

September 30, 2024

Office of the New York State Attorney General
Attorney General Letitia James
The Capitol
Albany NY 12224-0341

Submitted electronically at: ProtectNYKidsOnline.ag.ny.gov

Re: ANPRM for the SAFE for Kids Act and the NY Child Data Protection Act.

Dear Attorney General James,

On behalf of Privacy Vaults Online, Inc. ("PRIVO"), thank you for the opportunity to provide comments on the Office of the New York State Attorney General ("OAG") Advanced Notice of Proposed Rulemaking ("ANPRM") to assist the office in crafting rules to protect children's privacy pursuant to the New York SAFE for Kids Act and the Child Data Protection Act ("CDPA"). PRIVO shares the OAG's goal of protecting children online from current and emerging privacy risks and harms to minors from the use of social media platforms and appreciates the opportunity to provide comments that may assist the office in crafting rules to protect children pursuant to New York General Business Law section 1500 et seq. (GBL section 1500).

Introduction and Overview of PRIVO

Over the past 20 years, PRIVO has emerged as one of the leading global industry experts in minors' online privacy, identity and consent management. PRIVO has served as an FTC-approved COPPA Safe Harbor since 2004 and provides its Kids Privacy Assured Program globally.

Our comments reflect insights and lessons learned from years of experience consulting with corporations and organizations to practically apply the regulatory requirements of COPPA and other child privacy regulations globally. PRIVO has developed privacy compliant technology solutions to support privacy preserving engagement with minors, across a wide range of commercial and education use cases. PRIVO's privacy tech platform provides companies with compliant microservices, APIs and SDKs to be configured based on use case specifics and relevant regulations by jurisdiction. PRIVO microservices include SMART age gates (which protect companies and kids by limiting user ability to change ages to an older age or delete and resubmit), software for properly providing parent notice and securing consent, and configurations to complete a diverse range of identity and age assurance and verification workflows. These solutions have been tested by companies across many industries and have the benefit of extensive feedback and iteration, to ensure compliance while supporting companies' interests in minimizing friction. PRIVO's newest configurable tools enhance the existing services by combining the power of an opt-in minors' protection registry that associates parent provided, minors'

true age with a simple-to-integrate query and response signal for companies, alerting subscribing companies (without creating new friction) when a minor is requesting access or engagement. PRIVO's privacy tech platform is also readily configurable for blocking minors' access based on user age, digital provider TOS, and relevant regulations. The company's leadership has invested time and attention to deeply understand the operational challenges introduced by minors' privacy compliance requirements in the United States and globally. We take great pride in the role we play in ensuring children's privacy and we look forward to collaborating with all efforts to improve the entire ecosystem of protection for minors.

Age determination methods

All age determination methods should include the following properties: data minimization, proportionality, data security, transparency, accuracy, ease of use and choice and dispute resolution. Each method should come with a data processing impact assessment to identify and mitigate risks.

Assessing methods is a challenge. Method providers need to give transparent information to relevant third parties such as regulators or assessors regarding processing activities and provide robust DPIAs and testing data.

To ensure the verification has integrity and is valid some transactional data needs to be stored. For example, in relation to a consent receipt where the user was asserted to be an adult associated to a child under the age of consent the operator must be able to deliver privacy notices to the parent and retain a consent receipt. Without this there is a lack of accountability and auditability that consent was provided by a parent or legal guardian.

There is no one size fits all solution, and the use of age assurance (resulting from proportional verification, estimation or determination) needs to be mapped to risk. Method providers would need to allow access to code and back-end processes for assessment and vendor agreements to ensure privacy principles such as data minimization are adhered to, to assess a method.

Users under the age of 18 do not generally have the hard attributes such as government issued ID required to verify their age and biometric methods are high risk for a child for several reasons we expand on below. It should be noted however that users under the age of 18 are highly verified in the school system and in healthcare.

As a result, one of the desired properties of an age determination method where the user is a child under 18 is to ensure a privacy preserving method that may include leveraging their well-established offline records. Any digital method should include the parent or legal guardian in the process. A verified adult could vouch for the age of their child or provide other hard attributes consistent with how the child is registered for school, sports clubs, summer camps, insurance plans and so on.

