1350 Eye Street NW, Suite 350, Washington, DC 20005 | 202-768-8950 | fpf.org

September 30, 2024

Via Electronic Submission

Office of the New York State Attorney General
The Capitol
Albany NY 12224-0341
ProtectNYKidsOnline@ag.ny.gov

Re: Advanced Notice of Proposed Rulemaking pursuant to New York General Business Law section 1500 *et seq*.

Dear Office of the Attorney General,

The Future of Privacy Forum ("FPF") is pleased to submit comments to the New York Attorney General's Office regarding the Advanced Notice of Proposed Rulemaking ("ANPRM") on the recently enacted New York SAFE for Kids Act ("SAFE Act").[1] FPF is a global non-profit organization dedicated to advancing privacy leadership, scholarship, and principled data practices.[2]

We appreciate the New York State Attorney General's Office's invitation for input on several timely topics subject to agency rulemaking under the recently enacted SAFE Act. Our comment addresses two key areas of child privacy compliance: age assurance and verifiable parental consent ("VPC"). FPF's comments are informational in nature, and do not seek to recommend or endorse any particular approach for conducting age assurance or verifiable parental consent, but instead intend to provide information about current industry practices to further inform the agency's rulemaking efforts.

Accordingly, we address the following:

1. **Age Assurance:** There are three primary categories of age assurance in the United States: age declaration, age estimation, and age verification. Each method has its own challenges and risks that should be carefully balanced between the state interest in protecting minors online, US tech industry infrastructure and capacity, and end-user realities when considering how to craft specific regulations for an age assurance requirement.
2. **Verifiable Parental Consent:** When exploring appropriate methods for verifiable parental consent, consider the known problems, concerns, and friction points that already exist with verifiable parental consent under COPPA.

---

[1] *Advanced Notices of Proposed Rulemaking on the New York Safe for Kids Act,* Office of the New York State Attorney General (released Aug. 1, 2024), https://ag.ny.gov/resources/individuals/consumer-issues/technology/protecting-children-online.

[2] The views expressed in this comment are those of FPF and do not necessarily reflect the views of FPF's supporters or Advisory Board.

3. **Strong data minimization, use limitations, and data retention standards could enhance data protection and user trust in age assurance and VPC requirements:** considerations for drafting regulations with user privacy in mind.

I. THERE ARE THREE PRIMARY CATEGORIES OF AGE ASSURANCE IN THE UNITED STATES: AGE DECLARATION, AGE ESTIMATION, AND AGE VERIFICATION. EACH METHOD HAS ITS OWN CHALLENGES AND RISKS THAT SHOULD BE CAREFULLY BALANCED BETWEEN THE STATE INTEREST IN PROTECTING MINORS ONLINE, US TECH INDUSTRY INFRASTRUCTURE AND CAPACITY, AND END-USER REALITIES WHEN CONSIDERING HOW TO CRAFT SPECIFIC REGULATIONS FOR AN AGE ASSURANCE REQUIREMENT.

The SAFE Act prohibits covered operators from providing covered users with addictive feeds unless the covered operator has used "commercially reasonable and technically feasible" methods of age assurance to determine that the user is not a minor.[3] In the case of a minor, covered operators must first obtain verifiable parental consent to provide an addictive feed to a minor.[4] A minor is defined under the SAFE Act as anyone under the age of 18.[5] Beyond establishing the feature-specific requirement for age determination, the SAFE Act designates the Office of the Attorney General as the rulemaking authority.[6] With this designation, the OAG is responsible for establishing regulations prescribing commercially reasonable and technically feasible methods of age determination and the appropriate levels of accuracy, while implementing statutorily-mandated considerations when drafting regulations – including a directive to identify at least one method that does not require a government ID or that allows a user to maintain anonymity to the covered operator.[7]

The OAG's ANPRM asks twenty-one questions concerning commercially reasonable and technically feasible age determination methods, incorporating the considerations for age determination established in the statute. FPF appreciates the clear efforts made by the New York Attorney General's Office to solicit a range of important perspectives and answers to best understand the current state of age assurance ahead of releasing a proposed rule. Age assurance is an umbrella term for methods used to discern the age or age range of an individual. In response to the increased demand for age assurance over time, three categories of age assurance have emerged which collectively capture the variety of methods available today: age declaration, age estimation, and age verification. Each category can be roughly defined by the practice with which the categorical methods are conducted, the general level of assurance of the methods, and the risks associated with the practices in each category. In response to the considerations established in the SAFE Act and the questions in the OAG ANPRM, FPF writes to engage on a few aspects of age assurance: identifying and explaining the three age assurance categories, key risks and challenges of these categories, and considerations for implementing an age assurance requirement within the scope of covered operators.

