 62 products evaluated by Common Sense that claim to not be intended for children, but are still used by children every day, data indicates that nearly 60% of products have disclosed risky, and possibly unlawful practices ("worse" practices) that use personal information to display targeted advertising to other users of the product, who could include consumers, parents, and educators.[3] Common Sense has also looked into whether popular apps and platforms disclose if (and how) they sell and share personal data.[4] The California Consumer Privacy Act (CCPA) became law in the state of California in 2020, but in the last year, the California Privacy Rights Act (CPRA) expanded the state's privacy laws and made explicit that the definition of selling data includes any practice by which apps or platforms track user behavior and then share that information for advertising purposes. Common Sense's research found that most businesses in the industry are either not in compliance with California's restrictions on selling or sharing data, or are not being transparent about how they are really monetizing our data. As a result, companies are misleading kids and families about privacy.

It's not just social media sites that fail to protect children. Common Sense research has also demonstrated that streaming services offer little additional privacy protections for children. And popular app store platforms are misleading families and children about privacy practices. Research into the privacy practices of the most popular streaming media services used by children, such as Netflix, Disney, Hulu and others has found evidence that stronger privacy protections for children are not disclosed in privacy policies, even when child profiles or

---

[1]Joseff, K. (2022). Behavioral Advertising Harms: Kids and Teens. https://www.commonsensemedia.org/sites/default/files/featured-content/files/behavioral_-surveillance-advertising-brief.pdf

[2] Kelly, G., Graham, J., Bronfman, J., & Garton, S. (2021). 2021 State of Kids' Privacy. San Francisco, CA: Common Sense, https://www.commonsensemedia.org/research/state-of-kids-privacy-report-2021.

[3] *See* id.

[4] Kelly, G., Graham, J., & Garton, S. (2023). 2023 State of Kids' Privacy. San Francisco, CA: Common Sense, https://www.commonsensemedia.org/research/2023-state-of-kids-privacy.

age-appropriate content moderation features are available.[5] None of the most popular streaming apps and devices evaluated provided a separate child profile with stronger privacy practices for children across all evaluation criteria.[6] If the most popular media streaming applications with children do not disclose how they protect children with stronger privacy protections, or engage in worse privacy practices for adults but still have child-directed content in adult accounts that can be accessed by children, then there can be no meaningful clarity and accessibility of privacy for children.

Unfortunately, efforts to achieve this transparency and accessibility have fallen short–so short, in fact, as to mislead children, teens, and families about practices. To provide more clarity and accessibility of a product's privacy practices, some companies have published separate "privacy principles" or "privacy center" webpages to help summarize their privacy practices, but often these privacy summary websites do not actually disclose any of the "worse" privacy practices they engage in with children, teens, or adults' data.[7] This can create a false sense of safety for children and parents who believe these products are more privacy protecting then they actually are because not all the most important facts are included. In addition, Apple's recent introduction of its App Store "privacy nutrition label" and Google's new "Data Safety section" in the Play Store for app developers have attempted to redefine what "privacy" means to consumers in the App Stores for hundreds of millions of users to build trust and improve clarity and accessibility of privacy.

Based on Common Sense research, which included reading and rating the full privacy policies of apps in both the Apple and Google App Stores, Common Sense was able to validate a company's privacy information displayed to consumers in App Store labels and product pages. These privacy and safety labels are self-reported by app developers without validation by Apple or Google. Recent research has found evidence of apps in App Stores that claim in their privacy labels that they have safer privacy practices than what their privacy policies state.[8] Some of these apps have problematic privacy practices for children such as selling data to third parties and targeted ads that use misinformation. This contradiction and privacy misinformation practice is spreading. Upwards of 60% of popular apps used by children and teens in both App Stores currently display false privacy information to parents and children, completely negating trust and any shared clarity or accessibility of a product's privacy practices.[9] Privacy misinformation is

