Submission to the European Commission's Targeted Public Consultation on the Protection of Minors Guidelines under the Digital Services Act

Submitted by the Electronic Frontier Foundation
June 13th, 2025

About the Electronic Frontier Foundation

The Electronic Frontier Foundation (EFF) is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. EFF's mission is to ensure that technology supports freedom, justice, and innovation for all people of the world.

Introduction and General Remarks

We welcome the opportunity to provide feedback on the targeted consultation of the European Commission ('the Commission') for input to their draft guidelines pursuant to Article 28(4) of the Digital Services Act (DSA). Art 28(4) provides that the Commission may issue, after consulting the Board of Digital Services Coordinators, guidelines to assist providers of online platforms in the application of Article 28(1) DSA to "ensure a high level of privacy, safety and security for minors online".

As a benchmark that will guide the Commission in its assessments of providers' compliance with Article 28, the guidelines are a crucial element to the enforcement and implementation of the DSA. The guidelines present a comprehensive set of recommendations and measures that incorporate important evidence and research on risks posed by some online platforms to the privacy, safety and security of users. We recognize the Commission for prioritizing the protection of minors online, and for withstanding the pressure from Member States to introduce disproportionate and rights-undermining approaches like banning young people from social media platforms. We also want to acknowledge the commitment of the Commission to include and consult young people in the drafting of the guidelines, which we believe is crucial to achieve equitable outcomes.

We strongly welcome the Commission's acknowledgement that creating a privacy preserving, secure and safe environment for *all* users will contribute to the privacy, security and safety of minors. Similarly, we welcome the general principles that underpin the guidelines, including proportionality, the focus on childrens' rights and privacy-, safety-, and security-by-design.

However, some of these principles and rights can stand in tension with each other, which require careful balancing. For example, measures to protect childrens' rights to protection may undermine their rights to privacy, non-discrimination and freedom of expression. The guidelines do not resolve these fundamental tensions, but instead put an overly strong emphasis on safety, risking to undermine the privacy and security of all users.

Feedback on Selected Aspects

Risk Review

As the heart of the risk-based approach of the guidelines, the risk review framework proposed in section 5 is of central importance. We generally welcome the risk-based approach taken and the reference to the 5Cs typology of risks. However, the risk review lacks guidance in important areas.

Scope
The scope of Article 28 includes all online platforms. Providers of smaller online providers are often less versed in the assessment of complex risks than very large online platforms (VLOPs) and search engines (VLOSEs) and usually have significantly fewer resources available. The guidelines do not differentiate between the obligations of smaller and very large providers, which risks placing disproportionate burdens on smaller platforms that do not predominantly target young people, and whose overall impact on the safety of minors is much lower. Such disproportionate burdens risk cementing the dominance of VLOPs and VLOSEs, undermine competition and innovation, and increase barriers to enter digital markets.

We recommend providing additional guidance to avoid disproportionate burdens on smaller providers of online platforms.

Proportionality and Transparency
Lines 192 – 195 acknowledge that children's rights may be adversely affected by some measures providers might take to protect minors, but do not provide guidance on how this tension should be resolved. The Commission should provide guidance on how providers should balance children's rights to avoid disproportionate measures that may risk children's fundamental rights. Additionally, we suggest that providers should also consider the effects of measures taken to protect minors on the fundamental rights of all users.

Risk levels
Crucially, the Commission should provide guidance for how providers should determine the required "high" levels of privacy, safety and security as well as levels of risks to privacy, safety and security. As all recommendations and expectations for specific measures flow from the risk level of a given functionality or service, guidance on how risk levels should be determined is necessary. For example, lines 259 – 262 set out that providers should adopt age verification methods when they identify "high risks" to minors' privacy, safety and security that cannot be mitigated by less intrusive measures. Not providing guidance on how risk levels should be assessed exacerbate the risk of providers implementing age verification methods although less invasive tools are available.

Similarly, in line 284, the guidelines suggest that "medium risk" services should adopt age estimation measures, but it remains unclear how such a risk level should be determined in

practice. Given the significant privacy and security risks attached to many age estimation techniques (see below), this uncertainty risks undermining the security and privacy of all users, including minors through an unnecessary proliferation of age estimation.

Regardless of the risk levels of a certain feature or service, we believe that age determination is an ineffective and disproportionate tool to achieve the goals of Article 28, as age determination tools significantly undermine all users', including minors' security, privacy and other fundamental rights, including the rights to access to information and free expression.

Age Assurance

We welcome that the guidelines note the general tension between age assurance and privacy, safety and security, and the acknowledgment that age assurance can restrict fundamental rights such as the freedom of expression. However, the guidelines are guided by the assumption that age assurance is a necessary, appropriate and proportionate tool, without providing evidence that age assurance is indeed the most effective, and an appropriate and proportionate approach to safeguarding minors.