A. Category One: Age Declaration

Age declaration is the practice of having a user declare to a service provider, either for themselves or through a third party, that user's age. Due to the low threshold of information

[3] N.Y Gen. Bus. Law § 1501(1)(a) (2024).
[4] N.Y Gen. Bus. Law § 1501(1)(b) (2024).
[5] N.Y Gen. Bus. Law § 1500(3) (2024).
[6] N.Y Gen. Bus. Law § 1501(2)(A) (2024).
[7] N.Y Gen. Bus. Law 1501(2)(B) & (C) (2024).

required to engage in age declaration, this category generally offers the lowest degree of privacy risks and the lowest degree of accuracy to the service provider. Common methods of age declaration include self-declaration age gating and third-party or parent vouching. For self-declaration, a user typically self-attests their age in a neutral manner. An example of a neutral age screen would be a system that allows a user freely to enter the month and year of birth.[8] For vouching either by a parent or others, a parent can submit a form attesting to a user's age, or third-party individuals may be selected by a user to confirm the user's age to a service provider through a method called 'social vouching.'[9]

While the privacy risks involved in age declaration are low and anonymity is best preserved through age declaration methods, the greatest challenge to this category is the lower level of efficacy in confidently and accurately confirming a user's age. Self-declaration poses a low barrier to entry and involves less friction to an end user's ability to access a particular site or service since declaration methods typically require little to no verifiable information about an individual. However, the low barrier to entry also makes it very easy for an end user to lie about their age, leading to inaccuracies in the specific age or age range reported to an online service provider and a limited capacity for effectively ensuring a user truly is the age reported. Even though the privacy risk to users who engage with age declaration methods is low, the risk is not absent. As a result, consideration should still be afforded to assessing and mitigating potential privacy risks, especially in circumstances where age declaration would involve collecting a user's birthdate, social connections, or other cursory information about a particular individual necessary for carrying out vouching methods.

B. Category Two: Age Estimation

Age estimation is the practice of estimating a user's age via algorithmic analysis of that user's biometric information, such as facial data, or data collected on their online presence and behavior, such as their profile and activity.[10] Age estimation, depending on the technical implementation, could carry a higher degree of privacy risks as a result of a greater demand for and processing of personal data collection to execute such methods. However, this category of methods can also be more effective than age declaration for ensuring a given user's age. Common methods of age estimation include AI facial characterization and social graphing.[11] AI facial characterization methods utilize AI systems trained to analyze a live video or still photo of a user's face to estimate their age range. While this method can be generally effective for placing users into age bands or signaling that a user meets a specific age threshold, this method is less effective at accurately discerning a user's exact age or narrow age ranges, such as the difference between a 17-year-old and an 18-year-old. Social graphing is an algorithmic estimation method that estimates a particular age or age range based on browsing history, voice, gait, or using multiple data points or signals from a user's activity to infer age.[12]

---

[8] FTC, Complying with COPPA: Frequently Asked Questions, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions

[9] Sarah Forland, Nat Meysenburg, & Erika Solis, *Age Verification: The Complicated Effort to Protect Youth Online,* New America (April 2024), at 12 https://d1y8sb8igg2f8e.cloudfront.net/documents/Age_Verification_The_Complicated_Effort_to_Protect_Youth_Online_2024-04-22_165_bS2AcQ5.pdf; Meta, *Introducing New Ways to Verify Age on Instagram* (June 22, 2023), https://about.fb.com/news/2022/06/new-ways-to-verify-age-on-instagram/.

[10] See Bailey Sanchez and Jim Siegl, *New FPF Infographic Analyzes Age Assurance Technology & Privacy Tradeoffs*, Future of Privacy Forum (June 26, 2023), https://fpf.org/blog/new-fpf-infographic-analyzes-age-assurance-technology-privacy-tradeoffs/; and, Forland, Meysenburg, & Soils, *supra* note 9 at 10.

[11] See Forland, Meysenburg, & Soils, *supra* note 9 at 12.

[12] Sanchez and Siegl, *supra* note 10 at 12.

