epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@epic.org
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORAMTION CENTER

to the

New York State Attorney General

Notice of Proposed Rulemaking for the SAFE for Kids Act

Pursuant to New York General Business Law Section 1500 *et seq*.

December 1, 2025

The Electronic Privacy Information Center (EPIC) submits these comments with recommendations for the New York State Attorney General rulemaking for the NY SAFE for Kids Act. EPIC is an independent nonprofit research organization focused on protecting privacy, freedom of expression, and democratic values in the information age.[1] EPIC has provided courts, legislators, and Attorneys General with guidance about the constitutional, privacy, and access questions implicated by kids' online privacy and safety legislation.[2] In particular, EPIC has filed two amicus briefs in the California SB 976 litigation supporting the constitutionality of the restriction on providing addictive feeds to minors and the age assurance requirement.[3] Last year, EPIC filed

[1] EPIC, *About EPIC*, https://epic.org/about/.
[2] EPIC, *Platform Accountability & Governance*, https://epic.org/issues/platform-accountability-governance/.
[3] Brief of EPIC et al. as Amici Curiae Supporting Defendant-Appellee and Affirmance, No. 25-146 (9th Cir. Mar. 6, 2025), https://epic.org/wp-content/uploads/2025/03/EPIC-Amicus-Brief-NetChoice-v-Bonta-SB-976.pdf; Brief EPIC as Amicus Curiae Supporting Defendant, *NetChoice v. Bonta*, No. 5:24-cv-07885-EJD (N.D. Cal. Nov. 12, 2024), https://epic.org/wp-content/uploads/2024/12/EPIC-Amicus-SB-976-NDCal.pdf.

comments in response to the Advanced Notice for Proposed Rulemaking urging the NY AG to prioritize privacy-protective age assurance and center data minimization in the rulemaking.[4]

The proposed rules set out critical protections for minors online. This comment will provide recommendations to minimize the number of users required to go through age assurance, to further strengthen the data protection rules, to improve user choice, to add an Attorney General approval process, to ensure that small platforms still comply with the law in some way, and to strengthen the non-discrimination provisions.

I. Privacy- and Speech-Protective Age Assurance Principles

Age assurance is an important component of the NY SAFE for Kids Act. Age assurance will help ensure that minors receive the important privacy and online safety protections the law provides. EPIC believes that age assurance can be deployed in a way that respects the privacy and speech rights of users. Strong data protection requirements, the ability for users to choose which age assurance method to use, effective appeals processes, transparency, and minimizing the burden of age assurance are critical. These measures help ensure that age assurance does not contribute to the commercial surveillance system and broader data protection crisis and that age assurance does not prevent users from accessing online forums for speech.

EPIC commends the Attorney General for including many of the privacy- and speech-protective age assurance principles in the proposed rules that EPIC recommended in our previous comment, including strong data minimization, user choice and appeals processes, and strong transparency, privacy and data security requirements.[5] The proposed rules rightly extend data

[4] EPIC, Comments to the NY Attorney General on the Advanced Notice of Proposed Rulemaking for the NY SAFE for Kids Act (September 30, 2024), https://epic.org/wp-content/uploads/2024/10/EPIC-Comments_NY-SAFE-For-Kids-Act.pdf.

[5] *Id*.

minimization requirements to all operators involved in the age assurance process.[6] These limitations will help protect all users from breach, fraud, and abuse. They will also help boost users' confidence that their personal information will be protected, making it less likely that users will be unwilling to submit themselves to the process.

This section offers recommendations to further strengthen privacy- and speech-protective age principles in the rules and, in turn, to make the law's protections more effective.

a. Minimize the Number of Users Who Must Submit Personal Information for Age Assurance.

NY SAFE For Kids Act can be implemented in a way that does not burden users' abilities to access online forums for speech. Minimizing the number of users who must submit new personal information to the covered operator to determine age is a key way to lower this burden. Covered operators can minimize the number of users for whom they must collect new personal data to determine age by (1) turning regulated features off by default for all users and only requiring users to go through age assurance to turn them on; and (2) using data they already collect or process to determine whether the user is an adult.

