CELE
Centro de Estudios en Libertad de Expresión y Acceso a la Información

Documento de posición

20

Submission in response to the Call for Evidence for the development of guidelines for the protection of minors under Article 28 (4) of the DSA

CELE

Septiembre 2024

CELE, Submission in response to the Call for Evidence for the development of guidelines for the protection of minors under Article 28 (4) of the DSA, Documento de posición No. 20, Centro de Estudios en Libertad de Expresión (CELE), Buenos Aires (2024)

Facultad de Derecho
Centro de Estudios en Libertad de Expresión y Acceso a la Información

UP
Universidad de Palermo

CELE's Submission in response to the Call for Evidence for the development of guidelines for the protection of minors under Article 28 (4) of the DSA

September 30, 2024
Buenos Aires, Argentina

The Center for Studies on Freedom of Expression and Access to Information (CELE) is an academic research center affiliated with Universidad de Palermo in Argentina. The Center provides technical and legal analysis on issues affecting this fundamental right, and since 2012 has been studying freedom of expression on the Internet as a specific research area. The Center is a leading voice on the promotion and protection of freedom of expression nationally, regionally, and internationally.

This submission was prepared in response to the Call for Evidence for the development of guidelines for the protection of minors under Article 28 (4) of the DSA. It aims to contribute to the efforts of the European Commission in implementing these obligations, with an analysis that emphasizes minors' freedom of expression and privacy.

According to Article 24 (2) of the European Charter of Fundamental Rights, public and private entities must put the rights of minors at the heart of any action they take that can affect their interests. Children are entitled to all protection and care as necessary for their well-being. Article 24 (1) of the Charter recognizes children's right to express their views freely.

Several provisions in the Digital Services Act are concerned with the protection of Children. Among them, article 28 establishes general due diligence obligations for providers of online platforms accessible to minors. It requires them to set up appropriate and proportionate measures to ensure they enjoy high levels of privacy, safety, and security. Accordingly, the DSA provides that VLOPs and VLOSEs must include any actual or

foreseeable negative effects concerning the protection of minors in their risk assessments under Article 34[1], and mitigate them accordingly[2].

Systemic risks to minors

The DSA mandates VLOPs and VLOSEs to assess and mitigate any actual or foreseeable negative effects concerning the protection of minors[3]. This vague language should be narrowed down so these companies know exactly what is expected of them. Not doing so will create incentives for VLOPs to limit their legal exposure, by either over removing content that can be considered not appropriate for kids or blocking it for users of certain age groups. Several human rights organizations are making this point in the United States regarding the Kids Online Safety Act (KOSA) bill in the United States (CDT et al). This could have a disparate impact on certain kinds of legal, even desirable content. Under such a law, *"it will be harder for suicide prevention messages to reach kids experiencing acute crises, harder for young people to find sexual health information and gender identity support, and generally, harder for adults who don't want to risk the privacy- and security-invasion of age verification technology to access that content as well"* (Kelley and Mackey).

Children's autonomy and parental controls

Not all content is suitable for all ages, and the DSA acknowledges this by mandating the establishment of parental controls and digital age verification measures. However, any restriction on the activities that minors can do online must be reconciled with their rights. As children become more autonomous and capable of making informed decisions, the basis for protecting their rights evolves – from safeguarding their interests to upholding their choices (Brennan). The United Nations Convention on the Rights of the Child guarantees the freedom of Children to access information, which is an essential condition for the progressive

[1] Digital Services Act, article 34.1(d)
[2] Digital Services Act, article 35 (1)
[3] Digital Services Act, article 34.1(d) and 35.1

acquisition of their autonomy, understood as the "series of abilities that enable them to make life choices appropriately and independently" (Freeman, 1997). Adolescence must be respected as a key stage in human development, in which youth seek independence from parents and experience greater needs to express their identity in public and connect with their peers (Meeus et al). As a result, any parental controls put in place by companies must consider that older children have the right and need to be exposed to a greater range of content than younger ones, according to their evolving capacities (UNICEF, 2018). This aspect could be considered a mitigation measure as it contributes to the gradual acquisition of digital literacy and the ability to identify disinformation, deepfakes, etc, in newer generations of internet users. Moreover, parental controls should be presented as facilitators of dialogue instances between older children and guardians on which content they want to see online.

Since not all adults have the necessary skills to use parental controls in a way that can protect children's safety effectively, the guidelines should instruct platforms to design easy-to-use parental controls and to provide adults with user-friendly video or written tutorials. The availability of parental controls and other tools to protect minors should feature prominently in the platform's interface. While the mandatory establishment of parental controls is an important step forward, it is also key that neither the platforms nor the state replace parents and guardians in having the final say on which contents are appropriate for their children.

