September 30th, 2024

To: European Commission

Re: Call for Evidence on Guidelines to Enforce the Protection of Minors Online

By David Klotsonis and Aliya Bhatia

Protecting young people's free expression and privacy rights helps keep young people safe online.

Online services are a critical venue for young people to exercise their fundamental rights to access information and express themselves freely. Through these services, young people gain access to online communities and peer support, find supplemental educational resources, boost their literacy and digital skills, and find help when dealing with difficult mental or physical health circumstances.

According to research conducted in 2020 by the EU Kids Online Network, more than half of the 25,000 9-16-year-olds surveyed across 19 European countries used online services at least weekly to watch videos, help with school work, communicate with friends and family, listen to music, and play online games.

The report finds that young users experience the benefits and harms of online services based on several variables, including socio-economic background, age, country of origin, and gender. It concludes that "in most cases, online activities cannot be conclusively defined as generally positive or generally negative. Rather, the same activity can have positive consequences for one child and negative consequences for another." An approach that empowers young people to navigate online services with tools and resources at their disposal to tailor online services to their needs is necessary to respond to the ways the benefits and harms of online spaces may be disparately experienced.

Ensuring young people's ability to freely access online spaces while protecting them from privacy violations, harmful content, and dangerous interactions is essential. Any guidance to address risks to young people's well-being must not come at the expense of or inadvertently undermine their rights to privacy, free expression, or security.

I. Young people have free expression and privacy rights too.

Efforts to protect young people online must balance their rights to access essential information and do so privately against actions necessary to safeguard them from potential harm. Article 28 of the Digital Services Act (DSA) provides an opportunity to establish robust guidelines prioritizing young people's well-being. As stated in Article 13 of the United Nations Convention

on the Rights of the Child and Article 24 of the European Charter of Fundamental Rights, young people have the right to access information necessary for their development. This is reinforced by the Louvain-la-Neuve Declaration of 12 April 2024, which highlights the need for secure and empowering online spaces for youth.

II. A one-size-fits-all approach risks undermining young people's rights.

Comprehensive child rights-centered protections should take into account the different ways young people access online services and the disparate nature of the risks posed to them. Research has found that LGBTIQ teenagers are particularly likely to benefit from access to online services, especially those curious about their sexuality who are seeking information they feel they cannot safely discuss with their peers or caregivers, yet they also face disproportionately more risk of harm as a consequence of their increased dependence on online spaces. Similarly, different socioeconomic or ethnocultural backgrounds, family types, and ages are all contributing factors to how young people experience harm and seek resolution online.

Imposing age verification techniques for all users raises privacy, free expression, and equity concerns.

Upholding young people's rights online requires a careful approach, with any measures being appropriate to the risks and guided by the best interests of minors. A safer and more private online environment should be built by design and by default. In the absence of properly built systems, some argue that age verification of users is necessary to protect youth online, but these verification mechanisms can have exclusionary effects on adults and minors alike and may not always offer better protection to young people. It is therefore important to stress that age verification can be one tool among many, rather than a comprehensive solution – as noted by the European Commission in a recent report, age verification must be context-sensitive, and no universal approach exists.

Mandating that all platforms pursue age assurance or estimation risks requiring further data collection on all users. Age assurance methods often involve the processing of personal or sensitive data, including that of minors; the guidelines should underscore that providers are required to adhere to the General Data Protection Regulation (GDPR), the ePrivacy Directive, recital 71 of the DSA, and the standard of proportionality in this context. Unlike verifying the ages of individuals in person, online services are unable to distinguish between adult users and minor users without verifying all users. As a result, the risks or limits of age assurance systems can burden adults, not just younger users or their parents.

Increasing data collection and retention on all users also will undermine users' ability to anonymously access online services and information hosted on them. This is particularly concerning for users seeking sensitive information including, for example, resources related to sexuality, health diagnoses, or even domestic violence. If users must provide government identification or other personal information to verify their age as a condition of accessing content

of these types, they may be deterred from accessing the content at all or will face the risk of intentional or unintentional disclosure of their identities.

The European Commission and member states have sought to address concerns about privacy and lack of inclusivity in current age assurance methods by expanding the use of the EU Digital Identity Wallet. However, the capabilities and limitations of this system to enable access to online services, while addressing all possible concerns regarding privacy, security, and useability, have not been sufficiently studied and are not known.

The Digital Identity Regulation mandates that by 2026, all EU citizens and residents will be offered at least one EU Digital Identity Wallet by their Member State. While this wallet is seen as a potential solution for age verification, both online and in physical settings, several challenges remain. The technology, though promising, is not expected to provide a comprehensive or widely adopted solution in the near future. Although the European Commission expects the EU Digital Identity Wallet to be available to 80% of adults by 2030, research has called this goal into question, calling it over-ambitious. In any event, the Digital Wallet will not resolve many of the concerns associated with mandatory age verification.

