September 30, 2024

The Honorable Letitia James
Office of the New York State Attorney General
The Capitol
Albany, NY 12224

Introduction

The Family Online Safety Institute (FOSI) appreciates the opportunity to contribute to the New York Office of the Attorney General's (OAG) Advanced Notice of Proposed Rulemaking (ANPR) pursuant to New York General Business Law section 1500 et. seq related to the SAFE for Kids Act.

FOSI is an international, non-profit, membership organization working to make the online world a safer place for children and their families. We achieve this by identifying and promoting the best practices, tools, and solutions in the field of online safety. FOSI convenes leaders in industry, government, academia, and the non-profit sectors to collaborate and innovate new solutions and policies in the field of online safety. Through research, resources, events, and special projects, FOSI promotes a culture of responsibility online and encourages a sense of digital citizenship for all.

FOSI defines online safety as *acknowledging the risks and mitigating the harms in order to reap the rewards of digital life*. Our work directly relates to aspects of the SAFE for Kids Act such as age assurance, parental consent for certain online features, and ensuring children have a safe experience online. We appreciate that the Attorney General is soliciting comments and guidance to ensure the implementation of the best policies that keep the children of New York safe online.

Age Assurange, Age Verification, and Age Determination Methods

A significant portion of the ANPR is focused on “commercially reasonable and technically feasible age determination methods”. This is an issue that FOSI has explored extensively in recent years, and there are two main resources we would like to bring to your attention.

In 2022 we released original research into the awareness, attitudes, and behaviors of parents and children regarding age assurance. The report features qualitative and quantitative studies across three countries: the United States, United Kingdom, and France. The findings may be of considerable interest to your office as they highlight cultural similarities and differences in how families navigate their online lives.

The second resource is our 2023 white paper Coming to Terms with Age Assurance. The product of a year-long working group and significantly informed by our own research cited above, this paper outlines in detail the benefits, risks, and complexities of implementing each age assurance method.

We define age assurance as a broad term that is used to describe the methods that determine a user's age or age range. Age assurance can include methods like “age verification” which often require users to upload hard identifiers such as a driver's license or other government issued ID. Other methods of age assurance include “age estimation” which estimates a user's age or age range, often based on biometric data such as facial scanning. The lowest level of age assurance is self-declaration, where the user simply checks a box that they are older than a certain age or inputs their birthday.

It is important to know that both age verification and age estimation methods require users to provide sensitive personal data, including personally identifiable information such as birthdates and immutable characteristics such as unique facial features. Some users may not feel comfortable sharing this information with social media platforms. Question 19 of the ANPR acknowledges that some underrepresented populations such as undocumented New Yorkers or LGBTQ+ young people may not have a government issued ID, a government issued ID that aligns with their identity, or feel safe using their government ID to get online.

The internet can provide a safe space for people to connect with each other online. All New Yorkers should have equal access to the internet and all the benefits it provides.

Age assurance is an essential part of creating age-appropriate online experiences. Verifying a user's age allows platforms to offer certain features such as privacy settings set high by default for minors and ensures the youngest users are kept safe, while preventing older users from being relegated to a “kids only” experience online. However, it is critical that the type of age assurance method used is congruent to the level of risk posed to a child accessing that platform. For example, a digital game specifically designed for kids might only need an “age gate,” which is the most common form of age assurance method that requires users to self-declare their age before gaining access to the platform. Age gating is the easiest method of age assurance to circumvent, however, it can still be used in some instances in conjunction with other methods when the risks of a child experiencing harm are low.

This is why we recommend a risk-based and proportional approach to age assurance. There are situations in which age assurance should have the highest level of confidence about a user’s age, such as if the content or product of an online service is physically dangerous. There are also situations where the converse is true, when a low level self-declaration or broader age range estimation is appropriate to access an app or platform. The highest risk activities online should have correspondingly high levels of assurance, whereas the least risky activities should not require sharing excessively personal information in order to access.

This highlights another takeaway from our work on age assurance: the balance of safety and privacy, or more specifically, effectiveness vs. invasiveness. The more effective the method of age assurance (such as verification), the more invasive it is (processing the most sensitive data about someone). This is a tradeoff that must be considered by any regulator issuing guidance on age assurance practices.

In issuing age assurance guidance, the OAG should aim to strike the difficult balance of providing clarity for compliance purposes while not being overly prescriptive about age assurance methods. There are frequent improvements in age assurance technologies and no single company or technology should be prescribed as the only

solution. Focusing on risk-based, proportional methods will help ensure all New Yorkers continue to have access to information, enjoy safe spaces online, and protect their personal data from unnecessary collection and use.

Verifiable Parental Consent (VPC)

One of the three pillars of FOSI is our Good Digital Parenting platform. FOSI emphasizes the role parents and guardians play in supporting their children in becoming good digital citizens. This includes holding conversations with their children about what is safe and acceptable behavior online as well as being a good digital role model for children.

The SAFE for Kids Act outlines two circumstances in which users under 18 would need parental consent. The first being for overnight notifications. As the Surgeon General acknowledges in a 2023 report on social media and youth mental health, much of the problematic results of excessive time online is that it replaces healthy offline habits like sleeping, eating, and in-person interactions with family and friends. Thoughtful restrictions on social media use for young users are necessary for youth development.

FOSI conducted research in 2020 that finds that parents are already overwhelmed by the variety of parental controls that exist across platforms. Users would like a "one-stop-shop" on each platform that has all of the safety features they need. Additionally, some parents are eager for tools that make managing their kids' online experiences easier. It is imperative that parental consent requirements do not inhibit or replace social media platforms' innovation surrounding parenting tools.