Under Article 14 (3) of the DSA, providers of intermediary services primarily directed at minors or predominantly used by them must provide children with explanations for their terms and conditions that they can easily understand[4]. Respect for children's developing autonomy entails that younger minors have access to simpler versions of these explanations, while older adolescents can access longer, more complex ones.

[4] Also see recital 46 of the DSA

Children's privacy and parental controls

The right to privacy in Article 16 of the Convention on the Rights of the Child encompasses their right to know if their parents monitor their online behavior. Conversely, children ought to know what kind of control their guardians exert on what content they are allowed to see. Guidelines should require platforms to explain any restrictions imposed on them by parental controls in ways minors of different age groups can easily understand.

Children's Autonomy and AI-driven Safety solutions

A comprehensive study exploring children's responses to AI-driven cyberbullying interventions uncovered nuanced perspectives on personal agency and technology's role in online safety (Milosevic et al., 2023). Many children expressed a preference for handling cyberbullying situations independently, viewing individual responsibility as a key factor in addressing such challenges. This inclination reflects a broader concern among young people about maintaining autonomy in digital spaces, which they perceive as essential to their personal growth and resilience.

The study also highlighted the potential risks of over-reliance on AI in managing online safety, particularly regarding proactive content moderation. While AI technologies can effectively detect and mitigate harmful behaviors, the findings suggest that automated interventions must be carefully balanced with efforts to empower children to resolve conflicts autonomously. This approach is crucial for fostering what researchers term "digital resilience"—the capacity to navigate online environments with confidence and self-reliance—.

The implications of this research are significant, especially in the context of policies that lean heavily on technological solutions for online safety. An overly technological approach may inadvertently stifle the development of critical social skills, such as conflict resolution and peer negotiation, which are vital for children's social and emotional development. Moreover, the study warns that focusing exclusively on protection mechanisms could overlook children's right to participation, which is enshrined in the United Nations

Convention on the Rights of the Child (UNCRC). As per UNCRC Article 12, children have the right to express their views, feelings, and wishes in all matters affecting them, and to have their views considered and taken seriously. When applied to the digital environment, this could be understood as the right for minors to have some sort of involvement in managing their online experiences by being consulted on matters that concern them.

Therefore, while AI-based systems offer substantial advantages in identifying and responding to cyberbullying, this research underscores the importance of integrating these technologies with strategies that promote children's active participation. Such integration could prevent the inadvertent creation of a disempowering environment, ensuring that technology serves to complement rather than replace the crucial human element in online safety practice.

Privacy Risks in the use of age assurance mechanisms

While intended to be a solution to protect minors online, age verification systems suffer from several shortcomings that undermine the privacy and security of users. As outlined by Kelley & Schwartz (2023), the ability to browse the Internet anonymously is fundamental to freedom of expression and privacy online, and age verification mandates pose a significant threat to this freedom. Thus, any age verification method that forces users to reveal identity documents to access websites would have a chilling effect on open and unfettered participation in online discourse. Anonymity allows people, especially those seeking sensitive information or expressing unpopular opinions, to participate in online discourse without fear of retaliation or discrimination. Removing this layer of protection could silence critical voices and undermine the free exchange of ideas that characterizes an open and democratic Internet.

No age verification method is foolproof, and all have limitations in terms of their reliability, coverage, and respect for privacy. Rather than providing an effective solution, age verification mandates could create a false sense of security while exposing users to unnecessary privacy risks.

The DSA establishes guidelines for privacy protection and age verification on online platforms accessible to minors. Under Article 28, the DSA mandates that platforms implement appropriate and proportionate measures to ensure high levels of privacy, safety, and security for minors. However, under Recital 71, the DSA **disincentivizes** the use of profiling tools for age verification, which are typically employed by platforms to estimate a user's age based on their behavior. Instead, the DSA encourages the design of default settings that respect privacy and adopt age-appropriate standards and codes of conduct. Recital 71 also emphasizes that prohibiting targeted advertising to children should not incentivize platforms to collect age data, discouraging invasive data practices. Similarly, the OECD (2021) warns that increased data collection for age determination and identity verification can exacerbate privacy risks, aligning with concerns raised by privacy advocates.

Despite these limitations, Article 35(1)(j) of the DSA allows for age verification as a risk mitigation tool specifically for Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs), such as YouTube, Instagram, and TikTok, when addressing systemic risks to children's rights. This provision requires that age verification methods be reasonable, proportionate, and tailored to the specific risks while respecting fundamental rights. Under the GDPR, age-based consent is a critical factor in data processing, further complicating the question of how platforms can accurately determine a user's age without violating their privacy.

This is a question that should be addressed carefully, without falling into false dychotomies. Less privacy means more vulnerability and less safety. All age verification techniques affect users' privacy. Generally, the more accurate age-verification techniques are, the more invasive they turn out to be for users' privacy. Document-based techniques are uniquely disproportionate to users' privacy interests and should be discouraged.