We are therefore concerned by the implicit obligations on a wide range of different services to adopt age assurance methods, and believe that the guidelines do not adequately take into account the risks to fundamental rights, including the rights to data protection and privacy, freedom of expression and information, and participation, posed by different age assurance methods.

By placing a disproportionate emphasis on age assurance as a necessary tool to safeguard minors, the guidelines do not address the root causes of risks encountered by all users, including minors, and instead merely focus on treating their symptoms.

Age verification

Age verification systems rely on physical identifiers or other verified sources that rely on government-issues IDs. Millions of people in Europe do not have access to government-issued IDs, including migrants, members of marginalized groups and unhoused people, exchange students, refugees and tourists. While there are some harmonized standards regarding ID cards[1], obligations to carry IDs, and the age from which identity documentation is compulsory, vary between Member States[2]. Age verification "solutions" like the upcoming EU Digital Identity Wallet or the Commission's age verification app therefore risk undercutting access to information and services for a wide range of people, who are often among society's most vulnerable groups. While the Commission's age verification app does foresee different pathways

[1] See Regulation (Eu) 2019/1157 Of The European Parliament And Of The Council on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R1157

[2] See State of play concerning the electronic identity cards in the EU Member States, http://www.statewatch.org/media/documents/news/2010/jun/eu-council-ID-cards-9949-10.pdf

for proving one's age, including banks, notaries or telecommunication providers[3], these alternatives do not provide fair and equitable access for all users. Neither banks nor notary offices are especially accessible for people who are undocumented, unhoused, don't speak a Member State's official language, or are otherwise marginalized or discriminated against. Banks and notaries also often require a physical ID in order to verify a client's identity, so the fundamental access issues outlined above persist. Finally, the specification suggests that third party apps that have already verified a user's identity, such as banking apps or mobile network operators, could provide age verification signals. In many European countries, however, showing an ID is a necessary prerequisite for opening a bank account, setting up a phone contract, or even buying a SIM card.

Beyond age verification methods' risks to users' freedom of expression, information and participation, they can also pose significant privacy and security risks. While the specifications for the Commission's age verification app note that the app should implement privacy protections such as salted hashes and Zero Knowledge Proofs (ZKPs), the specifications do not *require* these measures to be implemented. The app's specifications include ZKPs, while simultaneously acknowledging that no compatible ZKP solution is currently available[4]. It is also assumed that frequently used ZKPs will avoid privacy concerns, and that verifiers won't combine this data with existing information, such as account data, profiles, or interests, for other purposes, such as advertising.

Additionally, the Commission's age verification app does not require registration certificates across all EU member states for verifiers (the service providers asking for age attestations). Users will be asked to prove how old they are without the restraint on verifiers that protects from request abuse. Without verifier accountability, or at least industry-level data categories being given a determined scope, users are being asked to enter into an imbalanced relationship which may expose them to illegitimate and abusive verification requests.

In our perspective, Article 28 should not be interpreted as requiring providers of online platforms to implement age verification or age assurance systems to meet the objectives of ensuring high levels of privacy, safety and security for minors. Thus, the Commission should refrain from mandating the implementation of such systems through the guidelines, especially since the availability of age verification methods that ensure users' privacy, security and rights to free expression, access to information and participation can not be guaranteed.

Age estimation

The guidelines (lines 27 – 289) implicitly require the implementation of age estimation techniques in an even wider range of scenarios than those for which age verification is deemed appropriate. While line 292 notes that providers should conduct a proportionality assessment to

[3] See general architecture of the AV app, https://github.com/eu-digital-identity-wallet/av-doc-technical-specification/blob/main/docs/media/general_architecture.png

[4] See Annex 2, High-Level Requirements https://github.com/eu-digital-identity-wallet/av-doc-technical-specification/blob/main/docs/annexes/annex-2/annex-2-high-level-requirements.md

understand whether age estimation methods are justified, no guidance is given for how providers should balance these competing instructions in practice. This risks that a wide range of providers implement unnecessary age estimation measures out of fear of being in non-compliance with Article 28 of the DSA.

While lines 294 – 296 note that providers opting for an age assurance method that involves the processing of personal data should take into account the EDPB's statement on age assurance[5], it fails to acknowledge that *all* age assurance methods necessitate the processing of personal data. Age estimation methods in particular, which usually rely on the processing of vast amounts of behavioural data or the processing of biometric data, carry significant privacy risks.

Biometric Age Estimation
A recent NIST review[6] of several major biometric age estimation algorithms determined that for each, accuracy is strongly influenced by sex, image quality, region-of-birth and race, and interactions between those factors.