Methods that potentially collect and process data using AI to determine or infer age for example on a social media platform¹ will likely be collecting more data than required. Misuse of this profile by the

¹ [Introducing New Ways to Verify Age on Instagram](#) *about.fb.com* Meta June 23, 2022, updated March 2, 2023

online services /platforms is a real concern and there is a clear and obvious public mistrust in such services that have consistently shown lack of integrity when dealing with children's data².

Determining a user is a child by subjecting them to biometric methods brings risks. Children are taught not to share personal information online but then required to turn on their camera for facial age estimation. A child cannot agree terms and conditions of the method and can be easily defrauded.

The risks associated with fast, frictionless, anonymous age estimation of adults are not theoretical. The anonymity that the method provides, its data minimization, is the very aspect of it that invites its misuse. Concerns that adults will assist related and unrelated children by scanning their faces to pass as an older user when presented with facial age estimation methods is real. Indeed, the anonymity of the method creates the risk of bad actors using the method to permission many children onto online services precisely so that they can groom them entirely out of parental view.

Other, less nefarious scenarios also exist in which the method would allow circumvention of parental consent and rights. The child might create a new email for their parent, receive the email from the operator and simply bring their device to their parent asking the parent to look at the camera, explaining that it is merely a game or app that will give an answer as to whether they are 25 or older. The parent will not have received the notices and disclosures such as those required under the Children's Online Privacy Protection Act (COPPA)³ or been afforded the transparency required under the EU General Data Protection Act⁴ that by placing their face into the field, they have given their child access to what might be inappropriate and harmful online content.

While live testing is said to deter the use of static photographs children might proffer to trick the system, there is a real risk of deep fakes. In the child space, a single, successful deep fake created by one child or teen, could be sold, or passed around and used repeatedly to provide access to online services with no accountability for where the deep fake originated.

While broken age gates have led to high volumes of children accessing online services that do not offer adequate privacy and safety protections for them, self-declaration using a smarter robust age gate could be a first line of defense coupled with additional age assurance methods.

Children easily circumvent industry currently deployed versions of age gates meant to prevent access to online services or screen for age-appropriate experiences. When faced with an age gate, children often provide their current age and are denied access or at least instant access to the service as a result. They then attempt to circumvent the age gate by clearing their browser, switching to another browser, uninstalling and re-installing the app or similar tactics. Testing of current age gates on social media platforms show the gates will block a user that enters an age of 12 or under but if the user then opens an incognito window in the browser, they can enter an older date of birth in the age gate and sign up for an

² Allyn, Bobby, [Instagram makes all teen accounts private, in a highly scrutinized push for child safety](#) *NPR.org* NPR September 17, 2024

³ [Children's Online Privacy Protection Act](#) 16 CFR 312.4(a)

⁴ General Data Protection Act Article [13](#) & [14](#) The right to be informed (transparency)

account meant for an older user. Some parents, just as they may do with the R-rated movie, will allow, instruct, or facilitate their child circumventing the age gate. They may do this because they want to play a 13+ game with their eight-year child and are not worried about the risks that would normally be associated allowing the child to engage in that activity because the parent will be in the game and able to react to any negative situation. Or they may do it out of exhaustion with the seemingly unending blocking of the child from services that they are attracted to and want to join along with their friends, classmates and family.

What is important to understand, though, is that, unlike allowing a child to view an isolated R-rated movie, when an eight-year-old child (or parent on the child's behalf) lies to the age gate, they create a profile of an online user who appears to be 13 years or older and that profile lives on the Internet long after and is relied upon by untold number of downstream data providers and marketers.

However, rather than giving up on age gates as a sensible way to restrict children from accessing online services or providing them a dumbed down version of the service, regulators should encourage the development of smarter age gates.

PRIVO has developed age aware™ technology to complement its in-market smart age gate and parental consent service to strengthen online services' age gates and entry points. The technology uses opted-in attribute and device-level data to alert services that a child is at their digital door, preventing children being turned away from the age gate and then simply clearing the browser, changing browsers or re-installing the app to get a second bite at the age gate apple. Parents can enroll unique attributes and identifiers (cell phone, browser, device ids, email, parent contact data etc.) for protection when they purchase the device or hand it down to the child so that services will know that the device is primarily used by a child at or under a certain age.⁵ Regulators should encourage online services to begin to interoperate with solutions such as this so that the service or restricted activity within the service can gain the knowledge that an age protected child is attempting to access. It could then take the appropriate action to prevent child access or secure parental consent for the child to participate if appropriate.