Implementing Age Verification with Caution

When risks justify the need for age verification, the level of accuracy in the verification process should align with the severity of the risks associated with the service. The more

accurate and reliable the age verification, the more invasive it tends to be. For example, methods that provide a high degree of certainty about a user's age often require official documentation, which can expose users to identification risks such as profiling or identity theft. Therefore, only services presenting significant risks to children should rely on such verification methods, while lower-risk services could require users to self-declare their age without further verification (Sas & Mühlberg, 2024). Additionally, as highlighted by Beltrán & de Salvador (2024), age assurance technologies themselves carry inherent risks, as they often lead to the collection of more personal data than necessary, creating "parallel identity frameworks" that may be used for purposes beyond age verification, including microtargeting.

Moreover, before implementing age verification, VLOPs and VLOSEs should consider less intrusive alternatives, such as parental controls. However, these alternatives are not without limitations. As noted by Smirnova, Livingstone, & Stoilova (2021), while parental control tools can offer parents a sense of security, relying solely on control and restriction without enabling mediation can backfire, negatively affecting parent-child relationships and children's autonomy. The authors stress the importance of holistic approaches that prioritize open communication, child participation, and the development of digital resilience while acknowledging the evolving capacities and needs of children in digital environments.

Third-party age verification solutions, while effective, also raise concerns about privacy risks and the costs involved for businesses. Such tools often involve gathering and processing sensitive personal data, such as identity documents or biometric data. This collection creates inherent risks of data breaches, online tracking, and potential misuse of personal information for surveillance or advertising purposes, as underscored by European Digital Rights (EDRi) (2023) in a recent position paper. Moreover, the same document points out that relying on third parties to handle this sensitive data raises concerns about transparency, accountability, and potential retention of data beyond what is necessary for age verification: it is not always clear how these companies handle, store, and use the data collected during the verification

process. This lack of transparency can leave users vulnerable to illegal or unethical data practices, or misuse of their information without their knowledge or consent.

Encryption and anonymity for child safety

The Convention on the Rights of the Child recognizes that children have a right to privacy. Article 16 states that "[n]o child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, or correspondence, nor to unlawful attacks on his or her honour and reputation". Encryption, anonymity, and pseudonymity are central aspects of the protection of the right to privacy, enshrined in Article 8 of the ECHR and Article 17 of the ICCPR. Under international Human Rights Law, states cannot interfere with privacy unless by law and if necessary in a democratic society.

Some argue that end-to-end encryption cuts against child safety, as it operates as a barrier to the detection of the spread of CSAM materials via private messaging. They point to an inherent tension between privacy and child safety. However, we want to emphasize the importance of encryption as a tool for the protection of children.

Encryption is a centerpiece to children's online safety, for "[c]hildren's digital communications contain personal information. If that were to fall into the wrong hands, it could jeopardize both their privacy and safety" (UNICEF, 2020). As we established earlier, children also have a right to freedom of expression. Private, secure communications are essential to its enjoyment. When communications are not private, people –including children– tend to self-censor themselves. This is especially critical in adolescence, a state where minors tend to feel the need to express themselves publicly and assert various aspects of their personality within their peers.

The same is true for anonymity and pseudonymity. Any limitations on the possibility of communicating anonymously online constitute a serious threat to the right to privacy of both adults and children alike and produce a chilling effect on online discussion.

Conclusions

We consider this call for evidence a unique opportunity for the European Commission to learn from the experience gained elsewhere and avoid the mistakes that other legislations and bills around the world have already made. While it is undisputed that child safety must be a priority in government action, there is no unanimity as to what it entails in terms of concrete rules for online platforms. We believe that the European Commission's efforts to protect children online should reflect the values championed by the DSA: thus, they should be conducted in strict compliance with international human rights law, especially the right to privacy and freedom of expression of children. The following key takeaways should inform the discussion on the appropriate guidelines for child protection under the DSA.

1. The enjoyment of high levels of privacy, safety, and security online by children cannot be achieved through restrictive legislation only, as is the case with their enjoyment offline. While lawmakers and platforms can play a part in making the internet a safer place for children, their influence must not be overstated, for it is the empowerment of the children themselves and their guardians that can make a difference.
2. The vague language in Article 34 of the Digital Services Act could serve as an incentive for an over-removal of content that is legal but inappropriate for minors. To avoid this, the European Commission should provide guidance to VLOPS and VLOSEs so they know exactly what they are expected to do.
3. The state should not claim the power to decide what is safe for children to see online. Parental controls must be implemented with caution, leaving the guardians with the final decision on the content to which children will be exposed.
4. The design of parental control tools ought not to foreclose the open dialogue that must exist between children and their guardians over the kinds of content they are allowed to see online.
5. Access to information is crucial in the progressive development of children's autonomy. Therefore, parental controls must acknowledge that adolescents need to be

exposed to a wider range of content than younger children, including some unpleasant content, while allowing for some monitoring from their parents.

