



TO: The European Commission Directorate-General
for Communications Networks, Content, and
Technology

FROM: Common Sense Media

DATE: 15 June 2025

RE: [Protection of Minors Guidelines Response Request](#) - Pursuant to Article 28 of the Digital Services Act (DSA)

Introduction:

Common Sense Media is the leading international nonprofit organisation working on behalf of children and teens to make their world healthier, safer, and more equitable. Backed by the research that's the foundation of everything we do, we champion quality media that entertains and inspires, and support legislation that aims to close the digital divide and hold social media platforms accountable. 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 the release of the Digital Services Act (DSA) guidelines. Common Sense supports the Commission's efforts to protect the safety of minors online and with these comments we seek to offer constructive suggestions and evidence to support the Commission's guidance so that the Commission can guide providers so that they can ensure a high level of privacy, safety and security for minor users on their platforms.

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 - Part 3: Comments per section:

Risk Review

In considering risk review or when a provider of an online platform accessible to minors is determining which measures are appropriate and proportionate to ensure a high level of safety, privacy, and security to minors on their platform Common Sense Media agrees it is essential to distinguish between the risk of the platform to minors - and as has been identified by the Commission - how likely it is that minors will access it's service. This means that age assurance, which is proportional to the risks involved for minor users, is essential. The situations in which

platforms and lawmakers have sought age assurance vary. Primarily, these situations fall into three categories: design, access, and privacy.

As the reasons for seeking age assurance vary, so do the consequences of assurance procedures getting age wrong. Concerns about age assurance leading to privacy protections for everyone, or limiting addictive features for everyone, may be less problematic than if age assurance unwittingly cuts off access to an adult making a desired purchase or obtaining desired content. This is why one of the key considerations in determining which age assurance method is most viable or appropriate in a given situation should be whether the chosen method has the potential to limit access to products or content for adults, and what measures have been taken to mitigate this issue.

When considering age assurance related to a minor's privacy, the key consideration is whether the minor user's data is being protected. This includes avoiding profiling, targeted ads, and the commercialisation of data. According to the guidance provided by the Commission, when conducting this review, providers of online platforms accessible to minors should always be guided by the best interests of the minor. The risk involved here is primarily dependent on the platform's default settings, and what happens if a user is misidentified as either an adult or a minor. For example, when an age assurance method is used, and the method identifies the user as a minor, but the user is not a minor, if the settings are set at heightened privacy by default, this would mean that the consequence of the age verification getting the user's age wrong is that the user's data would enjoy heightened privacy protection. This is a relatively low-risk situation. Likewise, when considering product and design features, the risk is relatively low if the default settings are high, for example, those that limit addictive features like notifications and auto-scroll, or unhealthy features like algorithmic targeting and plastic surgery filters. However, if these safety settings are not set by default, the risk of harm to a user (particularly a minor user) is significantly greater, as the consequences of the age assurance method getting the age wrong could include the minor accessing harmful content or design features. Finally, when considering access to social media platforms in general or even riskier, adult content such as pornography, violence, gambling, and contact with strangers, it is essential that the age assurance method is accurate, not unduly to burden adult users, but also to protect minor users.

Age Assurance

As indicated in the comments regarding risk reviews, we appreciate the Commission's emphasis on risk to minors. We agree with the Commission in that a risk assessment is important to ensure that "any restriction to the exercise of fundamental rights and freedoms is proportionate." Last year, we published a white paper on age assurance, which examined youth online protection and age assurance efforts in the U.S, reviewed the history of age assurance, considered current mechanisms of age assurance, what kids are experiencing on social media platforms, and what

lawmakers are motivated to fix.¹ We encourage the Commission to review this white paper, as it provides an analysis of the different age assurance methods available for use.

Additionally, in providing comments on New York state's SAFE for Kids Act,² enacted in 2024, we emphasised the need for any age assurance method used to be "commercially reasonable and technically feasible."³ We further expressed that the SAFE for Kids Act should weigh the risk of harm to kids associated with the platform as well as the risk of negative consequences related to the age assurance method (often claimed to be a violation of the user's First Amendment rights in the form of limiting access to information content or free speech).