[5] Kelly, G., Graham, J., Bronfman, J., & Garton, S. (2021). Privacy of Streaming Apps and Devices: Watching TV that Watches Us. San Francisco, CA: Common Sense Media, https://www.commonsensemedia.org/research/privacy-of-streaming-apps-and-devices-watching-tv-that-watches-us.
[6] *See* id.
[7] *See* Microsoft Privacy Principles, https://privacy.microsoft.com/en-US ("Microsoft's privacy center does not disclose its"worse " privacy practices of selling data, displaying targeted advertisements, or tracking users across the internet and over time for commercial purposes.")
[8] Anne Stopper and Jen Caltrider, Mozilla, No Evil: Loopholes in Google's Data Safety Labels Keep Companies in the Clear and Consumers in the Dark, https://foundation.mozilla.org/en/campaigns/googles-data-safety-labels.
[9] Li, Y., Chen, D., Li, Tianshi, Agarwal, Y., Cranor, L., & Hong, J.I. (2022, April 28). Understanding iOS privacy nutrition labels: An exploratory large-scale analysis of app store data. CHI Conference on Human Factors in Computing Systems Extended Abstracts (CHI '22 Extended Abstracts). https://doi.org/10.1145/3491101.3519739.

inherently unfair and deceptive because it is misleading parents and other consumers to download and purchase apps for themselves and their children that they believe to be "healthier" and more privacy-protecting.

Misuse of Information, Inappropriate Content, Sexual Exploitation

When information is collected from children, teens, and all users, it can be used to label and limit, and put individuals into ad categories. These categories can be based on their preferences and interests, purchases, and even state of mind. A leaked Meta (then Facebook) memo told Advertisers it could identify when teenagers felt worthless, stressed, or insecure.[10] In 2019, Meta categorized almost three-quarters of a million kids under 18 as interested in gambling, and almost a million as interested in alcoholic beverages.[11] Whether or not social media companies actually push alcohol or gambling on these minors, they can profit from it by advertising games with gambling elements or other features that would be particularly appealing to such users.

And, not infrequently, children and teens are exposed to ads and sites pushing adult content. Common Sense research found that one in five YouTube videos aimed at young children 0-8 contained age-inappropriate content, violent content, sexual content, and content involving drugs/alcohol, or politics.[12] Twenty-percent of videos watched by children 0-8 contained interpersonal violence.[13] Common Sense's Teens and Pornography (2023) research report detailed how social media sites are both a source of accidental exposure and–following pornography specific websites (e.g., Pornhub)--the most used sites for teens who regularly intentionally view pornography.[14] Smartphones allow access to many age-inappropriate experiences, with 68% of children under 13 saying they access "teen" rated apps and social media apps, and almost 45% saying they used apps with mature (17+) or adult (18+) ratings, including porn sites, Reddit, casino games, or violent games like Call of Duty.[15]

Children experiencing sexual exploitation and abuse is also far too common. Meta's own and independent research shows distressing levels of abuse. Meta's research shows a quarter of

---

[10] Joseff, K. (2022). Behavioral Advertising Harms: Kids and Teens. https://www.commonsensemedia.org/sites/default/files/featured-content/files/behavioral_-surveillance-advertising-brief.pdf., p. 4

[11] *Ibid*., p. 4

[12] Radesky, J. S., Schaller, A., Yeo, S. L., Weeks, H. M., & Robb, M. B. (2020). Young kids and YouTube: How ads, toys, and games dominate viewing, 2020. Common Sense Media. https://www.commonsensemedia.org/sites/default/files/research/report/2020_youngkidsyoutube-report_final-release_forweb_1.pdf., p. 3

[13] *Ibid*., p. 3

[14] https://www.commonsensemedia.org/sites/default/files/research/report/2022-teens-and-pornography-final-web.pdf Figure 5, Table 2

[15] Constant Companion https://www.commonsensemedia.org/sites/default/files/research/report/2023-cs-smartphone-research-report_final-for-web.pdf

13-15 year olds had received unwanted advances online in the past week.[16] This is consistent with independent research, which showed 1 in 4 children between the ages of 9 and 17 reported a sexual encounter with an adult online. More than half of youths were recontacted by individuals, even if they blocked or reported the problem.[17] And the companies seem to go to great lengths to make reporting itself difficult. Recent Meta whistleblower testimony shows that past efforts to address reporting of harassment and bullying were ignored, and that despite "troubling evidence that young teens were experiencing great distress and abuse on the Instagram platform," senior management, including Mark Zuckerberg, instead ignored the issue.