Although this category of methods can be more effective at accurately determining a user's age, the heightened privacy risks incurred by the increased demand for data should be carefully considered and mitigated before implementation. In addition to the heightened privacy risks for methods in this category, there are also some equity and efficacy challenges associated with this method that should be considered when determining whether age estimation methods of age assurance are appropriate for a particular use case. For instance, efficacy challenges may limit the accuracy of this method where, as noted above, the estimation process is unable to precisely measure a user's specific age or make a distinction between narrow age ranges. Such efficacy limitations can also be paired with and compounded by equity challenges. For example, studies have found that AI facial recognition methods are less effective at accurately assessing various characteristics between different races and genders, leading to discriminatory results.[13] The overall impact of the efficacy and equity challenges could cause an increase in unequal access to online sites, services, and features whereby some users are limited from otherwise legitimate access resulting from estimation inaccuracies. This friction and unequal access to content might result in a burden to industry competition and users' chilled access to content.

C. Category Three: Age Verification

Age verification is the practice of validating a user's age, oftentimes using government identifiers or other sensitive information capable of authenticating whether a user is an adult or a minor.[14] Because methods in this category allow an age authenticator to accurately discern a user's age or adult status, this category provides the highest level of accuracy of all the available categories and methods. The tradeoff for the higher level of accuracy is a higher risk to privacy since methods in this category typically require users to provide sensitive personal information to online service providers or third-party authentication providers to participate in the verification process. Examples of methods within this category include verification using a digital ID through a service like Yoti,[15] verification of bank account or credit card information, verification through a combined biometric and government ID process whereby a user's face is compared against the government ID using facial recognition, or just verification via government ID submission.[16]

Even though age verification yields a high degree of efficacy for discerning a user's age, this category of methods still faces several challenges that should be considered by the OAG when assessing whether age verification is appropriate in light of the policy goals. For instance, equity risks complicate some verification methods where there are disparities in individuals' possession of a government ID, credit card, or bank account, which may hinder some users' ability to complete required age verification processes.[17] Along with equity and privacy risks, another key challenge that should be considered when determining whether age verification methods are

---

[13] See Tzvi Ganel, Carmel Sofer & Melvyn A. Goodale, *Biases in human perception of facial age are present and more exaggerated in current AI technology*, 12 Sci Rep Page (2022), https://www.nature.com/articles/s41598-022-27009-w; and, Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Proceedings of Machine Learning Research (2018), https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[14] See Sanchez & Siegl, *supra* note 10 at 10.

[15] See generally Yoti, *Digital ID: the fastest way to connect with verified customers* (last visited September 25, 2024), https://www.yoti.com/business/digital-id/.

[16] See generally Sanchez & Siegl, *supra* note 10; see also, Forland, Meysenburg, and Solis, supra note 9 at 12.

[17] See e.g., Fed. Deposit Ins. Corp. *FDIC National Survey of Unbanked and Underbanked Households,* 1, 13 (2021) https://www.fdic.gov/analysis/household-survey/2021report.pdf (finding that roughly 5.9 million households in the United States lack accounts in a bank or other financial institution); FUTURE OF PRIVACY FORUM, *The State Of Play: Is Verifiable Parental Consent Fit For Purpose?*, at 12 (Jun. 2023), https://fpf.org/wp-content/uploads/2023/06/FPF-VPC-White-Paper-06-02-23-final2.pdf.

appropriate includes the potential for increased friction in the process for access to or use of an online service.[18]

D. Considerations For Implementing Age Assurance

Despite the development of three distinct categories and a variety of methods to conduct age assurance, there is no one-size fits all approach to how age should be determined online in response to the surge of new legislative proposals. The best age assurance method for a particular site, service, or feature is generally context and use case specific. When crafting regulations for age assurance under the SAFE Act, the OAG should consider how to direct or otherwise allow for proportionality between the child safety goals of an age assurance requirement and the risks to privacy and legitimate access to services when identifying acceptable methods and levels of accuracy.

