

From: Common Sense
Re: Draft Online Safety Bill - Call for Evidence
Date: September 13, 2021

Common Sense is an independent, not-for-profit organisation dedicated to helping children and families thrive in a rapidly changing digital world. We are based in San Francisco, with offices across the United States and in the United Kingdom. We are a leading organization that parents, teachers, and policymakers go to for unbiased information, trusted advice, and innovative tools to harness the power of media and technology as a positive force in all children's lives.

Common Sense has watched with interest as the Online Safety Bill has developed, and has supported its development as an important tool to protect children, families, and society. Too often, online platforms take advantage of young people, exposing them to bullying, harassment, and hate as well as far too many inappropriate ads and unfair commercial practices. Common Sense has recommended that the government create safeguards to protect children from exposure to inappropriate content, help protect children from manipulative practices, and require more industry transparency.¹ Common Sense has also championed the importance of digital literacy as a piece -- though certainly not the entire -- solution.

We applaud your efforts on the Online Safety Bill and continuing to lead in protecting children in the online space. We are especially excited about the support for digital literacy. We write to offer suggestions to make the safeguards of the bill more effective and cement the UK's leadership position. **We offer three main suggestions to help ensure that children, a particularly vulnerable group, are effectively protected from harmful activity and content: (1) the bill should more explicitly address amplification and systemic design as drivers of potential harm and "legal but harmful" content; (2) the bill's exclusion of commercial, financial, and advertising harms is a missed opportunity; (3) the phrase "likely to be accessed" by children should be interpreted as equivalent to the AADC.**

- 1. It is critical to more explicitly address amplification and systems that themselves push harmful content and cause harm.**

We appreciate that the children's risk assessments require companies to take into account, for example, differently aged children differently, and the requirement to consider how overall design may increase or decrease risks. However, the focus appears to be very much on content, with amplification and the algorithms and systems that may promote harmful content an afterthought. While the assessment requires that one take "into account (in particular) algorithms used by the service and how easily, quickly and widely content may be disseminated

¹See e.g., Common Sense Response Submission for the United Kingdom's Online Harms White Paper. (June 2019). https://www.common sense media.org/sites/default/files/featured-content/files/20190619_common_sense_media_submission_to_consultation_on_online_harms_white_paper_1.pdf

by means of the service” (Chapter 2 (7 Risk assessment duties) (9 Children’s risk assessments)), that should be a primary consideration in any risk assessment, not just a factor to consider when assessing harmful content. Further, the requirement that companies assess overall design is broad and vague enough to enable companies to ignore algorithms and amplification if they choose. We recommend inclusion of addressing amplification specifically.

Amplification and the opaque algorithms that drive it determine the content that young people see online. Content-shaping algorithms determine the contours of a user’s Facebook NewsFeed, what autoplay presents them on YouTube, or what pops up on TikTok²; they also dictate when, where, and what type of advertisements are shown. Both advertising and content personalization are only possible because of the vast troves of detailed information that the companies have accumulated about their users and their online behavior, often without specific, informed and unambiguous consent of the people being targeted. The underlying business model, which is premised on extensive data collection and sharing, also encourages platforms to design algorithmic curation in a way that prioritizes sensational, controversial, and inappropriate content to maximize user engagement. Children on social media are regularly exposed to violence, self-harm, profanity, porn, hate speech, and even violent livestreams. During the pandemic, reports have found that 47% of children and teens have seen content they’d rather avoid, leaving them feeling uncomfortable (29%), scared (23%) and confused (19%).³ Sixty-one percent of parents whose children watch YouTube say their child has encountered content they felt was unsuitable for children.⁴

This not only subjects children and young people to harmful and inappropriate material, but, as we have seen, it amplifies content that encourages the spread of conspiracy theories, undermines democracy, and can lead to misinformation about vital public health matters. Platforms directly profit from spreading misinformation and further indoctrinating users into harmful conspiracy theories. This is why Common Sense has, for example, supported limits to children’s exposure to unhealthy online content via social media and other algorithmically curated platforms, limits to incentives for pushing inappropriate ads and disturbing and illegal content onto children, as well as controls on algorithmic amplification and user interface design that subverts user choice and amplifies harmful content, S.3411 Kids Internet Design and Safety (KIDS) Act, (5 March 2020); S. 1084, Deceptive Experiences To Online Users Reduction Act (2019).

Ultimately, we hope that the Online Safety legislation can focus not just on specific content but also more directly on algorithms that increase children’s exposure to unhealthy, disturbing, inappropriate, and illegal content.

² Barry, R., Wells, G., West, J., and Stern, J. (Sept. 8, 2021). [How Tik Tok Serves Up Sex and Drug Videos to Minors](#). *The Wall Street Journal*.