What's more, young people do not just stumble upon inappropriate or harmful content. Social media companies and other platforms, who have devoted billions of dollars to intimately understanding their users, have done extensive research to know precisely what sort of content will "engage" them–even though this content may be "civic misinfo, civic toxicity, and health misinfo."[18] And they consistently prioritize profits over people. Meta knew, for example, that Instagram made body image worse for a third of teen girls.[19] It knew that certain cosmetic surgery filters in particular caused harm to young girls–negatively impacting teen mental health and wellbeing. And yet Meta CEO Mark Zuckerberg himself rejected any efforts to remove such features.[20] Research from Fairplay found that Meta makes millions of dollars every year by promoting pro-eating disorder content to children and teens on Instagram.[21] Among teen girls with moderate or severe depressive symptoms, roughly 7 in 10 users of Instagram and TikTok say they come across problematic suicide-related content at least monthly.[22] Teens want to see more positive content on these platforms, want explicit content to be blocked, and want adults not to follow them.[23]

Difficulty Disconnecting

---

[16] Senate Judiciary Committee. (2023, November 7). Written testimony of Arturo Bejar before the Subcommittee on Privacy, Technology, and the Law. https://www.judiciary.senate.gov/imo/media/doc/2023-11-07_-_testimony_-_bejar.pdf

[17] Thorn & Benenson Strategy Group. (May 2021). Responding to online threats: Minors' perspectives on disclosing, reporting, and blocking. Thorn. https://info.thorn.org/hubfs/Research/Responding%20to%20Online%20Threats_2021-Full-Report.pdf

[18] 5 Five points for anger, one for a 'like': How Facebook's formula fostered rage and misinformation, WASH. POST (Oct. 26, 2021).

[19] https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739

[20] Commonwealth of Massachusetts v. Meta Platforms, Inc. and Instagram, LLC. (Superior Court October 24, 2023). Retrieved from https://www.mass.gov/files/documents/2023/10/25/2023-10-24-Meta%20Complaint%20-%20REDACTED.pdf., p. 56-59.

[21] Fairplay, *Designing for Disorder: Instagram's Pro-eating Disorder Bubble* (June 2022), https://fairplayforkids.org/wp-content/uploads/2022/04/designing_for_disorder.pdf.

[22] Nesi, J., Mann, S. and Robb, M. B. (2023). Teens and mental health: How girls really feel about social media. San Francisco, CA: Common Sense.

[23] *Ibid.,* p. 12

Young people are also bothered by the addictive nature of these platforms. They report feelings of always needing to be responsive to peers and on their devices, and a struggle to set boundaries for themselves.[24] Notifications–often coming from social media platforms–fire off on young people's phones throughout the day, including school hours and late at night–with 11 to 17 year olds receiving over 237 notifications on a typical day.[25] It is difficult for children and teens to disconnect–and very intentionally so, given the platforms make more money for themselves and any advertisers the more time young people spend on them.

Contributing to the Obesity Crisis

Big Tech and Big Food also deploy many tactics to market unhealthy products to children and teens in digital settings. They are using AI, machine learning, and other data-driven techniques to ensure that food marketing permeates all the online cultural spaces where children and teenagers congregate. Research shows that marketing of these products contributes to childhood obesity and related illnesses.

Their constant immersion in digital culture has exposed youth to a steady flow of marketing for fast foods, soft drinks, and other unhealthy products, much of it under the radar of parents and teachers. Food and beverage companies have made digital media ground zero for their youth promotion efforts, employing a growing spectrum of new strategies and high-tech tools to penetrate every aspect of young peoples' lives. The so-called "influencer economy," gaming and esports platforms, and the rapidly expanding streaming and online video industry contribute to this trend.

Black and Brown youth are particularly vulnerable to new online promotional strategies. Food and beverage marketers are "appropriating some of the most powerful 'multicultural' icons of youth pop culture and enlisting these celebrities in marketing campaigns for sodas, 'branded' fast-food meals, and caffeine-infused energy drinks".[26] These promotions can "compound health risks for young Blacks and Hispanics," subjecting them to "multiple layers of vulnerability, reinforcing existing patterns of health disparity that many of them experience."