A proportionality approach to age assurance carefully balances the necessary level of certainty in a user's age for access to a given online site, service, or feature against the risks of privacy violations, efficacy and equity issues, or barriers to legitimate access to content. Assessing age assurance requirements through the lens of proportionality is highly beneficial because doing so could offer covered operators the flexibility necessary to adequately and appropriately comply with age restriction requirements based on context and specific use case. By building age assurance mechanisms around context and use case, covered operators would be better positioned to implement requirements while simultaneously preventing an undue burden on a user's legitimate access to online services and more successfully mitigating the risks and challenges of various methods.[19]

II. WHEN EXPLORING APPROPRIATE METHODS FOR VERIFIABLE PARENTAL CONSENT, CONSIDER THE KNOWN CONCERNS AND FRICTION POINTS THAT ALREADY EXIST WITH VERIFIABLE PARENTAL CONSENT UNDER COPPA.

The SAFE Act prohibits social media platforms from providing children with addictive feeds or overnight notifications unless platforms obtain verifiable parental consent from the child's parent. The OAG asked several questions about parental consent, including what methods are presently used, what are the costs of these methods, how to make requests for consent understandable and effective, and obligations the OAG regulations should specify concerning how platforms request VPC. FPF writes to address these specified topics.

COPPA established the process of verifiable parental consent ("VPC") with the goal of keeping children safe online and ensuring parents are informed and engaged in their child's online activity.[20] COPPA requires operators to obtain VPC before any collection, use, or disclosure of child information unless one of eight narrow exceptions to the VPC requirement apply.[21] In similar fashion and spirit, many child privacy and safety legislative proposals today continue to incorporate parental consent requirements, including the SAFE Act. As a result of the longevity of COPPA and the pre-established framework for obtaining VPC, FPF recommends that the lessons and observations around the known problems, concerns and friction points under COPPA should be considered when developing a VPC rule under New York law.

---

[18] See generally Sanchez & Siegl, *supra* note 10.
[19] See *id.*
[20] See the Future of Privacy Forum, *supra* note 17.
[21] See 15 U.S.C. 6501 *et seq.*; 16 C.F.R. 312.5.

A. Brief Overview of VPC Methods Under COPPA

Under COPPA, when an operator is required to obtain VPC, they must implement a method that is "reasonably designed in light of available technology" to verify that a child's parent gives consent.[22] In furtherance of this requirement, the FTC has determined that several methods meet the rule's standard and provided a non-exhaustive list of approved VPC methods.[23] Current FTC-approved methods for obtaining VPC under COPPA include:

- Signing a physical consent form and sending it back via fax, mail, or electronic scan;
- Using a credit card, debit card, or other online payment system that provides notification of each separate transaction to the account holder;
- Calling a toll-free number staffed by trained personnel;
- Connecting to trained personnel via a video conferencing;
- Provide a copy of a form of government-issued ID that the operator checks against a database, as long as that identification is deleted from internal records upon completion of the verification process;
- Answer a series of knowledge-based challenge questions that would be difficult for someone other than the parent to answer;
- Verify a picture of a driver's license or other photo ID submitted by the parent, and then compare that photo to a second photo submitted by the parent, using facial recognition technology.[24]

Even with a limited number of approved methods, it is important to note that the list above is not a comprehensive catalog of all methods currently available or used by industry to achieve VPC today. Although the FTC provides a list of approved methods, COPPA does not require operators to only use methods approved by the FTC.[25] Out of an abundance of caution, most operators utilize FTC approved methods for gaining consent.[26] However, operators who opt to employ novel, non-FTC-approved methods of VPC run the risk of noncompliance with COPPA and subsequent agency enforcement.

One of the biggest criticisms of the VPC structure under COPPA is that the methods of VPC currently provided within this framework are limited and quickly get outdated where agency action cannot keep up with technological change.[27] To address this criticism, in 2013 the FTC added a VPC approval mechanism within COPPA regulations.[28] This mechanism provided operators or other industry members with a process to submit proposals for new VPC approaches to the FTC for agency consideration. FTC approval of a proposal secures the

---

[22] Federal Trade Commission, *Verifiable Parental Consent and the Children's Online Privacy Rule,* (Accessed Sept. 19, 2024), https://www.ftc.gov/tips-advice/business-center/privacy-and-security/verifiable-parental-consent-childrens-online-privacy-rule.

[23] See the Future of Privacy Forum, *The State Of Play: Is Verifiable Parental Consent Fit For Purpose?, supra* note 12.

[24] See Federal Trade Commission, *Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business* (last accessed Sept. 25, 2024), https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business#step4. See also See 16 C.F.R. § 312.5.

[25] See FTC; see also *supra* note 19.

[26] See the Future of Privacy Forum, *supra* note 17 at 16.

[27] See *id.* (p. 16-17).