6. As a result of their right to privacy, minors, especially teenagers, must be informed all the time that they are under parental control systems.
7. Overreliance on AI tools can create a whole series of new problems and must be carefully balanced with efforts to empower children to resolve conflicts autonomously.
8. End-to-end encryption is not a risk but a critical tool for the privacy and safety of internet communications that benefits all internet users, including children. Therefore, regulators must not require or accept any carveout for encryption in communications, since that would unlawfully impinge upon the right to privacy of minors and adults alike.
9. No exceptions to anonymity and pseudonymity in online communications should be mandated, for they are an essential instrument of the right to privacy for both adults and children.
10. All age verification techniques affect users' privacy. Document-based techniques are uniquely disproportionate to users' privacy interests and should be discouraged.

Thank you,

Agustina Del Campo
Director
Center for Studies on Freedom of Expression and Access to Information (CELE)

References

Beltrán, M., & de Salvador, L. (2024, August). Implications of Age Assurance on Privacy and Data Protection: A Systematic Threat Model. In Annual Privacy Forum (pp. 1-22). Cham: Springer Nature Switzerland.

Brennan, S, Children's Choices or Children's interests: which do their rights protect?, in Archard, D. and Macleod, C. (eds), The Moral and Political Status of Children, Oxford University Press, Reino Unido, 2002, p. 63.

CDT, ACLU, Fight For the Future, Open Technology Institute and EFF, Civil Society Letter, https://cdt.org/wp-content/uploads/2024/05/Civil-Society-Letter-Kids-Online-Safety-Act-05.17.24.pdf

EDRi. (2023). Online age verification and children's rights. https://edri.org/our-work/policy-paper-age-verification-cant-childproof-the-internet/

Freeman M (1997) The moral status of children: essays on the rights of the child. Martinus Nijhoff Publishers, London, p. 34, cited in Ke, T. The development of children's autonomy and reasonable paternalistic intervention. Humanit Soc Sci Commun 10, 874 (2023). https://doi.org/10.1057/s41599-023-02395-2

Kelley, J. and Mackey, A., The New U.S. House Version of KOSA Doesn't Fix Its Biggest Problems, Electronic Frontier Foundation, September 17 2024, https://www.eff.org/deeplinks/2024/09/new-us-house-version-kosa-doesnt-fix-its-biggest-problems

Kelley, J. & Schwartz, A. (March 10th, 2023). Age Verification Mandates Would Undermine Anonymity Online. Electronic Frontier Foundation. https://www.eff.org/es/deeplinks/2023/03/age-verification-mandates-would-undermine-anonymity-online

Meeus W, Iedema J, Maassen G, & Engels R (2005). Separation-individuation revisited: On the interplay of parent-adolescent relations, identity and emotional adjustment in adolescence. *Journal of Adolescence*, 28, 89–106. 10.1016/j.adolescence.2004.07.003, cited in Pfeifer JH, Berkman ET. The Development of Self and Identity in Adolescence: Neural Evidence and Implications for a Value-Based Choice Perspective on Motivated Behavior. Child Dev Perspect. 2018 Sep;12(3):158-164. doi: 10.1111/cdep.12279. Epub 2018 Feb 8. PMID: 31363361; PMCID: PMC6667174.

Milosevic, T., Verma, K., Carter, M., Vigil, S., Laffan, D., Davis, B., & O'Higgins Norman, J. (2023). Effectiveness of Artificial Intelligence–Based Cyberbullying Interventions From Youth Perspective. Social Media+ Society, 9(1), 20563051221147325.

OECD (2021), "Children in the digital environment: Revised typology of risks", OECD Digital Economy Papers, No. 302, OECD Publishing, Paris, https://doi.org/10.1787/9b8f222e-en.

Sas, M., & Mühlberg, J. T. (2024, February). Trustworthy Age Assurance?. In The Greens Cluster: Social & Economy, Location: The European Parliament.

Smirnova, S., Livingstone, S., & Stoilova, M. (2021). Understanding of user needs and problems: A rapid evidence review of age assurance and parental controls.

UNICEF, Industry toolkit: Children's online privacy and freedom of expression, 2018. Available at https://sites.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf

UNICEF, What is encryption and why does it matter for children?, Office of Research-Innocenti Summary Note by UNICEF's Cross-divisional Working Group on Child Online Protection, https://www.unicef.org/innocenti/documents/what-is-encryption-and-why-does-it-matter-for-children