Parents need simple to use solutions to managing the ever-increasing number of online services that their children will interact with throughout their development and to support older teens in navigating the services and providing age-appropriate evolving experiences as they get older. This solution could also be used by teens that need to verify age when they can provide their own consent. Online services also need a simpler solution to regulatory compliance than age verifying all users. Smarter age gates and innovations like the use of the age-aware device-level data solution that PRIVO has created meet both needs.

The only other signal in industry today is the Global Privacy Control (GPC)⁶ which provides a blanket opt out (do not sell my data). It does not provide for communicating age information, parental contact

⁵ Minors Protection Registry <https://www.privo.com/mpr> PRIVO

⁶ Global Privacy Control <https://globalprivacycontrol.org/>

information, is not jurisdictionally aware nor service specific, and is not robust enough to meet the needs of age determination.

In short parents should be able to protect their child by simply making the internet age aware™ once without having to continually share their child's or their personal data for inspection, surveillance and exploitation.

Parental Consent

Regarding the methods of obtaining parent consent industry today relies on what is reasonable in light of available technology mapped to levels of risk i.e. a sliding scale of consent proportionate to risk. To date and historically under COPPA the parent provides an assurance that they are the parent and verifies that they are an adult using one of the enumerated methods.⁷ There are widely adopted solely online methods for establishing the adult is the parent or legal guardian. However, as stated above, PRIVO encourages allowing parents and children to leverage already existing relationships widely used in an offline context, such as schools, and onboarding them for digital use. This would provide a high level of relationship assurance as well as a privacy preserving method for establishing age.

For consent to be valid⁸ it should be freely given, specific, informed and unambiguous. To be informed, notice must be in clear and accessible language. Notice should include the same requirements and standards already present in COPPA.⁹ Methods for revoking consent should be easily accessible. Looking to existing regulations such as COPPA and the GDPR to harmonize is vital if online services are to successfully implement and align requirements.

Regarding the cost of verification by approved methods, these can range from minimal for frictionless methods (such as an employee trusted domain, exiting verified digital credentials or school initiated) to 50 cents for verification of hard attributes against government databases.

Contextual Advertising & Permissible Processing

COPPA allows for the limited collection of identifiers solely to support the operation of a service. This exception¹⁰ to the Rule allows for limited advertising where no user information is disclosed onwards, and no profile is built to track the user across the internet to target or market to them. This limited form of contextual advertising ensures that many services in the children's space can earn revenue and do not have to charge users to access the online service. This collection for contextual advertising is vital to ensure a level playing field for children who should be able to enjoy online experience in a privacy safe manner at no financial cost while allowing such services to continue operating. PRIVO would urge that this same permissible use be included in these rules.

⁷ [Children's Online Privacy Protection Act](#) 16 CFR 312.2 "Obtaining verifiable consent"

⁸ [General Data Protection Act](#) Article 7 Conditions for Consent

⁹ [Children's Online Privacy Protection Act](#) 16 CFR 312.4(c)

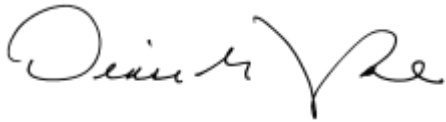
¹⁰ [Children's Online Privacy Protection Act](#) 16 CFR 312.2 "Support for the internal operations of the Web site or online service means"

Conclusion

PRIVO would urge the OAG to look to existing regulations such as COPPA, the GDPR and state privacy laws when crafting rules to protect children. This will support harmonization and ensure that industry can align requirements, particularly when it comes to the permissible processing of data, notices and parent consent. The OAG should also consider requiring online services to interoperate with neutral third-party privacy preserving solutions to support a privacy and safety enhanced online ecosystem.

PRIVO appreciates the opportunity to submit comments to the on this important topic. If we can provide any additional information, or otherwise assist your office as it continues to engage in the rulemaking process, please do not hesitate to contact us at dtayloe@privo.com and cquinn@privo.com.

Respectively submitted,



Denise G. Tayloe
Co-Founder & CEO
PRIVO



Claire Quinn
Chief Privacy Officer
PRIVO