³ BBFC. (May 2020). *Half of children and teens exposed to harmful online content while in lockdown*. <https://www.bbfc.co.uk/about-us/news/half-of-children-and-teens-exposed-to-harmful-online-content-while-in-lockdown>

⁴ 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*. San Francisco, CA: Common Sense Media.

2. It is a missed opportunity to not include certain financial, advertising, and commercial harms.

The draft bill does not appear to address online risks and harms which can flow to children based on commercial conduct, including inappropriate advertisements and exhortations to purchase or spend money. The bill proposes that content's "potential financial impact" is not relevant to risk of harms. (Chapter 6 (45 Meaning of Content that is harmful to children)). This is a huge missed opportunity. Both advertisements which induce children to purchase, and in-app purchasing opportunities themselves, are harmful to children.⁵ Online ads often prey unfairly upon children, who are especially susceptible to advertising. Children and teens' developing brains have trouble both identifying and understanding advertising, and new technologies and advertising techniques, like native ads and influencer marketing, exacerbate these difficulties.⁶ The lack of separation between sponsored and non-sponsored content online can make it harder for a child to discern an advertisement from entertainment.⁷ Companies also hide commercial requests in advergimes, which are videos and online games that integrate advertising into a game to promote products. Children play these without realizing they are engaging with an ad.⁸ And, even when children can differentiate between ads and other content, they still struggle to understand the commercial purpose of the advertisement. Indeed, some researchers have found that children ages 6–7 predominantly view advertisements as informational breaks for the watchers or the makers of a tv program.⁹

Unfortunately, online ads are pervasive. Product placement, branded content, and influencers are some of the most popular children's content. Common Sense research looking at children's content on YouTube found advertising occurred in 95% of early childhood videos. Over one-third of videos in the early childhood category contained three or more ads, while 59% contained one to two ads. Ad design in these videos was often problematic, including banner

⁵ See e.g. [Letter from Common Sense and Dr. Jenny Radesky on Article 26 of the Digital Services Act](#), (2021).; *Hearing on "Kids Online During COVID: Child Safety in an Increasingly Digital Age."*, House Subcommittee on Consumer Protection and Commerce, 117th Congress. (11 March 2021). Written Testimony by Ariel Fox Johnson. https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Witness%20Testimony_Fox%20Johnson_CPC_2021.03.11.pdf

⁶ [Common Sense Comments to the Federal Trade Commission on Guides Concerning the Use of Endorsements and Testimonials in Advertising](#), (June 22, 2020).

⁷ American Psychological Association. (20 February 2004). *Advertising and Children*.

<http://www.apa.org/pubs/info/reports/advertising-children>; Hudders, Liselot & Cauberghe, Verolien & Panic, Katarina. (2015). How Advertising Literacy Training Affects Children's Responses to Television Commercials versus Advergimes. *International Journal of Advertising*. doi:10.1080/02650487.2015.1090045.

⁸ Soontae An, Hyun Seung Jin & Eun Hae Park. (2014). Children's Advertising Literacy for Advergimes: Perception of the Game as Advertising. *Journal of Advertising* 43(1), 63-72. doi: 10.1080/00913367.2013.795123.

⁹ Graff, Samantha, Dale Kunkel & Seth E. Mermin. (2012). Government Can Regulate Food Advertising to Children Because Cognitive Research Shows that it is Inherently Misleading. *Health Affairs* 2, 392-398.; Valkenburg, P. M., & Cantor, J. (2001). The development of a child into a consumer. *Journal of Applied Developmental Psychology* 22(1), 61–72. [https://doi.org/10.1016/S0193-3973\(00\)00066-6](https://doi.org/10.1016/S0193-3973(00)00066-6); Most children's understanding of the "selling intent" of television food ads did not emerge until around 7–8 years, reaching 90% by 11–12 years. Carter, Owen B.J. et al. (March 2011). Children's understanding of the selling versus persuasive intent of junk food advertising: Implications for regulation. *Social Science & Medicine* 72(6), p. 962-968.

ads that blocked educational content, sidebar ads that could be confused for recommended videos, or ads for video games that showed doctored versions of popular children’s characters, such as Peppa Pig.¹⁰ Past research on advertising in children’s apps has shown a high prevalence of manipulative or disruptive ad designs, as well as adult ad content that is easily clicked on by child users.¹¹ Additionally, apps encourage children to watch ads by offering in-app rewards in exchange.¹² Host-selling is pervasive online, with characters pushing products in ways that take advantage of children’s special relationships with the hosts. While young children may develop parasocial relationships with favored characters, teens do the same thing with influencers, whom teens look to as peers.¹³