[28] See 16 C.F.R. § 312.12.

submitter formal assurance from the agency that their method complies with COPPA and provides a new method to be included within the FTC's approved VPC methods list.

Despite the addition of this approval mechanism, approved VPC methods remain limited and fall behind the realities of technological modernity. The FTC's VPC approval mechanism is complicated by a time-consuming and at times arduous process that results in few method approvals.[29] The high rate of rejection paired with the time and cost of participating in the submission process has stymied the submission of new VPC proposals to the FTC.[30]

Additionally, under COPPA's safe harbor program, a safe harbor may approve its member operators' use of a parental consent method not currently enumerated under COPPA where the safe harbor program determines that such parental consent method meets the requirements of COPPA[31].

These observations regarding the VPC framework under COPPA provide key insights for drafting regulations on VPC today. In light of the challenges facing the VPC framework under COPPA, FPF recommends that the OAG considers how to best factor flexibility into the required VPC framework while still achieving the policy goals motivating the authorizing statute. Suggested ways in which the OAG could best learn from the lessons of COPPA and draft a rule with sufficient flexibility for both covered operators and parents to complete the VPC process include:

- Adopting a regulatory approach which prescribes a criteria-based framework describing elements or standards for VPC that a social media platform must achieve for compliance as opposed to strictly prescribing a limited number of approved methods; or,
- If the OAG were to adopt a regulatory framework similar to the FTC's approved VPC methods list, to consider including alternative and more technologically relevant methods of obtaining VPC, such as through mobile phone text messaging, platform-mediated VPC, VPC during setup at the direction of the parent, alternatives to credit card VPC methods, and other more timely and appropriate methods. Along with including more technologically relevant methods within an approved methods list, the OAG could also address the longevity and relevancy challenges observed under the COPPA VPC framework by offering a more timely approval process for new methods. An alternate, more timely approval process could either incorporate an independent review panel dedicated to reviewing and approving new methods or implement a "regulatory sandbox" where new VPC approaches could be tested and assessed for regulatory approval.

B. Concerns and Friction Points with VPC

Aside from the problems besetting the availability of approved VPC methods, there are still considerable challenges in implementing existing VPC requirements which generates friction points for parents and children seeking access to online services. For the OAG's consideration during rulemaking, the costs of VPC to online service providers, parents, and children stem largely through identified friction points. Therefore, awareness and consideration of common friction points during the rulemaking process should provide insights for crafting a more effective rule under New York law for all stakeholders.

---

[29] Between 2013 when the approval mechanism was first introduced and 2015, six VPC proposals were submitted to the FTC but only 2 were ultimately approved. The last VPC proposal was submitted to the FTC for review in 2015 – no new VPC proposals have been submitted through the approval mechanism since. See the Future of Privacy Forum, *supra* note 17 at 16-17.

[30] See *id* at 17.

[31] COPPA § 312.5(c).

There are four relevant friction points to consider when crafting a rule for VPC under the SAFE Act based on concerns and challenges observed through the approved methods of the COPPA framework: (1) efficacy; (2) accessibility; (3) hesitancies, privacy, and security; and, (4) convenience and cost barriers.

1. Efficacy challenges: Efficacy challenges occur where children can easily circumvent low-assurance age declaration processes or VPC methods to get access to age-restricted content and services. When FPF engaged parents on their experiences and challenges with VPC, one parent noted that there are various ways that children can easily get around VPC requirements "by making up birthdays, finding wallets around the house for their parents' IDs, or entering their own credit card or email information into a VPC prompt."[32] The efficacy issues observed in some of the current methods beg the question of whether utilizing methods with greater privacy and security risks, such as methods that rely on the collection or use of credit card information or government IDs, are proportional to the purported benefits of requiring VPC. Despite the challenges around efficacy, parents expressed greater comfort with participation in lower risk methods such as calling a phone number or signing a parental consent form even if these methods can also be easy for savvy children to circumvent.[33] Additionally, efficacy around the VPC methods involving credit card information are increasingly called into question.[34] With more and more children today having access to credit cards, the assumption that credit card information can successfully communicate to an online service that a particular individual is an adult or is a parent is becoming increasingly tenuous.[35]
2. Accessibility challenges: Accessibility challenges are largely exacerbated by the fact that prevailing methods for VPC often necessitate the provision of credit card or debit card information or government ID information, which causes equity issues. As a 2021 Federal Deposit Insurance Corporation survey found, roughly 5.9 million households in the United States lack accounts in a bank or other financial institution, which undermines their ability to complete VPC steps requiring such information.[36] Additionally, when it comes to methods requiring use of a government ID, equity issues exist where certain segments of the population, such as undocumented immigrants, lack access to government identification, causing higher bars to access certain content and features for specific populations.[37]
3. Hesitancies, privacy, and security challenges: Where current approved VPC mechanisms may require a parent to provide sensitive personal information, such as credit or debit card information or a government ID, privacy and security risks increase. Along with the increase in risk, parents broadly demonstrate "discomfort" with requests to share this sensitive personal information and "having that information linked to their children's online presence."[38] Compounding the privacy issues within currently approved VPC methods is the fact that relying on methods which require collection and use of sensitive personal information for VPC and age assurance processes runs counter to data

