Thank you for the opportunity to provide feedback on the Advanced Notice of Proposed Rulemaking. The Software & Information Industry Association (SIIA) is the principal trade association for the information industry. From digital platforms and global financial networks to education technology providers and B2B media companies – SIIA represents the businesses and organizations that make the world work.

The intent of the SAFE for Kids Act is to protect the mental health of children from addictive feeds and from disrupted sleep due to night-time social media use.[1] In this vein, our comments are driven by a recognition that kids deserve access to information and the virtual tools critical in keeping them connected and engrained in their communities – without fear of being exploited. Through a careful approach that incorporates lessons from past successes at protecting children online, we believe policymakers have the opportunity to prioritize the privacy and safety of kids while empowering parents to be active participants in how their child operates online.

Our responses to select questions for public comment follow:

Commercially reasonable and technically feasible age determination methods

Question 1: The SAFE for Kids Act requires social media platforms to use "commercially reasonable and technically feasible methods" to determine if a user is under the age of 18 (GBL section 1501(1)(a)). What are the key desired properties of an age determination method? What are key challenges to assessing any age-determination method?

Age determination mechanisms in general are highly likely to result in a company collecting more personal information than necessary for the requested activity, including about those under the age of 13. For example, a provider of an online service that allows readers to review books may collect only persistent identifiers, and may not even require users to create an account in order to use the service. The service would have no need to collect information such as name or email address, let alone sensitive information such as government identification, biometric information, bank information, or cognitive test results. This leads to an increased risk to individuals' privacy. It also heightens cybersecurity risk because operators holding a richer array of data are more attractive targets for malicious actors.

Furthermore, individuals who lack certain forms of identification, those with intellectual disabilities, and those who are especially privacy-conscious, may not want to or be able to provide the types of information necessary to determine user age. Even if a platform were to make available multiple methods of age determination from which the user could choose, those users who are unable to choose certain options — such as providing government identification

[1] NY State Senate Bill 2023-S7694A (nysenate.gov).

or taking a cognitive test — may be forced to choose among the remaining, possibly more privacy-invasive options, such as biometric assessments.

To the extent the OAG recommends age-verification mechanisms, it should take care to avoid those that 1) undermine the privacy of consumers, 2) impose an undue burden on users that deters Internet usage, 3) chill access to constitutionally protected speech, 4) perpetuate bias, or 5) are too prescriptive and fail to account for the unique characteristics and risks posed by each platform. Instead, the OAG should adopt requirements that limit the burden on users, require the least amount of information from users that is necessary, and preserve a platform's flexibility to determine or estimate age with a level of accuracy that is appropriate to the risks posed by its underlying service. This will help to avoid encouraging companies to collect more information than they otherwise would need to operate their services. The rules should also recognize the limitations of current technology and view age verification as a probabilistic determination.

Question 8: A number of entities currently have access to information that may reliably convey age, including banks, email providers (who may know how old an email address is), telecommunications companies, and smartphone operators. How could OAG's regulations ensure that age determination based on attestation from such entities is secure and protects user privacy?

We caution relying on entities including banks, email providers, telecommunications companies, and cell phone operators to determine. These companies and the data they are charged with collecting and protecting are subject to a variety of state and federal privacy laws. Using data in this manner may be far outside the scope of what those privacy laws allow. Any effort to rely on these entities should be done with great caution.

Question 11: How should OAG regulations account for technological changes in available age-determination methods, or changes in users' willingness to use certain methods?

We encourage the use of language that is technology neutral in any rulemaking that would allow for future innovations in this space.

Question 12: If OAG regulations require social media platforms to monitor browser or device signals concerning a user's age or minor status (similar to the do-not-track or universal-opt-out signals some browsers or devices presently employ), what factors should OAG consider when specifying an appropriate standard for those browser or device signals?

In creating standards for browser or device signals concerning a user's age or minor status, it is important to recognize that these tools may still be ineffective in some circumstances. For example, at a high level, these signals are incapable of differentiating when minors are using adult accounts to access social media platforms. Furthermore, especially if age data is sourced from a variety of third parties, conflicting or unreliable signals could result.

Any regulation must account for the fact that this technology is relatively new. The OAG regulations should include appropriate safeguards and requirements to ensure technologies used in this space are secure, particularly since they will be used to collect sensitive children's data. Additionally, the OAG should be careful in drafting regulations to ensure that they do not open avenues for malicious actors to take advantage of new data troves and a need for new technology solutions to perpetuate scams or other harms. It will be important for the OAG's office to provide oversight and assistance to this sector to protect New Yorkers from any adverse impacts of age flags.

Further, if a user reaches the age of majority, there may be scenarios where a local site is able to detect such a user's newfound adult status. However, a universal signal based on potentially out-of-date biometric information, bank information, or cognitive test results would not pick this up. Any regulations must account for this complication or other scenarios where a user might use a VPN, chooses privacy settings that limit flags, multiple users on one device or browser, multiple browsers on one device, for example.

Finally, signals indicating a user's age or minor status based on a patchwork of third party data could be in conflict. "Government data, biometric information, bank information, or cognitive test results," in particular, could each create conflicting indicators as to whether or not a user is a minor.

Question 15: While some social media platforms are open to the general public for all purposes, many are focused on a specific audience, such as professional networking or discussion of specific hobbies. In some cases, users may be significantly more likely to be an adult, or more likely to accurately self-attest concerning their age. How should OAG's regulations assess the audience of a given social media platform when assessing the cost and effectiveness of age-determination methods?

It is important to distinguish and understand that the search for learning and information is not limited to a child. Different platforms can be offered for specific adult populations through employers and companies. Companies will develop their own platforms or work with existing online platforms to provide educational services (professional development, education credit incentives, certifications) for their employees so that education benefits can be offered throughout an employee's career journey. These types of online platforms/services should not have to process their users through age verification. Requiring all users to disclose even more personal information than they do now to meet age-verification would mandate that they submit sensitive personal information like government IDs and biometrics to access online platforms. All of this to receive professional development or workforce training may be more cumbersome and potentially cause more harm than necessary.

<u>Parental consent</u>

Question 1: The SAFE for Kids Act permits social media platforms to provide children with an addictive feed or overnight notifications only when the platform had obtained

"verifiable parental consent" (GBL sections 1501(2), 1502). What methods do websites, online services, online applications, mobile applications, or connected devices presently use to determine whether an individual is the parent or legal guardian of a given user? What costs — either to the parent or to the website, online service, online application, mobile application, or connected device — are associated with these methods? What information do they rely on?

It is critical to avoid both decision and information fatigue on behalf of parents who are asked to provide parental consent on behalf of their children under the SAFE for Kids Act. The SAFE for Kids Act is distinct from COPPA and presents a greater risk of burdening parents because, unlike COPPA, the SAFE for Kids Act requires services to collect children's personal information *before* seeking parental consent. A natural risk of such a regime is that a company may contact parents several times seeking consent for a child's use of their service. In order to reduce the burden on parents, disclosing what information has been collected from a child and how it may be used, followed by a single request for consent, is the optimal method to acquire consent while reducing the burden on parents under the SAFE for Kids Act.

Conclusion

Thank you for your time and consideration. If you have further questions, please contact Sara Kloek at skloek@siia.net or Anton van Seventer at avanseventer@siia.net.