Registration

In Section 6.2 of the guidelines, the Commission has required that "where registration is required or offered as a possibility to access an online platform accessible to minors, the Commission has required that the platform takes measures so that the minor user is aware of the risks and benefits of registration." In the Kids Online Safety Act (KOSA), which was reintroduced in the United States Senate this year, notice to users is also a requirement. Specifically, in Section 104. Disclosure, notice is required to be provided to minor users in a clear, conspicuous, and easy to understand manner that include the policies and practices of the covered platform concerning safeguards for minors; information about how to access the safeguards and parental tools required under the Act; and notice about how to access the information on personalized recommendation systems needed.⁴

Default Settings

Common Sense Media appreciates the emphasis on default settings in the guidance from the Commission. In the United States, several laws have been passed and legislation considered at both the state and federal levels, which include requirements ensuring that privacy, safety, and security by design principles are consistently applied to all account settings for minors.

The KOSA legislation introduced this session in the United States Senate includes several provisions that are aligned with the Commission's guidelines related to default settings. Specifically, section 103 Safeguards for Minors includes several readily accessible and easy-to-use safeguards that a covered platform shall provide to a user or visitor that the platform knows is a minor, including: limiting the ability of other users or visitors to communicate with the minor; preventing other users or visitors, whether registered or not, from viewing the minor's personal data collected by or shared on the covered platform, in particular restricting public

¹https://www.common sense media.org/sites/default/files/featured-content/files/2024-us-age-assurance-white-paper_final.pdf

² <https://www.nysenate.gov/legislation/bills/2023/A8148/amendment/A>

³<https://www.common sense media.org/sites/default/files/featured-content/files/safe-for-kids-act-comments.pdf>

⁴ <https://www.congress.gov/bill/119th-congress/senate-bill/1748/text>

access to personal data; limiting by default design features that encourage or increase the frequency, time spent, or activity of minors on the covered platform, such as infinite scrolling, auto playing, rewards for time spent on the platform, notifications, and other design features that result in compulsive usage of the covered platform by the minor; control personalized recommendation systems, including the ability for a minor to have— (i) a prominently displayed option to opt out of such personalized recommendation systems, while still allowing the display of content based on a chronological format; and (ii) a prominently displayed option to limit types or categories of recommendations from such systems; and restrict the sharing of the geolocation of the minor and provide notice regarding the tracking of the minor's geolocation.⁵ Additionally, a covered platform shall provide a user that the covered platform knows is a minor with a readily accessible and easy-to-use option to limit the amount of time spent by the minor on the covered platform.⁶ Finally, a covered platform shall provide that, in the case of a user or visitor that the platform knows is a minor, the default setting for any safeguard shall be the option available on the platform that provides the most protective level of control that is offered by the platform over privacy and safety for that user or visitor, unless otherwise enabled by the parent of the minor.⁷

Additionally, in New York and California, legislation was enacted in 2024 that by default limits the social media platforms ability to use addictive feeds that keep kids glued to their devices, and it prevents companies from waking kids at all hours of the night with notifications and pings from addictive feeds, unless parents' consent. In New York's law, the Stop Addictive Feeds Exploitation (SAFE) for Kids Act, these settings are by default for all users until it is determined by the platform that the user is not a minor.⁸ Finally, this year in New York, the New York Children's Online Safety Act (NY COSA) was introduced. Although it did not pass the legislature this year, NY COSA demonstrated the momentum this type of regulation has in statehouses. In the NY COSA bill, kids and teens would have been protected online by limiting how strangers interact with minors on social media and gaming platforms with chat functions. These restrictions include direct messaging, profile visibility, and financial transactions. It also limits the use of manipulative design practices referred to as "dark patterns."

Recommender Systems and Search Features

Common Sense Media commends the Commission for recognising that these social media companies use addictive feeds to encourage kids and teens to view and engage with platforms for more extended periods, thereby generating greater profits. For social media companies, time online equals more money. Addictive feeds have had an increasingly devastating effect on children and teens, contributing to significantly higher rates of youth depression, anxiety, suicidal ideation, and self-harm.

⁵ Id.

⁶ Id.

⁷ Id.