Additionally, these efforts must be tailored for age groups. As currently written, the SAFE for Kids Act treats all young people ages 0 to 18 the same even though it is evident these age groups have different developmental needs. Older teens need autonomy to make healthy choices as they begin navigating the digital and physical worlds away from their parents. FOSI encourages the OAG to consider the different stages of children's development when crafting the rules surrounding when minors need parental consent. The UK's Information Commissioner's Office has thoughtful

guidance on this subject, as an annex to their Children's Code for age appropriate design.

The second and more complicated VPC requirement in the SAFE for Kids Act is for the use of algorithmic feeds as opposed to the default setting of chronological feeds. While the crux of the law names algorithms as responsible for the harm caused to a child, the American Psychological Association's recent health advisory on social media use in adolescence acknowledges that a variety of factors contribute to a child's experience online and that different children can respond to the same situations in different ways. While excessive use of technology can certainly be harmful, other harms that youth experience online unfortunately mirror offline experiences such as racism and bullying.

A benefit to algorithmic curation is that it allows young people to see age appropriate content related to their interests. For example, older teens showing interest in art, STEM, or other healthy habits should be allowed to curate an experience that nourishes that interest. This is just one of the benefits of social media. Age appropriate spaces coupled with thoughtful restrictions on social media use for young users can help ensure safer experiences online.

Question 5 of the ANPR under the title "Parental Consent" acknowledges that the same challenges and privacy concerns that are present with age assurance also exist with obtaining parental consent. While parental consent may be straightforward for some households, young people with unsupportive families may not have a guardian that supports their right to privacy or access information. Much like with age assurance, there is no perfect one size fits all solution. Methods of VPC that require the most friction and effort from parents and guardians will usually provide the highest certainty that the adult has provided consent, while the easiest consent methods leave open the possibility that meaningful consent was not provided.

Recent research shows that while most young people benefit from online spaces, LGBTQ+ youth reported that they are 20 points more likely to say that online communities are essential to their lives. This demonstrates the importance of online spaces particularly for underrepresented youth. Additionally, a webinar hosted by

FOSI titled A Connected Community: Empowering LGBTQ+ Youth Online outlined the variety of ways that LGBTQ+ youth benefit uniquely from online communities.

All young people should have equal access to community and information. Parental consent may infringe on that right for some users.

The FTC has worked on this issue for decades, and has recently considered updates to VPC options as technology has progressed. We would encourage your office to engage with the FTC on their approach and learn from their significant experience with VPC.

Addictive Social Media Platform

As the first state in the country to pass a law targeting algorithmic social media feeds for minors, and with another state already copying such a law, it is imperative that New York set an example on the best policies for young people online. We've seen laws across the country that have not withstood legal challenges due to the First Amendment protections of platforms and users. Children have First Amendment rights. Moreover, the recent *NetChoice v. Moody* ruling established that platforms have discretion on the prioritization or deprioritization of content hosted on their platform.

While FOSI commends the SAFE for Kids Act for acknowledging that a platform is not addictive "*if the user expressly and unambiguously requested the specific media, media by the author, creator, or poster of media the user has subscribed to, or media shared by users to a page or group the user has subscribed…*", the law and definitions do not sufficiently acknowledge a minor's choice to engage in healthy, age appropriate recommended content. This is especially important for older teens.

Lastly, more collaboration between families, policymakers, civil society organizations, and industry members is needed to ensure the best practices surrounding online safety for children are implemented. FOSI calls this the culture of responsibility: where each entity plays a role in protecting children online. Definitions, particularly those surrounding addiction, should include all stakeholders, especially medical professionals.

Data Privacy

While our expertise is in online safety and we are submitting these comments for the SAFE for Kids Act, it is still worth highlighting a couple points that are applicable to the Child Data Protection Act APRN as well. The Child Data Protection Act contains some important benefits for minors including prohibiting the sale, use, or collection of their data without their informed consent. This is a step in the right direction as we have seen that safety and privacy laws work best when they consider each other. For instance, users are more comfortable providing personal information for safety purposes when there is already a data privacy law on the books that limits the sale, storage, and use of that information.

As we have outlined above, age assurance is technically and operationally complex. Age assurance at the device level can be a helpful approach as a "signal" or "flag" of the user's age could theoretically be used to allow or restrict access to other apps and websites, however there are some major questions and limitations to this approach as well. There are significant technical questions about how a "signal" would actually flow interoperably between the hardware of the device and the software of the app stores and individual apps and websites themselves. We will defer to technical experts to expand on this issue.

Then there are the simple logistical questions of families who share devices between multiple people, which is especially true among low income families. Sharing a device across siblings or even intergenerationally significantly reduces the promise of device-level age assurance. We will also note that an age "signal" or "flag" are new terminologies that need to be carefully, thoughtfully, and technologically defined in order to give clarity to industries that must comply with the new law.

There have been significant efforts to work through the feasibility of interoperable age assurance solutions, and I would point you towards two resources for more information: the euCONSENT project and the Age Verification Providers Association.

Conclusion

FOSI applauds New York's commitment to ensuring a safe online experience for young people. The SAFE for Kids Act acknowledges that parents should not have complete

control over a minor's access to social media or information and that some parental guidance is needed. However, the complex issue of age assurance and the consequences of some youth being disproportionately impacted by the losses of privacy and access to information leaves room for the OAG to ensure thoughtful consideration when developing its rules for this law.

Thank you for the opportunity to comment. FOSI looks forward to working with the Office of the Attorney General as the rulemaking process continues and on future projects that involve youth online safety.

Respectfully,

Marissa Edmund
Policy Specialist
Family Online Safety Institute