For those near the age of eighteen, NIST's review indicated that the algorithms are simply not very accurate. False positive error rates are considerable when used on younger faces: every algorithm incorrectly estimated more than 40% of seventeen-year-olds to be above a challenge age of eighteen. For eighteen to twenty-one-year olds, the mean absolute error rate of all algorithms was generally three or more years. Use of this type of age estimation could result in an enormous number of inaccurate estimates – both false positives and false negatives. It's important to note that the NIST review clearly demonstrates the racialized aspect of failure for this technology; across the board these tools fail at estimating the ages of Black and Asian people, further engendering harms that facial mapping technologies cause them. Recent investigations into Yoti, a market leader in biometric age estimations has further revealed how data collected by age estimation providers may be used to profile users, and could expose them to over-identification and data breaches[7].

User Activity Age Estimation
Assessment based on analyzing user activity is another inaccurate, and dangerous path for companies to take, which relies on the processing of vast amounts of user data. Estimating a user's age by combining signals such as user history with predictive analytics routinely expose the most sensitive categories of personal data, such as biometric information or browsing history, and are error-prone.

Plurality of Age Assurance Options

---

[5] EDPB Statement 1/2025 on Age Assurance
https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/statement-12025-age-assurance_en
[6] Face Analysis Technology Evaluation (fate) age estimation & verification. (n.d.).
https://pages.nist.gov/frvt/html/frvt_age_estimation.htm
[7] See Data protection and IT security issues with age verification app „Yoti",
https://mint-secure.de/dataprotection-it-security-risks-with-ageverificationapp-yoti/

Obliging service providers to offer a plurality of these age assurance options (lines 301 – 302) glosses over the fact that every solution has serious privacy, accuracy, or security problems. This puts the burden on the individual to decide whether they are most concerned with accuracy or privacy, generally without giving them the tools they need to determine which option is safest for them.

Account Settings, Online Interface Design and Recommender Systems

Account Settings and Interface Design
We welcome that the guidelines recognize the important role of account settings and interface design in protecting vulnerable users and the privacy, safety and security of all users.

However, vulnerability does not necessarily correlate to age. This is why all users would benefit from measures that protect their privacy, especially default settings that turn off the collection and processing of personal and behavioural data. While not a requirement under the DSA, we believe that all online platforms should extend privacy preserving account settings and interface features to all users.

To ensure the acceptance and proportionality of the measures suggested, it is crucial to balance safety with minors' rights to express themselves or access information relevant to them. For example, we welcome measures to ensure that minors can only be directly contacted by accounts they have previously accepted as contacts. However, accounts of minors should be discoverable to other minors, and accounts and content by adults should be allowed to be recommended to minors. Especially for young people from marginalized communities, finding like minded people online can be crucial to establish a sense of identity and community. These positive elements of online platforms should not be unduly restricted. We therefore recommend removing lines 458 – 460.

Recommender Systems
Recommender systems are among the core functionalities of many online platforms and help determine which content is presented to users. When it comes to defining parameters and objectives of recommender systems, we note that recommender systems generally do not *only* optimize for engagement metrics. To ensure that all recommender systems that *also* optimize for engagement metrics are captured, we recommend removing "only" in line 529.

We are concerned that measures aimed at preventing minors' exposure to potentially risky content (lines 551 – 561) could lead to overblocking and restrictions of the freedom of expression and access to information. Vague categories like "promoting unrealistic beauty standards" (line 553) ignore that what content is appropriate for minors can vary depending on cultural norms and the person in question. We recommend removing this specific reference. Similarly, we are concerned that suggested limitations to search and discovery features through automated block lists or filters (lines 568 – 573). Such measures can seriously undermine

minors' freedom of expression and will impair their access to lawful, legitimate and at times life-saving information. We recommend removing this measure from the guidelines.

In general, platforms should not define unilaterally what information is "relevant and adequate" for minors (line 534). Such broad categories can be easily weaponized to suppress content deemed sensitive by some, for example information related to LGBTQIA+, sexual health or political content. Instead, the guidelines should encourage platforms to prioritize content plurality. This should be accompanied by adequate transparency to their users about factors used to recommend content, mechanisms to prioritize explicit user signals (line 539) and options for users to influence what categories of content are presented to them.

User Control and Empowerment

We welcome the emphasis put on user control and empowerment in the context of recommender systems, which we believe to be a crucial lever to strengthen users self-determination online. The DSA allows users to easily choose between different recommendation systems when multiple options are available. The DSA also obliges VLOPs that use recommender systems to offer at least one option that is not based on profiling users, thereby giving users of large platforms the choice to protect themselves from the often privacy-invasive personalization of their feeds. However, forgoing all personalization will likely not be attractive to most users, and the guidelines should encourage platforms to give users the choice to use third-party recommender systems that better mirror their privacy and content preferences.