Harm and Child Development

Youth are particularly susceptible to these harms because of their unique developmental needs. For example, minors' executive functioning skills, which are critical to directing attention and behavior, are still developing throughout childhood and adolescence.[27] Young children do not understand the consequences of information shared with apps and platforms. They believe, for

---

[24] *Ibid*., p. 2; https://docs.google.com/document/d/1uWd4UbRHWYaWG3v2oE4DdaxsY9-KdnXzG-rM7DPSZY8/edit

[25] https://www.commonsensemedia.org/research/constant-companion-a-week-in-the-life-of-a-young-persons-smartphone-use

[26] https://democraticmedia.org/reports/big-food-big-tech-and-global-childhood-obesity-pandemic

[27] Heather J. Ferguson et al., *The Developmental Trajectories of Executive Function from Adolescence to Old Age*, Sci. Rep. (2021), https://www.nature.com/articles/s41598-020-80866-1.pdf.

example, that deleting an app or information within an app will delete it from the internet, and they do not expect or understand that a game they play may gather information about them from external sources.[28] Further, adolescence is a period of heightened reward-seeking behavior as a result of increased brain activity related to dopamine.[29] This contributes to teens' tendency to seek out reward stimuli,[30] such as those offered by social media and gaming platforms. Social acceptance also activates the reward center in adolescent brains,[31] rendering youth susceptible to the social manipulation and peer pressure applied by design features intended to maximize user engagement. It is critical to consider these and other unique aspects of minors' development when assessing the business practices and design techniques that companies use to attract young users' time and attention.

Q2, 6, 9. **Products that depend on "engagement," eyeballs, and targeted advertisements enable these risks and harms.**

Business models built around maximizing users, time-spent online, and highly sophisticated individual targeting enable harms. With each passing week, the public seems to learn more about how tech companies' business models–maximizing time spent on platforms and use of targeted and inflammatory content–hurt children. And how technology executives repeatedly prioritize profits over young people. Just this month a complaint by the Massachusetts Attorney General offered internal emails showing that, repeatedly, Meta executives, including CEO Mark Zuckerberg, rejected proposals to improve young users' well-being, as the company preferred instead to increase and maximize time spent on its platforms and therefore its profits.

For example, internal studies showed hiding "likes" helped make teen users feel less social comparison —and yet because Meta was worried this would limit time on the platform, it chose to offer that option only as an opt-in, not as the default, knowing that fewer people would choose it (.72% of users would voluntarily opt-in to a protective setting, vs. 35% who would otherwise leave the protective setting in place if it were the default).[32] Similarly, Meta saw that if it recommended and amplified "egregious content", it would push teens down rabbit holes. But it did not want to stop amplifying such content, because that would come with "a clear engagement cost."[33]

---

[28] Anonymous Author(s). 2021. "They See You're a Girl if You Pick a Pink Robot with a Skirt": How Children Conceptualize Data Processing and Digital Privacy Risks. In CHI '21: ACM CHI Conference on Human Factors in Computing Systems, May 8–13, 2021, Yokohama, Japan. ACM, New York, NY, USA
[29] Eveline A. Crone, Executive Functions in Adolescence: Inferences from Brain and Behavior, 12 Developmental Science 825, 829 (2009); Adriana Galvan, Adolescent Development of the Reward System, 4 Frontiers Hum. Neuroscience 1, 1 (2010).
[30] Ashley C. Parr et al., *Dopamine-Related Striatal Neurophysiology Is Associated with Specialization of Frontostriatal Reward Circuitry Through Adolescence*, 201 Progress in Neurobiology 1, 1 (2021); Dustin Albert & Laurence Steinberg, *Judgment and Decision Making in Adolescence*, 21 J. Res. on Adolescence 211, 217-219 (2011).
[31] Zara Abrams, Why Young Brains Are Especially Vulnerable to Social Media, APA (Feb. 3, 2022), https://www.apa.org/news/apa/2022/social-media-children-teens.
[32] Commonwealth of Massachusetts v. Meta Platforms, Inc. and Instagram, LLC., p. 54-56.
[33] Commonwealth of Massachusetts v. Meta Platforms, Inc. and Instagram, LLC., p. 59-60.

The tension between policy recommendations that would support young people, and social media companies' bottom lines, is detailed in Unseen Teen: The Challenges of Building Healthy Technology for Young People (2021). In this Data & Society study, researchers interviewed anonymous staff at major social media and social game companies about how they thought (or didn't think) about building products and features for digital well-being. It highlights that companies do not think about young users as the "average" user, and that they are often treated as an after thought. It explores how companies silo teams working on youth well-being, and create barriers for those who wish to improve well-being. And it highlights the tensions within companies from employees wanting to make changes to products to improve digital wellbeing and fiduciary duties to shareholders and investors to continue a robust return on investment, which pushes all decisionmaking away from anything that diminishes revenue/users/time on platform.

