



TO: The European Commission
Directorate-General
for Communications Networks, Content, and Technology
FROM: [Common Sense Media](#)
DATE: 24 October 2025
RE: [DSA - Digital Fairness Act Call for Evidence](#)

INTRODUCTION:

Common Sense Media is dedicated to improving the lives of children and families by providing the trustworthy information, education, and independent voice they need to thrive. Our ratings, research, and resources reach more than 150 million users worldwide, over 1.4 million educators, and more than 100,000 schools worldwide every year. Backed by the research that forms the foundation of everything we do, we champion quality media that entertains and inspires, and support legislation aimed at closing the digital divide and holding social media and AI platforms accountable for their effects on minors. We encourage students and educators to think critically about technology and become responsible digital citizens. And we safeguard children's health and well-being by protecting their data privacy and reducing potential online harms.

We are pleased to submit these comments in response to your DSA-Digital Fairness Act Call for Evidence. Common Sense Media supports the European Commission's efforts to address the lack of digital fairness for consumers, including the most vulnerable consumers like minors. As a trusted global brand for children and families, we look forward to helping bring American and international perspectives to consideration as the Commission develops essential regulatory guidance to improve children's lives around the world.

RESPONSE:

Common Sense Media applauds the Commission's focus on the issue of digital fairness for consumers, and we agree that children and teens across the world deserve to have their safety and privacy protected. In the United States, this concern is addressed through privacy laws and rules surrounding the protection of minors online, usually through the design of the platforms.

There is only one dominant US federal law that has been explicitly passed to protect children online. This is the Children's Online Privacy Protection Act (COPPA) of 1998. COPPA was - and still is - a landmark bill that first went into effect in 2000, aimed at strengthening protections related to the online collection, use, and disclosure of personal information of minors under the age of 13.¹ Legislation has been introduced multiple times over the past 25 years to update COPPA, including this year. COPPA 2.0, introduced by U.S. Senators Ed Mark and Bill Cassidy, would amend COPPA to strengthen protections related to the online collection, use, and disclosure of personal information of children up to 17 years old.²

Although COPPA is now 26 years old and in need of updating, COPPA's aim to protect children online remains as essential as ever. We now know that children and teens are uniquely vulnerable to online data collection. Young people's brains develop gradually, and they do not become capable of critically assessing what they see online until they are older.³ For example, research shows most children cannot distinguish an ad from content until they are at least 8 years old, and most children do not realize that ads can be customized to them.⁴ This enables businesses to manipulate young people without them even realizing it. Also, children are prone to oversharing without understanding the consequences of doing so.⁵ According to the Children's Commissioner report, children believe the information they share remains on their device or within an app or game, and that deleting it from the device or app will also remove it from the internet.⁶ Another

¹ Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (1998).

² [S.836 - Children and Teens' Online Privacy Protection Act](#)

³ [Common Sense Media COPPA 2.0 One-Pager](#) (2024).

⁴ JOSEPH JEROME & ARIEL FOX JOHNSON, *AdTech and Kids: Behavioral Ads Need a Time-Out*, Common Sense Media (2021), <https://www.common Sense Media.org/sites/default/files/uploads/pdfs/blog/adtech-and-kids-explainer.pdf>.

⁵ COMMON SENSE MEDIA, *supra* note 2.

⁶ CHILDREN'S COMMISSIONER FOR ENGLAND, *Who Knows What About Me? A Children's Commissioner Report into the Collection and Sharing of Children's Data* (Nov. 2018), <https://assets.childrenscommissioner.gov.uk/wpuploads/2018/11/cco-who-knows-what-about-me.pdf>.

research study revealed that children and teens also do not understand that an app may gather information about them from sources outside the app.⁷

The glaring holes in privacy law and protections for children and teens online play a key role in the current U.S. youth mental health crisis.⁸ Companies can collect loads of information about young people and then specifically target them where they are vulnerable and keep them hooked on their devices indefinitely. For instance, according to research from *SuperAwesome*, by the time a child is 13, over 72 million pieces of personal data will have been captured about them.⁹ Tech companies then use this data to serve up algorithmic recommendations and amplify addictive and harmful content, including posts promoting eating disorders and self-harm, to young users with extreme precision. Companies also use manipulative design features, such as personally tailored and targeted feeds, push notifications, endless scrolling, autoplay of videos, and dark patterns to increase their engagement and time on the platforms, ultimately increasing revenue.¹⁰ This is the landscape that has led to the proposed amendments of COPPA.¹¹ The overall goal of COPPA 2.0 is to minimize the data collected about and used on minors.¹² The amendments would expand these protections to teens aged 13-16 by requiring their opt-in consent before data collection and banning targeted advertising to all covered minors.¹³ Lastly, COPPA 2.0 would close a loophole in the original bill that allowed sites and apps to ignore young people using their services and evade compliance.¹⁴

Another federal bill in the US has been proposed several times and focuses on protecting youth online. This bill, the Kids Online Safety Act (KOSA), passed in the United States Senate 91-3 in 2024 alongside COPPA 2.0 as part of the Kids Online Safety and

⁷ KAIWEN SUN ET AL., “They See You’re a Girl if You Pick a Pink Robot with a Skirt”: A Qualitative Study of How Children Conceptualize Data Processing and Digital Privacy Risks, in *Proceedings of the ACM on Human-Computer Interaction* (CHI ’21), May 2021, <https://doi.org/10.1145/3411764.3445333>.