In-app spending is also a big problem. Teen apps are highly monetized--a recent study highlights that teen apps are over three times more likely to support in-app purchases than general audience apps.¹⁴ And even young and pre-literate children are directly encouraged to spend money within apps and games. Beloved cartoon characters berate preschool players for not spending money.¹⁵ Educational games allow children to advance faster than their friends if they purchase subscriptions.¹⁶ Often, the fact that a purchase involves actual money is not made clear to children, who believe their activities have no “real world” consequences and do not realize they are spending their parents’ money. Children do not have an understanding of virtual currency and value exchanges. Young people have spent hundreds and thousands of dollars, collectively totalling millions. Indeed, Google, Apple, and Amazon have all settled with the U.S. regulators over unfairly permitting minors to make in-app purchases when it was not clear a purchase was being made and when parents were not given a choice whether to allow the purchases.¹⁷ Facebook documents show the company allowing children as young as five unwittingly spending their parents’ money, and intentionally making it difficult for children and parents to get refunds.¹⁸

3. Likely to be accessed by children should not have a more limited scope than in the Age Appropriate Design Code.

¹⁰ Radesky, J. S. et. al. *Young kids and YouTube*.

¹¹ Ibid.

¹² Meyer M, Adkins V, Yuan N, Weeks HM, Chang YJ, Radesky J. (1 Jan 2019). Advertising in young children’s apps: A content analysis. *Journal of Developmental & Behavioral Pediatrics* 40(1), 32-9.

¹³ [Common Sense Comments to the Federal Trade Commission on Guides Concerning the Use of Endorsements and Testimonials in Advertising](#), (22 June 2020).

¹⁴ [Risky Business: A New Study Assessing Teen Privacy in Mobile Apps](#), BBB National Programs, (October 2020).

¹⁵ Meyer, et al. “Advertising in young children’s apps.”

¹⁶ Klein, Alyson. (23 February 2021). [Popular Interactive Math Game Prodigy Is Target of Complaint to Federal Trade Commission](#), Education Week.

¹⁷ See ruling in *FTC v. Amazon*, (2016). [Federal Court Finds Amazon Liable for Billing Parents for Children’s Unauthorized In-App Charges.](#), and *FTC v. Apple*, (2014). [FTC Approves Final Order in Case About Apple Inc. Charging for Kids’ In-App Purchases Without Parental Consent](#), and *FTC v. Google*, (2014). [FTC Approves Final Order in Case About Google Billing for Kids’ In-App Charges Without Parental Consent](#).

¹⁸ [Request for the Federal Trade Commission to Investigate Facebook In-App Purchases for Violating the Federal Trade Commission Act and the Children’s Online Privacy Protection Act](#). (21 February 2019).

While we understand from public presentations that “likely to be accessed” is intended to be roughly synonymous with definitions provided by the ICO, the proposed bill language on its face indicates that “likely to be accessed” may have a more narrow interpretation in this context.

In terms of assessing access by children, the draft bill proposes that “a service is to be treated as “likely to be accessed by children” if the provider’s assessment of the service concludes that—(a) it is possible for children to access the service or any part of it, and (b) the child user condition is met in relation to—(i) the service, or (ii) a part of the service that it is possible for children to access.” The child user condition is further defined as follows: ““The “child user condition” is met in relation to a service, or a part of a service, if—(a) there are a significant number of children who are users of the service or of that part of it, or (b) the service, or that part of it, is of a kind likely to attract a significant number of users who are children.” (Chapter 4 (26 Assessment about access by children)). “Significant number” is given additional scope in the Explanatory Notes (“for the purposes of the ‘child user condition’ a ‘significant’ number should be considered as such where it is significant in proportion to the total number of United Kingdom users of a service or (as the case may be) a part of a service”). This leaves the phrase “significant number” open to a broad range of interpretations.

In common understanding having a significant number of children on a site would seem to be a higher bar than being “more probable than not” that children are on a site (the ICO definition). Having two potential standards for “likely to be accessed” is problematic for businesses seeking to comply with both the Age Appropriate Design Code and the Online Safety Bill. A more limited definition of sites covered by the Online Safety bill--such as only those with an undefined “significant number” of children--would limit the reach of critical protections.

Based on Common Sense’s experience with the Children’s Online Privacy Protection Act (COPPA), a too narrow definition of what sites are covered leaves children exposed. COPPA only applies to sites directed to children or with “actual knowledge” of children.¹⁹ Sites and platforms profiting off of tracking and marketing to children, in some cases millions of children, have still told U.S. regulators that they did not have “actual knowledge” of specific child users and resisted COPPA’s application. It is our fear that sites that have a large absolute number of child users, or a high but debatably not “significant” percentage of child users, would assert that the child-specific requirements in this bill do not apply.

We thank you again for your important work, and respectfully request that you consider these clarifications to provide the utmost in protections for young people.

¹⁹ Children’s Online Privacy Protection Act, 78 FR §312.2 (Jan. 17, 2013).