⁸ <https://www.nysenate.gov/legislation/bills/2023/S7694/amendment/A>

By prioritising ‘explicit user-provided signals’ over ‘implicit engagement-based signals’ to determine the content displayed and recommended to minors, the Commission has required that such signals should be justified in the best interest of the minor, which will help to ensure that the signals contribute to a high level of safety and security for minors. As mentioned in the default settings section (above), the New York SAFE for Kids Act and California’s Social Media Youth Addiction Law are state laws in the United States that limit social media companies’ ability to use addictive feeds that keep kids glued to their devices.⁹ These laws provide teenagers with a healthier online experience by prioritising content that the minor user is seeking, or has been determined to be sought, using explicit user-provided signals. Currently, with all of the “engagement-based signals,” such as the targeted advertising and content that an algorithm determines a user should see, feeds are loaded with content that the user didn’t choose.

Significantly, neither of these laws limits the platforms’ ability to moderate harmful content from a feed. Both laws explicitly state that the rules should not be construed as preventing any action taken in good faith to restrict access to or availability of media that the operator of an addictive social media platform considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected.

Finally, unlike the guidance of the Commission under the DSA, both the New York and California laws do not limit users’ ability to search for material that interests them. Due to First Amendment considerations in the U.S., under both laws, there is a rule of construction that allows users to search for any content they would like to see. These laws restrict no content. In New York, the law specifically allows for “implicit engagement-based signals,” so content is provided when “the user expressly and unambiguously requested the specific media or media by the author, creator, or poster of the media.” These laws in California and New York elevate the content the user is actually seeking by excluding the ability for the platform to choose the content that is to be displayed.

Tools for Guardians

The Commission has done a commendable job of identifying concerns with effective and child-friendly user reporting, feedback, and complaint tools that enable minors (and their guardians) to express and address issues with online platforms. In the United States we have considered the same concerns and therefore in KOSA, there are reporting tools that the covered platforms shall provide that include: a readily accessible and easy-to-use means for users and visitors to submit reports to the covered platform of harms to a minor on the covered platform; an electronic point of contact specific to matters involving harms to a minor; and confirmation of the receipt of such a report and, within the applicable period described, and a substantive response to the individual that submitted the report. Furthermore, as far as the timing of such reports, a covered platform shall establish an internal process to receive and substantively respond to such reports in a reasonable and timely manner, but in no case later than – 10 days after the receipt of

⁹ https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB976

a report, if, for the most recent calendar year, the platform averaged more than 10,000,000 active users every month in the United States; 21 days after the receipt of a report, if, for the most recent calendar year, the platform averaged less than 10,000,000 active users every month in the United States; and if the report involves an imminent threat to the safety of a minor, the report should be addressed as promptly as needed to address the reported threat to safety.¹⁰

Transparency

Common Sense Media also commends the Commission for placing such an emphasis on transparency in the guidelines. In several bills proposed in the U.S., like KOSA, there are transparency requirements. In KOSA these requirements include: an assessment of the extent to which the platform is likely to be accessed by minors; a description of the commercial interests of the covered platform being used by minors; an accounting, based on the data held by the covered platform, of— the number of users using the covered platform that the platform knows to be minors in the United States; the median and mean amounts of time spent on the platform by users known to be minors in the United States who have accessed the platform during the reporting year on a daily, weekly, and monthly basis; and the amount of content being accessed by users that the platform knows to be minors in the U.S. that is in English, and the top five non-English languages used by users accessing the platform in the United States; an accounting of total reports received through the reporting mechanism included in the Act, disaggregated by language, including English and the top five non-English languages used by users accessing the platform from the United States; and an assessment of the safeguards and parental tools representations regarding the use of the personal data of minors, and other matters regarding compliance with the law.¹¹

Additionally, we regularly encourage legislators in the U.S. to continue advocating for greater transparency in their legislation, as researchers need to understand the breadth and depth of harm to children to comprehend the extent of the issue entirely.

Conclusion

Common Sense Media believes that meaningful regulation is critical to our broader mission of protecting children and teens in the digital world. Moreover, strong global collaboration among regulators, civil society, and the tech industry is particularly crucial in addressing common pain points, such as age assurance, which can help enforce child safety policies effectively. To that end, we applaud the Commission's global engagement, regulatory progress to date, and investment in ample resources to help address these complex challenges.

¹⁰ Id.

¹¹ KOSA