[32] See *id* at .11.
[33] See *id.*
[34] See *id* (p. 11).
[35] See *11 Surprising Teen Credit Card Statistics,* CardRates (Jan. 23, 2024), https://www.cardrates.com/advice/teen-credit-card-statistics/#:~:text=Only%208%25%20of%20Teens%20Have,a%20credit%20card%2C%20on%20average; see also Herb Weisbaum, *How young is too young for a kid to have a credit card?*, NBC News (August 6, 2019), https://www.nbcnews.com/better/lifestyle/how-young-too-young-kid-have-credit-card-ncna1039536.
[36] See Fed. Deposit Ins. Corp., *supra* note 17.
[37] See the Future of Privacy Forum, *supra* note 17 at 12.
[38] *Id* at 12.

minimization goals motivating online privacy and safety frameworks like the SAFE Act. As noted by the Electronic Privacy Information Center in comments previously submitted to the FTC regarding VPC methods, methods requiring parents to provide sensitive personal information, "exposes…parents to the same privacy risks they are trying to protect their children from," generating hesitancy among parents about whether to complete the process.[39] Along similar lines, parents have expressed that requests to provide sensitive information during the VPC process causes them to question the appropriateness of the online site or service for their child, regardless of how well the operator actually protects user privacy.[40] Where the goals of the SAFE Act intend to empower parents to engage in their child's online experience and assess online services for appropriateness, establishing VPC frameworks predicated on the provision of sensitive personal information undermines the overall objectives of the statute.

4. Convenience and cost barriers: The lack of convenience in available VPC methods under COPPA, which struggle to keep up with modern technology and accessibility and are complicated by privacy and security concerns, takes a noticeable toll on children and parents, often resulting in user drop-off for COPPA-compliant services due to heightened time and effort costs. Given these existing lessons and observations, the OAG should carefully assess whether particular requirements or prescribed methods of obtaining parental consent under SAFE Act regulations would provide a meaningful *and* convenient way for parents to participate in their child's online experience or if the framework would cause hesitancy, confusion, or user dropoff among children and their parents.

The amalgamation of these challenges ultimately results in unintended consequences which undercut the goals of child privacy and safety frameworks. Consequences of these challenges include driving children towards adult-versions of websites and services and disincentivizing the development of child appropriate services and features. To address the common challenges and friction parents, children, and online service providers experience under existing VPC frameworks, FPF proposes the following two recommendations for the OAG:

- Approach drafting the rule with the goal of implementing a flexible criteria-based VPC approach that allows for modern, convenient methods of completing VPC and critically analyzing whether methods which require more data collection or sensitive data collection are actually effective in meeting the intended policy goals of the SAFE Act.
- Consider implementing within any required notice to users regarding the age assurance and VPC processes language which explains why the information necessary for these processes is being collected, how it will be used, how long it will be retained, and the purpose of collection and processing to alleviate user confusion and hesitation around completing these processes.

III. STRONG DATA MINIMIZATION, USE LIMITATION, AND RETENTION STANDARDS ENHANCE DATA PROTECTION AND USER TRUST IN AGE ASSURANCE AND VPC REQUIREMENTS: CONSIDERATIONS FOR DRAFTING REGULATIONS WITH USER PRIVACY IN MIND.

The OAG asked questions in both the age determination and parental consent sections regarding how regulations can ensure the privacy and security of data used in age determination and VPC processes and how to best communicate privacy and security assurances to users. FPF writes to

---

[39] EPIC, *EPIC, CDD, Fairplay Comments to the FTC on Proposed Parental Consent Method Submitted by Yoti Inc. under COPPA Rule*, 4 (2023), https://epic.org/documents/epic-cdd-fairplay-comments-to-the-ftc-on-proposed-parental-consent-method-submitted-by-yoti-inc-under-coppa-rule/.