⁸ COMMON SENSE MEDIA, *supra* note 2.

⁹ SUPERAWESOME, *SuperAwesome launches Kid-Safe Filter to prevent online ads from stealing children’s personal data* (Dec. 6, 2018), <https://www.superawesome.com/superawesome-launches-kid-safe-filter-to-prevent-online-ads-from-stealing-childrens-personal-data/>.

¹⁰ COMMON SENSE MEDIA, KOSPA One Pager (Dec. 2024), <https://www.common Sense Media.org/sites/default/files/featured-content/files/kospa-one-pager-2024-updated-12.10.24.pdf>.

¹¹ COMMON SENSE MEDIA, *supra* note 2.

¹² *Id.*

¹³ *Id.*

¹⁴ COMMON SENSE MEDIA, *supra* note 2; ADAM SATARIANO & MIKE ISAAC, *Fortnite Maker to Pay \$520 Million Over Children’s Privacy and Game-Purchase Practices*, N.Y. Times (Dec. 19, 2022), <https://www.nytimes.com/2022/12/19/completeness/ftc-epic-games-settlement.html>, (Epic Games paid \$275 million to settle COPPA violations for collecting personal information from children under 13 who played Fortnite without obtaining verifiable consent from a parent).

Privacy Act (KOSPA). Unfortunately, KOSPA was never brought to the floor of the US House of Representatives and has not become law.

If KOSA were enacted, this important legislation would require companies to design their platforms to prioritize children's and teens' health and well-being over engagement and profits.¹⁵ Importantly, KOSA would impose a “duty of care” on covered online platforms used by minors, requiring “reasonable measures” to mitigate harms like cyberbullying, sexual exploitation, promotion of self-harm, eating disorders, etc.¹⁶ Additionally, platforms would be required to default to the most protective settings for minors, offer tools to disable addictive features, and provide the ability to opt out of algorithmic recommendations.¹⁷ While critics warned that the bill might infringe on children’s access to certain information, KOSA does not require companies to take down or block specific content, and nothing in the act prevents young people from searching for content they are interested in.¹⁸ KOSA also does not prevent young people from communicating with friends or allow state Attorneys General to enforce prevention of or define harms to minors.¹⁹ Instead, KOSA shifts the responsibility to platforms while giving minors and parents more meaningful controls. Unfortunately, the United States Congress has been unable to advance this legislation in the United States House, although it was reintroduced in the United States Senate again in 2025. Common Sense Media is one of over 400 bipartisan organizations that are pushing to advance this legislation this year.²⁰

Because federal action has been slow to expand protections beyond children under 13, many states have stepped in with their own laws or proposed legislation. For instance, New York and California, states with some of the most robust protections for children online, both recently passed laws targeting platforms’ addictive features.²¹ Addictive feeds have an increasingly devastating effect on children and teens, contributing to

¹⁵ COMMON SENSE MEDIA, *supra* note 10; COMMON SENSE MEDIA, KOSA One Pager (Jul. 2024), <https://www.common sense media.org/sites/default/files/featured-content/files/kosa-one-pager-2024-updated-7.16.24.pdf>.

¹⁶ COMMON SENSE MEDIA, *supra* note 15.

¹⁷ S. 1748, 119th CONG. (2025) (introduced May 14, 2025), <https://www.congress.gov/bill/119th-congress/senate-bill/1748/text?utm=>.

¹⁸ OPEN TECHNOLOGY INSTITUTE, “Changes to KOSA Are Improvements, but Congress Must Still Address Remaining Challenges With the Bill, Says OTI,” *New America* (Feb. 16, 2024), <https://www.newamerica.org/oti/press-releases/changes-to-kosa-are-improvements-but-congress-must-still-address-remaining-challenges-with-the-bill-says-oti/>; COMMON SENSE MEDIA, *supra* note 15.

¹⁹ COMMON SENSE MEDIA, *supra* note 15.

²⁰ [#PassKOSA letter](#) (October 2025).