First, the current Digital Wallet roll-out plans do not include equipping minors with access. That means adults will be subject to verification online and platforms may assume that those without a wallet are child users who should be gated from accessing a whole range of information, burdening their rights to expression and access to information. Cultural concerns about privacy and trust in government-issued digital identities could also affect adoption. Solutions to these issues are possible, but significant gaps remain between the current wallet development and immediate age assurance needs.

Other inclusivity issues exist as well. Not all individuals will be able to adopt the digital wallet due to factors like access to devices, disabilities, or legal status. Current age assurance methods offer multiple options, but relying solely on digital wallets could create barriers. The Digital Identity Wallet is only available to EU citizens and residents, not for refugees and migrants who may have more trouble securing the documents necessary to establish their Digital Identity Wallet. Precluding access to online services on the basis of an EU Digital Identity will burden these users in gaining access to critical resources, including resources related to building a better life in the countries they have gained asylum or refugee status in. Requiring non-citizens and non-residents to pursue another form of age or identity verification risks subjecting these individuals to more privacy-invading processes, which will burden their privacy rights and their rights to non-discrimination.

Ultimately, the EU Digital Identity Wallet is not a silver bullet and its use by online services to grant access to a service entirely or in part should be assessed in relation to the risks it poses to the rights of all users, including young users. Overall, the guidelines should stress that age verification measures, whether using the EU Digital Identity Wallet or other methods, must be applied proportionately to the risks associated with a service, aiming to minimize any potential negative effects of this practice.

Scaling parental controls burdens free expression and access to information rights for all.

Requiring the adoption of parental controls over access to online services or content without adequate notice to young users, particularly older teenagers, also creates potential vectors of abuse for teenagers who may not be in healthy relationships with their families. Research shows that young people find parental control apps overly restrictive and invasive of their privacy, negatively impacting their relationships with their parents and their rights to free expression and privacy. In May 2024, the Director of the EU Agency for Fundamental Rights (FRA) noted that while progress has been made with regard to rights for LGBTIQ individuals in Europe, signs of "bullying, harassment, and violence remain constant threats". Some of those threats emerge within family dynamics and target young people. Equipping all parents with broad monitoring capabilities to oversee what types of information young people are accessing online, particularly if those young people are seeking resources on how to seek help, risks jeopardizing their privacy and safety further. A better approach would enable parents to control certain privacy settings and balance the need for protection with the rights of a child to access information privately.

In addition, research highlights the importance of striking a balance between parental control and fostering digital literacy, as overly restrictive measures can hinder young people's development and online engagement. According to the Global Kids Online 2019 survey, kids with less restrictive parents tended to use the internet for a range of informational and creative activities, while kids with more restrictive parents leaned toward entertainment-only activities. Another study revealed that broad restrictions on access to online services prevented kids from using the internet to complete simple tasks like homework. In a landmark systematic review of existing literature published in 2021, all surveys of young people aged 12 to 17-year old found that increased online activities resulted in the development of greater digital skills.

Previous Commission-led studies of broad parental control tools also find that most tools are overly restrictive and block non-harmful content which could prevent young users from accessing important information and rob parents of the ability to exercise their discretion over what content is and is not age appropriate for their young people. Parents want the ability to decide what their young people see, and researchers find that child controls are most effective when devised in conjunction with the child. Parents also increasingly find the array of parental tools and toggles overwhelming and often overly invasive and in fact, often ask their child to access settings or information online in a move researchers call "reverse mediation". Parental safeguards should be focused on helping parents protect their young people's privacy and encourage dialogue between parents and children, including with notice to children when they are on, and additional ability of older teenagers to maintain some privacy.

III. Approaches to protecting young people online should give them choices and tools to keep themselves safe.

Approaches to protecting young people online should consider the risk profile of a platform and offer choices to young users to equip them with the tools required to control their own experience. Here are a few steps that the guidance can cover.

Urging online services to empower all users including young users with tools to allow them to curate their online experience.

Protecting young people while promoting their rights requires resisting the tendency of mandating one-size-fits-all approaches or requiring prescriptive changes or modifications to blunt systems, like content moderation systems, which can erroneously prevent young users from accessing critical information they need for their development and well-being. Instead, early evidence suggests that when provided with the right tools, young people use thoughtful strategies to decide when and how to make use of them.

The EU Kids Online Network surveyed over 25,000 9-17-year-olds, and the majority report knowing how to respond to negative online experiences, with 77% of 15-16-year-olds and 72% of 12-14-year-olds reporting confidence in their response. With more user controls, young people can be equipped with the tools to control their online environment. According to a study by the Center for Democracy & Technology, young people aged 14-18 express clear preferences for tools that help them manage and mitigate unwanted interactions, such as the ability to block, delete, and report harmful messages. By offering customizable filters or allowing users to tailor their online experiences, platforms can empower young people to make decisions about their safety. Some companies are already moving towards this. For example, TikTok's hashtag blocking for videos and comment filtering features and Meta's recent rollout of topic selection features on Instagram introduced in compliance with the UK's Age Appropriate Design Code (AADC), allow users to create safer environments by controlling the types of content they are exposed to. Online services in addition to social media sites such as gaming sites, online forums, and distributed channels can do more to institute these levels of granular control to empower young users to navigate these spaces with more control and confidence.