Q8. Children and teens in different groups can be disproportionately affected by their experiences online.

It is important to understand how different groups of children are impacted differently. Common Sense research has found, in Teens and Mental Health: What Girls Really Think About Social Media (2023), that kids who are already struggling with mental health challenges are more likely to experience the extremes of social media - finding it both very positive and very negative. The study also does important work of focusing on what features across platforms girls find positive or negative. Notably girls like getting content customized for them, but dislike the ways in which certain features make them feel exposed, vulnerable, or visible.[34] In addition, social media was shown to both uniquely help and harm LGBTQ+ kids.[35] A study from Fairplay similarly found that LGBTQ+ identifying youth were more likely to report scrolling for too long, losing track of time, and seeing drug, drug use, and pro-eating disorder content on social media than their peers who do not identify as LGBTQ+.[36]

Children of diverse races may also be differently impacted by what they see–or don't see–on screens. Research has found a lack of diverse representation on YouTube.[37] But research also shows that representation is important. Exposure to negative media depictions of their own ethnic-racial groups can undermine children's sense of self, while watching favorable depictions of their own ethnic-racial group can have a positive impact on self-perceptions.[38] If children of

[34] Nesi, J., et al. (2023). Teens and mental health: How girls really feel about social media. San Francisco, CA: Common Sense., p. 34
[35] *Ibid*., p. 47-48
[36] Fairplay, *Unfair Impacts: How LGBTQIA+ Youth are Disproportionately Harmed by Online Platform Design Decisions* (June 2023), https://fairplayforkids.org/wp-content/uploads/2023/06/unfairimpacts.pdf.
[37] Who is the "You" in YouTube? Missed Opportunities in Race and Representation in Children's YouTube Videos (2022) (Q8) OR Rollins, D., Bridgewater, E., Munzer, T., Weeks, H. M., Schaller, A., Yancich, M., Gipson, W., Drogos, K., Robb, M. B., & Radesky, J.S. (2022). Who is the "you" in YouTube? Missed opportunities in race and representation in children's YouTube videos, 2022. San Francisco, CA: Common Sense.
[38] Rogers, O., Mastro, D., Robb, M. B., & Peebles, A. (2021). The Inclusion Imperative: Why Media Representation Matters for Kids' Ethnic-Racial Development. San Francisco, CA: Common Sense., p. 1

color only see themselves represented sparingly or in stereotypical ways, it has a negative influence on their self-perception and well-being.

In addition, it is important to consider how differently aged children experience media differently. The ICO has done tremendous research in this area and provided detailed guidance, addressing children in five different developmental age ranges of 0-5 (pre-literate & early literacy), 6-9 (core primary school years),10-12 (transition years), 13-15 (early teens), and 16-17 (approaching adulthood).[39]

Q20. Common Sense Media has long been a trusted source for sound evidence about how children, teens, and families are experiencing media and technology – and Common Sense's Privacy Program has shed light on how the technology itself operates.

Common Sense research is cited through this filing, as it provides real world evidence of how children and families are experiencing and using technology. The Common Sense Census has for the last thirteen years traced how kids (from 0-8, and 8-18) are spending time on these platforms. Other excellent research sources include: Fairplay, Center for Digital Democracy, Data & Society, Consumer Reports, Pew Research Center, Child Trends, World Health Organization[40], and Sonia Livingstone at the London School of Economics.[41]

Understanding how kids experience technology is step one. We also need to understand how the technology works, and we need to put in place appropriate protections. Just as we regulate our food system to protect the public's health and safety of food products in the grocery store, we also need to urgently protect the privacy of kids and families with the media and technology they use. To that end, research from the Common Sense Privacy Program is also cited through this filing. The Program uses trained privacy experts and attorneys to read and evaluate the privacy practices of thousands of popular applications and platforms used by children and families. These evaluations provide scientifically sound evidence of a company's privacy practices to help parents, children, and teens make better informed decisions.[42] Common Sense Privacy's data-informed research into the privacy practices of the most popular applications and services used by children and teens found that the majority of applications and services do not transparently disclose that they have stronger privacy protections for children. The research found that apps and platforms may be monetizing children's information in violation of the law. Common Sense research also found that popular streaming services used by children and adults did not appear to offer any stronger privacy protections for children. And in one study,

---

[39] https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf Age Range recommendations.