²¹ *Stop Addictive Feeds Exploitation (SAFE) for Kids Act*, S. 7694A, 2023–24 Reg. Sess. (N.Y. 2024), <https://www.nysenate.gov/legislation/bills/2023/S7694/amendment/A?utm=>; Cal. S.B. 976, 2023–24 Reg. Sess. (Cal. 2024) (to be codified at Cal. Health & Safety Code § 27000 et seq.), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB976.

significantly higher rates of youth depression, anxiety, suicidal ideation, and self-harm.²² According to a U.S. Surgeon General report, up to 95% of youth ages 13-17 report using social media, with more than a third saying they use social media “almost constantly.”²³ Meanwhile, through highly addictive, personally tailored, and targeted feeds, social media companies get children and teens to view and engage with their platforms longer and longer with the explicit goal of making money.²⁴ Both New York and California’s bills require social media companies that have child users to automatically disable their notifications between midnight and 6 am, and require parental consent for addictive features to be enabled.²⁵

One of the most popular types of state bills for child online safety is the “age-appropriate design codes” or “AADC laws,” which originated in the UK.²⁶ AADC laws require digital services to default to more protective settings for minors, limit certain design choices (e.g., addictive features, dark patterns), require opt-in for personalized advertising to minors, and require the completion of Data Protection Impact Assessments (DPIAs).²⁷ Five states have passed AADC or “Kids Code” laws including: California, Maryland, Nebraska, South Carolina, and Vermont. Common Sense Media has been active in the successful passage of each of these laws - and has also worked to defend some of them as they are challenged in the courts.²⁸ Some of the features of AADC laws, such as restricting minors from getting targeted ads or disabling precise geolocation, have made their way into other states’ laws, like Texas’s recently passed *Securing Children Online Through Parental Empowerment Act*.²⁹

²² COMMON SENSE MEDIA, SAFE for Kids Act Fact Sheet (Jun. 2024), <https://www.common sense media.org/sites/default/files/featured-content/files/safe-for-kids-act-updated-6-4-24-one-pager.pdf>.

²³ U.S. DEP’T OF HEALTH & HUMAN SERVS., Office of the Surgeon General, *Social Media and Youth Mental Health: The U.S. Surgeon General’s Advisory* (2023), <https://www.hhs.gov/sites/default/files/sq-youth-mental-health-social-media-advisory.pdf>.

²⁴ COMMON SENSE MEDIA, *supra* note 23.

²⁵ COMMON SENSE MEDIA, *supra* note 23; COMMON SENSE MEDIA, CA Social Media Youth Addiction Law (Skinner) One Pager (2024), <https://www.common sense media.org/sites/default/files/featured-content/files/ca-social-media-youth-addiction-law-skinner-one-pager-2024.pdf>.

²⁶ Lynn P. Dupree & Laura E. Brashear, *Age-Appropriate Design Codes: A New Wave of Online Privacy Legislation?*, FINNEGAN (Oct. 1, 2024), <https://www.finnegan.com/en/insights/articles/age-appropriate-design-codes-a-new-wave-of-online-privacy-legislation.html>; Tracy Shapiro et al., *Nebraska and Vermont Pass Age-Appropriate Design Codes*, WSGR DATA ADVISOR (June 24, 2025), <https://www.wsgr.com/en/insights/nebraska-and-vermont-pass-age-appropriate-design-codes.html>; Tracy Shapiro et al., *Maryland Passes Age-Appropriate Design Code*, WSGR DATA ADVISOR (May 21, 2024), <https://www.wsgr.com/en/insights/maryland-passes-age-appropriate-design-code.html>.

²⁷ Dupree & Brashear, *supra* note 27; Shapiro et. al., *supra* note 27; Shapiro et. al., *supra* note 27.

²⁸ Common Sense Media *Amicus Brief in Support of Attorney General Bonta*, *Netchoice v. Bonta*, No. 5:22-cv-08861-BLF (July 2025).

²⁹ *Texas’s Securing Children Online Through Parental Empowerment (SCOPE) Act*, H.B. 18, 88th Leg., Reg. Sess. (Tex. 2023), <https://www.capitol.texas.gov/tlodocs/88R/billtext/pdf/HB00018H.pdf>.

There are also broader US laws and proposed legislation that aim to address unfair practices in digital markets that affect all consumers, not only children. For instance, the Federal Trade Commission Act gives the FTC broad authority to prevent “unfair or deceptive acts or practices” in commerce, including online. While not explicitly phrased in terms of “digital fairness,” this authority has been, and increasingly so, continued to be used to challenge manipulative practices, misleading digital interfaces, and deceptive disclaimers. The FTC is also evaluating dark patterns and has taken enforcement actions, including filing lawsuits and sending warning letters, against platforms that manipulate user consent, bury opt-outs, or mislead through interface design.³⁰ While not always through formal legislation, this regulatory activity acts as a de facto guardrail.