One strength of user controls lies in their ability to respond dynamically to new and evolving risks, making them more agile than one-size-fits-all, top-down changes to content moderation. Content moderation systems can be slow to respond to new threats, but empowering young users with adaptable tools allows them to act quickly and independently. For example, young people are often the first to encounter emerging risks online, such as viral trends that could be harmful or inappropriate. Moreover, young people know which terms bring them additional distress such as a new slang term or a term used to bully them. In these cases, platform-wide moderation might not catch or address the issue immediately, but user controls can offer minors a way to protect themselves in real time. Customizable filters, blocklists, and privacy settings provide a flexible approach to safeguarding young users, allowing them to adapt their experience to their immediate needs. Platforms could even support interoperable blocklists, giving users more control over their experience across different platforms.

Offering young people more autonomy online is not only what they want, but it is also beneficial for their development. Research has shown that a decline in independent activities, such as self-regulation and decision-making, has contributed to a decrease in young people's mental well-being. Encouraging minors to manage their online interactions can build independence and promote better mental health, as they make decisions about what content they want to engage with, fostering a sense of agency and responsibility. Providing user controls could, therefore, be a way to support young people's development, giving them the tools they need to navigate the online world while maintaining their psychological well-being.

Requiring online services to conduct a child rights impact assessment before rolling out a new tool or feature.

Child rights impact assessments are measures that online service providers can use to identify areas where proposed features, services, and safety mechanisms may inadvertently pose barriers to young people and the enjoyment of their rights and develop methods to address or mitigate those barriers. DSA Articles 28 and 34 require that online service providers take into consideration systemic risks and child safety in the development and operation of their services. Other advocates calling for CRIAs include academics, companies, child safety and human rights organizations, and organizations ranging from the Council of Europe and UNICEF to LEGO. Similarly, guidance to online service providers can outline methods and standards to use when conducting a child rights impact assessment. Key tenets of a child rights impact assessment for the digital environment should include consultations with key stakeholders including young users, methods to study the risks and opportunities posed by forthcoming policies and product interventions on young users' safety and ability to access their rights, and proposed ways to mitigate these risks and related tradeoffs when pursuing these approaches among others.

Encouraging online services to consult with young users in the research and development of child safety policies and tools on a frequent and consistent basis.

Consulting young people in research and policy development is crucial for ensuring their online safety and fostering age appropriate design. CDT has advocated for including young people in discussions about their safety, and our research on child safety, conducted in collaboration with young people, highlights the value of their input in managing unwanted content and interactions. Directly involving young people ensures that the solutions developed are not only relevant but also aligned with their lived experiences, avoiding overly restrictive measures.

Similarly, ongoing consultation with young people during the development and review of Article 28 guidelines will ensure they remain responsive to evolving technologies and services. As a best practice, service providers should also actively involve young people when designing and implementing mitigating measures. This approach will result in more effective protections that are better suited to the real needs of young users.

Requiring online services to set strong privacy protections for young users' accounts such as setting their accounts to private as default.

Online services can set their youth accounts to be private as default and limit discoverability while allowing users to select a public profile when desired. Privacy as default provides users with both a safety net and the agency to change settings as desired.

Calling for more research on the impacts of child safety interventions on young people of different socioeconomic and ethnocultural backgrounds, disabilities, and more.

The EU Kids Online Network report outlines several individual factors that shape young people's digital experiences. More research is needed to increase our understanding of the way these factors impact online safety amongst youth, and the impact of different child safety interventions on these communities should be a critical focus of research to ensure that efforts to protect young people protect all of them.

Investing in more digital literacy resources to inform healthy and age appropriate behavior online.

Digital literacy initiatives can serve as important complements to guidance and legislation as they can empower young people to access age appropriate experiences on a range of online services. Digital literacy programs are particularly important for newly connected students, as studies show that students with limited broadband access have lower digital skills. These initiatives can look like external expert guidance and in-product notices for users. Developing a robust toolkit of media literacy guides is necessary, particularly for newer technologies like generative AI systems where most users, including many adults and parents, are unfamiliar with the way these systems work.

For more information, please contact dklotsonis@cdt.org or abhatia@cdt.org.

About Center for Democracy & Technology Europe:
At CDT Europe, we work to increase equality, amplify voices, and promote human rights in European level law and policy debates. We champion policies, laws, and technical designs that protect against invasive, discriminatory, and exploitative uses of new technologies. We use our in-depth tech policy knowledge to build capacity and, in turn, learn from other civil society partners on issues such as the discriminatory impact of algorithms and participation in online debates.

https://cdt.org/eu/