[40] See for example, World Health Organization-Europe, "Understanding the Digital Media Ecosystem: How the Evolution of the Digital Marketing Ecosystem Impacts Tobacco, Alcohol and Unhealthy Food Marketing," June 23, 2022, https://www.who.int/europe/publications/i/item/9789289057950 or World Health Organization, "Implementing Policies to Restrict Food Marketing: A Review of Contextual Factors," September 14, 2021, https://www.who.int/publications/i/item/9789240035041

[41] https://www.lse.ac.uk/media-and-communications/people/academic-staff/sonia-livingstone.

[42] Common Sense Media, Privacy Program, https://privacy.commonsense.org.

privacy “nutrition labels” or summaries in app stores for over 60% of apps evaluated displayed false information about privacy practices, leading to lack of privacy protections and distrust overall.

All together, this research can be of great value to the Task Force as it determines what protections are needed and why enforcement of such protections is critical.

Q16, 17. Policy Guidance and Recommendations for Companies, Congress, and Agencies

Young people need and deserve better online protections for their health and safety. And it is up to policymakers and industry to ensure that they get them. Below, we detail steps companies and agencies can take, as well as legislation Congress can pass–COPPA 2.0, KOSA, first and foremost–that would better protect youth online.

Companies can prioritize youth well-being and be transparent with kids and families.

Companies should adopt principles of data minimization, ban targeted ads to youth, adopt anti-discriminatory data practices, and demonstrate a “duty of care” for all users and especially children and teens. These principles are ones we hope to see in legislation, but companies do not need to wait to implement them.

In addition, companies need to be more transparent, in particular in explaining if and how they protect youth users differently than other users. Enhanced clarity and accessibility of the privacy practices of an application or service can help children, teens, and their parents make better informed decisions about the apps they use every day and hopefully choose better privacy protecting products. If children under the age of 13, or teens younger than 18, use an application or service, the company should disclose how they better protect the privacy of children and teens in their privacy policy. In addition, if an application or service has worse privacy practices for adult users or consumers, such as selling their data to third parties for profit, or displaying targeted advertising that could inadvertently harm children, then the company should disclose additional protections are in place to protect children or teens from these practices by default to minimize unintended harm. Streaming apps and devices with kid and family directed content should minimally include child profiles or child accounts to provide a safer experience with age-appropriate content recommendations and stronger privacy practices that protect children's data when they are using the streaming app or device. Additional privacy protections that apply to children's data when using separate child profiles also need to be clearly communicated to parents with a separate child privacy policy that explains what stronger privacy protecting practices are actually in place when children are using the streaming app or device.[43]

[43] *See* id.

While it is critical that information be provided in detailed notices for researchers and regulators, it is also important that information be clear and accessible to parents and kids. Information should be presented to them at relevant points in time in digestible formats. Parents and teens today seeking information often find themselves adrift in a sea of lengthy notices and legalese, causing many to simply give up with resignation. And while transparency is essential, it is not sufficient to protect young users online. Parents and other caregivers are too busy and in many cases too unfamiliar with technology to know, or have the time to know, which features to turn on or off and how to turn them on or off. That is why in addition to company action, federal and state lawmakers and regulators must act to protect kids and teens online.

Agencies have important work to do, Congress must pass laws, and the laws must be strongly enforced.

There is ample room for numerous players to work together to improve young people's experiences online. At the agency level, we are pleased that, thanks to the passage of the CAMRA Act, the National Institute of Health is awarding contracts to researchers in order to fulfill its directive to lead a research program on the longitudinal impact of technology on infants', children's, and adolescents' cognitive, physical, and socio-emotional development. This work must continue. In addition, we are grateful to the NTIA for its work in connecting more young people and their families to the internet. Now that more people are connected, it is critical to distribute information to these previously under-connected communities, so they learn ways to maximize digital benefits while minimizing harms and supporting youth well-being. Given the NTIA's breadth of work, it has additional opportunities to encourage data minimization, reduced targeting, and reduced data sharing in numerous contexts. It should seize these opportunities, as improvements elsewhere in the online ecosystem will trickle through to youth as well. And, of course, the Federal Trade Commission (FTC) is the trusted expert agency when it comes to privacy, and it must continue its critical work in advancing policy to protect children and teenagers, such as updating the COPPA rules–in addition to acting as a robust enforcer, discussed more below.