First, the rules should make clear that the Act does not require covered operators to make age assurance a condition of accessing their products and services. Instead of determining the age of every user before they can access the platform, a covered operator should turn addictive feeds and nighttime notifications off for all users by default and only determine a user's age status when the user expressly requests to turn addictive feeds or nighttime notifications on. This universal default will lower the frequency and volume of personal data collection by limiting the need for age

[6] NY Office of Attorney General, Notice of Proposed Rule to Implement the SAFE for Kids Act §700.9(a) (proposed September 15, 2025)(to be codified at Part 700 of Title 13 NYCRR), https://ag.ny.gov/sites/default/files/regulatory-documents/safe-for-kids-act-nprm.pdf [hereinafter *NPRM*].

assurance to when it is only necessary to process a user's request for a feature. It will also ensure full, unburdened access for all users to the rest of the platform, including to all user-generated content, deflating the constitutional arguments against the law.

Alternatively, the rules should explicitly require covered operators who ask users to assure their age prior to accessing their product or service to allow users to skip the age assurance process to immediately access the platform, wherein a covered operator would treat such a user as a covered minor for the purposes of complying with the law until the user wishes to turn on a regulated feature and goes through the age determination process.

To further minimize the number of users that must go through the age assurance process and the volume of data collected from users for age assurance, the rules should allow covered operators to infer adult age status based on data they already collect and process. As the rules are currently written, a covered operator may only consider user data in its possession to constitute actual knowledge of a covered user's minor age status, not adult age status.[7] Covered operators who wish to infer adult age status from existing user data must go through the certification process to use this inference as an age assurance method. This may discourage operators from using such existing data, as it may be easier to use a third-party tool that has already gone through the required testing. The rules should instead allow covered operators to rely on certain data or inferences they already collect if, upon disclosing to the AG which data and inferences they intend to rely on and how the inferences are determined, the AG approves of such use. The rules should, however, explicitly exempt self-declaration because of high false positive rates from self-declaring adult age status. The rules should also continue to require covered operators to provide certified age assurance methods to users if they do not go through the certification process for their existing data solution.

[7] *Id*. at §700.4(a)(3).

b. Strengthen Data Minimization Requirements.

The rules should limit the definition of "delete" to permanently destroying or removing information and should not include de-identification. As the rules are currently written, de-identification of personal data would constitute deletion,[8] severely weakening important requirements like §700.7(a)(4) to immediately delete data collected for age assurance. Deletion and de-identification are two distinct concepts and should not be conflated. De-identification techniques are often inadequate, leaving users' personal information at risk for re-identification.[9] A strong data deletion requirement is especially important in the context of age assurance because many users are concerned that their sensitive personal information might be misused or stolen. Further, there does not appear to be a good reason to allow covered operators to keep de-identified data, as testing for certification purposes will be conducted by third parties and the data required to comply with the reporting requirements in §7.007 could be collected prior to data deletion.

The Attorney General should remove the proposed section §700.7(c) that allows covered operators to maintain estimated ages of covered users if the user consents. The explanatory text of the NPRM elaborates that the purpose of §700.7(c) is to allow "the covered operator to make an informed decision as to when the covered user will reach adult status."[10] Allowing covered operators to retain this information, even with a consent mechanism, unnecessarily heightens privacy and data security risks for covered users' personal information, also weakening other data use and retention protections in the rules. There is sufficient process required in §700.4(d)(4) of the rules for covered

[8] *Id*. at §700.1(p).
[9] *See* Natasha Lomas, *Researchers spotlight the lie of 'anonymous' data*, Tech Crunch (July 24, 2019), https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/; Jules Polonetsky, *The Curse of Dimensionality: De-Identification Challenges in the Sharing of Highly Dimensional Datasets*, Future of Privacy Form (May 5, 2025), https://fpf.org/blog/the-curse-of-dimensionality-de-identification-challenges-in-the-sharing-of-highly-dimensional-datasets/ ("Decades of research and numerous real-world incidents have demonstrated that supposedly "de-identified" or "anonymized" data have been re-identified, sometimes with surprising ease.").
[10] NPRM, *supra* note 6 at 99.

minors to "update their minor status upon reaching adult status" without allowing covered operators to retain age estimation information outside of the age assurance process.

