



## Additional contribution to the targeted public consultation on the protection of minors guidelines under the Digital Services Act

June 2025

*The [National Center for Missing & Exploited Children](#) (NCMEC) offers these comments—including links to relevant resources—on the specified sections of the draft guidelines as an additional contribution to the consultation survey.*

### Section 6.1: Age assurance

*Comment:* Highly effective age assurance is a shared responsibility. The proposed guidelines for online platforms about age assurance are appropriate but insufficient, standing alone, without similar responsibilities imposed on app store operators, OS developers, and device manufacturers.

In April 2025, NCMEC briefly addressed this age assurance position in its written responses to questions for the record asked by members of a [U.S. Senate subcommittee](#).

### Section 6.3: Default settings

*Comment:* The proposed guidelines indicate that providers should design default settings to ensure that “No account, except the minor’s, can download or take screenshots of content uploaded or shared by the minor to the platform” (**line 400**). This may require some technically compatible engineering by OS developers and/or device manufacturers to grant apps the ability to disable screen capturing/recording functions on the device. Because the guidelines apply to online platforms (and not OS developers or device manufacturers), this may be a gap that creates an obligation/expectation dependent on out-of-scope third parties for compliance. An additional gap may exist when online platforms are accessed through a web browser instead of a platform-specific app.

*Comment:* The proposed guidelines indicate that providers should “Ensure that minors are not in any way encouraged or enticed to change their settings to lower levels of privacy, safety and security” (**line 430**). This guideline needs clarification. While the context suggests that it is intended to prohibit online platforms from encouraging or enticing a minor to change settings, it is not clearly stated which parties bear this responsibility. Additionally, the text itself (“...in any

way...” is expansive and suggests that the online platform must prevent anyone—an advertiser, another user, etc.—from encouraging or enticing a minor to change their settings, without detailing or providing tools to accomplish this mandate.

NCMEC has published a statement about [online platforms’ responsibilities](#), including discussion of default setting practices that vary by jurisdiction, on its [Global Platform for Child Exploitation Policy](#). Survivor perspectives included in that statement also affirm the importance of clear, consistent, and effective privacy settings for children online.

## **Section 6.7: Moderation**

*Comment:* The proposed guidelines address the importance of preventing prompts from being introduced into generative AI systems that are harmful to minors’ privacy, safety and/or security **(line 709)**. Generative AI systems should integrate stringent safeguards that detect and prevent both inputs (prompts) and outputs that harm minors.

NCMEC has published statements about [generative AI child sexual abuse material](#) (GAI CSAM) and called for [prevention measures in generative AI services](#) on its [Global Platform for Child Exploitation Policy](#). Survivor perspectives included in those statements stress the reality of harms associated with generative AI CSAM and the importance of prevention in generative AI services.

## **Section 7.3: Tools for guardians**

*Comment:* The proposed guidelines describe “real time” notification to a minor user that a monitoring function has been activated by an authorized guardian **(line 858)**. Such notifications may introduce increased vulnerability and incentivize secrecy by allowing minor users to feel free to engage in inappropriate or risky conduct when monitoring is inactive, knowing that they could quickly change behavior (disconnecting from a particular gaming server, ending a chat, deleting shared images, etc.) upon receiving a “real time” notification that monitoring functionality is activated. Instead, consider suggesting a notification scheme that indicates only whether such monitoring functionality has been enabled on a minor’s account. This provides transparency to minor users that their online activity is subject to monitoring by guardians at any time, thereby encouraging more appropriate online conduct at all times.

NCMEC has published additional recommendations—including in [this blog post](#) and through its [NetSmartz](#) program—for parents and guardians to promote children’s online safety.

▪