[40] See the Future of Privacy Forum, *supra* note 17 at 12.

offer recommendations in response to these questions, while also drawing on requirements for social media platforms already established in the SAFE Act statute.

The SAFE Act prescribes strict data use and retention limits, requiring that (1) information collected for purposes of age determination or VPC are not used for any other purpose than age determination or VPC; and, (2) the information must be deleted immediately after an attempt to determine age or obtain consent, unless applicable provisions of New York or federal law require otherwise.[41] As a result of these statutory provisions, the SAFE Act establishes a foundation of privacy and security standards by implementing strong use limitation and data retention provisions for the data collected and used for age assurance and VPC.

Beyond the use limitation and data retention safeguards included in the statute, the OAG's ANPRM asked related questions in both the age assurance and VPC sections about additional mechanisms or considerations the OAG should undertake to address user privacy and security during these processes. Furthermore, the ANPRM included a question about incorporating data minimization within this regulatory framework and what lessons are available from other regimes. Given these questions, another privacy principle that would improve the privacy and security of age assurance and VPC methods in tandem with the existing statutory requirements is data minimization. Data minimization is the practice of limiting the personal data collected by an operator to what is necessary and reasonable to a specific purpose or use case. While incorporating data minimization principles into the age assurance and VPC framework under the SAFE Act would be good for user privacy, establishing a single bright-line rule for data minimization across a variety of risk levels, differing methods, and use cases would be difficult in context of these regulations. Rather than focusing on a bright-line rule, data minimization can also be embraced through alternative regulatory framing. Considerations the OAG should think about when drafting guardrails to enhance privacy and security principles, such as data minimization, within this regulatory framework include:

- Offering flexibility and options in the age assurance and VPC methods covered operators can make available to users so they are able to choose methods that align with their preferences for data disclosure and collection. Emerging methods for age assurance include social graph age estimation, vouching, and reusable token;[42] and,

- Exploring and encouraging the feasibility of methods under this framework that minimize or prevent the disclosure of user personal information directly to covered operators, such as zero-knowledge proof methods. A zero-knowledge proof, or double-blind system, confirms to an operator that the user meets the age requirement but shares no other information. Researchers at CNIL's Digital Innovation Laboratory have demonstrated the feasibility of one such zero-knowledge proof.[43]

For more information on data minimization regimes and how data minimization principles are incorporated within other contexts and frameworks, FPF also submitted comments to the OAG on

---

[41] N.Y Gen. Bus. Law §§ 1501(3) and 1501(5) (2024) https://legislation.nysenate.gov/pdf/bills/2023/S7694A.
[42] See Sarah Forland, Nat Meysenburg, & Erika Solis, *Age Verification: The Complicated Effort to Protect Youth Online*, New America (April 2024), at 12 https://d1y8sb8igg2f8e.cloudfront.net/documents/Age_Verification_The_Complicated_Effort_to_Protect_Youth_Online_2024-04-22_165_bS2AcQ5.pdf.
[43] CNIL, Demonstration of a privacy-preserving age verification process, Accessed Sept. 27, 2024, https://linc.cnil.fr/demonstration-privacy-preserving-age-verification-process (June 2022).

the New York Child Data Protection Act and addressed the topic of data minimization standards within that comment.[44]

* * *

Thank you for this opportunity to provide comment on these proposed regulations. FPF welcomes any further opportunities to provide resources or information to assist in this important effort. If you have any questions regarding these comments and recommendations, please contact Daniel Hales at dhales@fpf.org.

Sincerely,

Daniel Hales

Youth & Education Policy Fellow

Future of Privacy Forum

[44] FPF's comments on the OAG's New York Child Data Protection Act ANPRM were submitted contemporaneously to these comments and therefore cannot be linked here. To view those comments, please contact Daniel Hales or find them on fpf.org if available. Additionally, for more on data minimization regimes and different approaches to data minimization, see generally, Jordan Francis, Unpacking the shift toward substantive data minimization rules in proposed legislation, IAPP (2024), https://iapp.org/news/a/unpacking-the-shift-towards-substantive-data-minimization-rules-in-proposed-legislation (last visited Sep 27, 2024).