Finally, the rules should limit the term "technical information concerning a user's device" to include stricter use and purpose limitations for location data. Location data is highly sensitive when linked to a user and can reveal further personal information about that user, especially when combined with other data.[11] Covered operators should be limited to using location data about a user's device for specific purposes consistent with the Act. Explanatory text in the NPRM suggests only one such use: when a covered operator estimates a user's general location from their IP address to determine whether they are in New York State.[12] We are unaware of another use that would be consistent with the Act. The Attorney General should modify the definition to read that "location data is only technical information concerning a user's device when used to determine whether a user is located in the state of New York for the purpose of complying with this law."

c. Improve User Choice in Age Assurance Method.

The rules should require covered operators to offer at least two methods of age assurance. It is important that covered operators provide users choices for age assurance based on users' differing levels of comfort with, and ability to use, certain age assurance methods. It also benefits covered operators to have flexibility with cost-effectiveness and user burden. One aspect of the proposed rules is that a covered operator only needs to offer multiple age assurance options if one of those options depends on providing government-issued ID.[13] But whether or not a covered operator offers the option of using government-issued ID to assure age, they should offer multiple age assurance

[11] *See* Jon Keegan & Alfred Ng, *There's a Multibillion-Dollar Market for Your Phone's Location Data*, The Markup (Sept. 30, 2021), https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data.
[12] NPRM, *supra* note 6 at 53.
[13] *Id*. at §700.4(c).

methods since this responds to the fact that different users will have different levels of comfort and familiarity with different methods.

d. Add an Age Assurance Plan Approval Process.

Some aspects of the proposed rules, as well as some of EPIC's recommendations, would be best facilitated by requiring covered operators to submit an age assurance plan to the Attorney General's office for approval. Such plans would outline, at minimum: (1) the certified age assurance methods the operator will offer users; (2) any data the operator collects or processes that they propose to use to determine the age of some or all users; and (3) an evaluation of the covered operator's chosen age assurance methods, as required by §700.4(g). Such an approval process would make it easier for covered operators to use data they already collect to determine age. It would also create a means of enforcing §700.4(g). As it is currently written, §700.4(g) requires covered operators to periodically review the accuracy, burden, and privacy-protectiveness of their chosen age assurance methods but does not specify a specific time period for this review. This requirement will be much stronger with annual oversight from the Attorney General.

II. Further Strengthening the Rules.

EPIC has two further suggestions for ensuring that the NY SAFE for Kids Act is most effective: broadening the scope of covered operators and refining the non-discrimination requirements.

a. Broaden the Scope of Covered Operators.

Smaller covered operators with addictive feeds should not be completely exempt from the Act.[14] Smaller platforms with addictive feeds also harm minors. The rules should exempt smaller platforms from the age assurance requirement but still require them to provide protections to users

[14] *Id*. at §700.1(q).

where they otherwise have actual knowledge the user is a minor. This would address concerns that age assurance places a greater financial burden on smaller platforms while also ensuring that these companies mitigate harm to minors if they otherwise meet the addictive online platform definition.

b. Refine The Non-Discrimination Provision.

The Attorney General should strengthen the nondiscrimination provision in §7.009(b)(2). The rules should make clear that the nondiscrimination provision requires covered operators to offer covered minors—and any user who does not wish to go through the age assurance process—with an alternative feed that is not addictive. Additionally, subsection §700.9(b)(3) of the non-discrimination clause that prohibits covered operators from increasing the price of their product or service used by a covered minor or parent should apply across the entirety of the rules. In the proposed rules, this provision does not apply when necessary for a covered operator to comply with two of the most fundamental sections of the rules: the prohibition of addictive feeds in §700.2 and prohibition of nighttime notifications in §700.3. The rules should not allow covered operators to increase the price of their services to covered minors or parents because they are complying with these sections.

III. Conclusion

EPIC applauds the Attorney General's attention to the important issues shaping privacy, security, and safety for minors and adults online. EPIC is eager to engage with the Attorney General further on age assurance, data privacy, or any other issue involved in the rulemaking. Please contact EPIC Counsel Suzanne Bernstein at Bernstein@epic.org with any questions.

Respectfully submitted,

/s/ Megan Iorio
Megan Iorio
EPIC Senior Counsel

/s/ Tom McBrien
Tom McBrien
EPIC Counsel

/s/ Suzanne Bernstein
Suzanne Bernstein
EPIC Counsel