These concerns about consumer autonomy have also been seen in state and federal law in the US. The California Privacy Rights Act, which was passed in 2020 as an amendment to the California Consumer Privacy Act, includes an explicit definition of “dark pattern” as “a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice.”³¹ CPRA prohibits obtaining consent through dark patterns, and specifically indicates that “agreement obtained through use of dark patterns does not constitute consent.”³² Likewise, in the Colorado Privacy Act, consumer consent is not valid consent if the agreement was obtained through the use of “dark patterns.”³³ Common Sense Media provided comments to this act and recommended going further than dark patterns as related to consent and recommended “prohibiting asymmetric platform design practices that limit users’ ability to change user settings, delete personal data, or delete their personal account.”³⁴ In New York this year, in the proposed rulemaking for the New York SAFE for Kids Act, the use of dark patterns is also prohibited and has been identified as being “incompatible with an individual’s ability to provide valid consent.”³⁵ This echoes similar language in the bipartisan federally introduced DETOUR Act, which was last introduced last year in the 118th Congress and, if passed, would make it unlawful for large online companies “to design, modify, or manipulate a user interface with the purpose or substantial effect of obscuring, subverting, or impairing user autonomy, decision-making, or choice to obtain consent or use data.”³⁶

³⁰ FTC Report Shows Rise in Sophisticated Dark Patterns Designed to Trick and Trap Consumers, <https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-report-shows-rise-sophisticated-dark-patterns-designed-trick-trap-consumers>

³¹ [California Sec. 1798.140\(l\)](#). (2018).

³² *Id.*

³³ [Colorado Privacy Act](#) - Senate Bill 21-190 (2021).

³⁴ [Colorado Privacy Act - Common Sense Media submitted comments for rulemaking](#) (2022).

³⁵ [New York SAFE for Kids Act](#) (2024).

³⁶ [S. 2708 - DETOUR Act](#) (2023-2024).

Common Sense Media commends the Commission for the work they have done in considering AI within digital fairness - and we understand that the EU's AI Act does provide guardrails in this space. However, we would encourage the Commission to go further in the Digital Fairness Act by developing regulations specifically addressing the use of AI companion chatbots with particular attention to manipulative design practices and the preservation of user autonomy.³⁷ The use of AI is already so prevalent among consumers, but particularly among teens. Our research, released earlier this year, revealed that seventy-two percent of teens have used AI companions at least once, and over half of these teens use the platforms at least a few times a month.³⁸ AI companions include both dedicated companion apps like Character.AI and general-purpose chatbots like ChatGPT when they are capable of being used for mental health support or emotional support. In particular, the ability of general-purpose chatbots to be used by users for emotional support alongside information retrieval or efficiency increases the risk that young users form emotional attachments and perceive chatbot responses as authoritative, personalized guidance.

We know that AI companion chatbots have already caused documented harm to both adults and children from horrific stories of children who took their own lives because of their interactions with these chatbots. These harms are not incidental; they are the direct result of design choices that are being made by these AI companies that intentionally simulate social attachment and emotional intimacy. These harms and the manipulative design of these platforms led Common Sense Media to conduct independent risk assessments of several of these AI products. These risk assessments have concluded that these products are not safe for minors.³⁹ This is why, earlier this year in California, Common Sense Media championed the Leading Ethical AI Development (LEAD) for Kids Act to establish risk based audits for all AI products that would impact children, require transparent reporting for all adverse incidents, consumer facing labels, privacy protection for children's inputs, and included restrictions on dangerous AI products including AI companion chatbots.⁴⁰ This comprehensive approach would place common sense guardrails on AI products - ensuring that the tools used by children are, above all, safe for children.

³⁷ Common Sense Media, [Social AI Companion Risk Assessment](#) (2025).

³⁸ Common Sense Media, [Talk Trust and Trade-Offs: How and Why Teens Use AI Companions](#) (2025).

³⁹ Common Sense Media, [AI Risk Assessments](#) (2025).

⁴⁰ California, [AB-1064 Leading Ethical AI Development \(LEAD\) for Kids Act](#) (2025-2026)

CONCLUSION.

Common Sense Media strongly supports the Commission's commitment to advancing digital fairness and protecting consumers, especially the most vulnerable consumers - children and teens - from manipulative and unsafe digital environments. Around the world, young people face increasing risks from exploitative design practices, excessive data collection, and emerging AI technologies that can undermine their safety, privacy, and autonomy.

As the Commission considers new rules to ensure fairness in the digital marketplace, we urge continued attention to child-specific risks, particularly those stemming from AI-driven systems and manipulative design. By centering youth safety, transparency, and autonomy in the design of digital and AI systems, the Commission can help ensure that innovation serves the best interests of children, not at their expense. Common Sense Media stands ready to support this work and to share our research and policy expertise as the EU advances its efforts to make technology safe and fair for all.