Congress also must act to set policy into clear legislative requirements. As a preliminary step to support kids and families Congress can and should finish their work to pass two pieces of bipartisan legislation, COPPA 2.0 and KOSA, that begin by updating and establishing protections for kids online.

Privacy is step number one when it comes to kids' online safety. Stemming the flow of minors' data to tech companies is critical to reducing the harms associated with online targeting and tracking; companies' ability to uniquely target individuals vastly exacerbates harms to youth. Congress should pass the bipartisan COPPA 2.0. Importantly, it would close a number of loopholes in COPPA, now 25 years old, and provide protections to teenagers. It would establish an opt-in regime for minors; expand COPPA's online protections to teens age 13 to 17; ban targeted advertising to kids and teens; prevent companies from turning a blind eye to minors on their platforms; guarantee minors the right to erase their internet history; and establish a Youth

Privacy and Marketing division at the FTC. Congress should also ensure that the FTC has sufficient funding for staff and enforcement.

In addition, Congress should pass the bipartisan KOSA in order to shift responsibility for safety away from families and onto platforms. KOSA imposes a "duty of care" on covered platforms, requiring them to prevent or mitigate the heightened risks of harm to minors posed by the platform. KOSA seeks to hold companies accountable for the business practices and choices they make, including decisions to design their services in ways they know are linked to: anxiety, depression, eating disorders, substance use disorders, and suicidal behaviors; addiction-like behavior; physical harm, bullying, and harassment; sexual exploitation; the promotion of drugs, gambling, and alcohol; and predatory, unfair, and deceptive marketing practices. Platforms would be required to provide safeguards and tools for minors, including defaulting to privacy-protective settings and enabling parents of young children, and teens themselves, to turn off addictive design features like autoplay and endless scroll. Platforms should also enable opt out of algorithmic recommendation systems, and allow limiting of financial transactions by minors. KOSA would also require that platforms issue annual independent audits identifying risks of harm. This is critical given mounting evidence that platforms know about harms but will not disclose their research.

This legislation is necessary as a baseline to protect children and teens. In addition, Congress should pass a comprehensive national privacy law to ensure protections for everyone. And, when considering that children and teens are also interacting with even newer technology in the form of AI–including on social media and other platforms–Congress should consider that actions taken now can help protect us in the future. And while these actions are necessary, more may be needed in the future as technology evolves.

Legislation is only as strong as its enforcement. When the FTC, or state AGs, see social media companies and platforms violating federal or state law, they should take action. One practice they can and should stop right now is companies' unfair and deceptive practices and their misrepresentations – about whether they know their products are harming kids, and about what their privacy practices are in the first place. Meta should not be able to publicly claim they support youth well-being while privately killing off efforts to actually support youth because it might hurt the bottom line. Apps should not be permitted to have "privacy nutrition labels" and platforms "privacy centers" that do not disclose companies' worse practices (only their better ones). Companies need to be held accountable when they market themselves as privacy-protecting in App Stores to increase the likelihood of more downloads, but their privacy policies transparently disclose inconsistent and problematic privacy practices. Companies also need to be held accountable for privacy misinformation so parents and children can make better informed decisions about the apps and services they use every day.

Parents are concerned about their children's interaction with technology and media. And they desperately want to understand the digital landscape, and know which apps and platforms are better for privacy and well-being, but now they have an additional challenge of identifying what is best amidst a raft of false privacy information. In many cases, children and families may have

opted in to use an app or a platform, thinking that their data is protected, when in reality, it isn't. If companies can say one thing but do another, then consumers don’t have a meaningful choice if their data is sold, and that's especially concerning when it comes to kids. For existing laws to have any real impact, and inform federal policy, we need to start holding companies accountable when they don't comply. Otherwise, the industry will continue making money by influencing and exploiting kids and families' data for commercial purposes, all while claiming they respect our privacy.

Conclusion

We appreciate the NTIA and the Task Force’s attention to these issues and would be happy to serve as a resource as the work continues.