Office of the New York Attorney General Letitia James

Economic Justice Division

Stop Addictive Feeds Exploitation (SAFE) for Kids Act

Assessment of Public Comment

July 2026

Table of Contents

Summary

On June 20, 2024, the Stop Addictive Feeds Exploitation (SAFE) for Kids Act (referred to as the "Act") was signed into law. The Act prohibits online platforms from providing minors with an addictive feed, defined as using data concerning a minor (or the minor's device) to personalize the material the minor sees. Addictive feeds are a feature linked to addictive behavior and extending time spent on social media to unsafe levels. The Act also prohibits covered operators from providing nighttime notifications to minors concerning addictive feeds between the hours of 12 AM and 6 AM Eastern. The Act allows for parental consent and includes other provisions that ensure users can benefit from the Act's protections while preserving user security and privacy and allowing a healthy online experience.

Sections 1501, 1505, and 1506 of the Act expressly charge OAG with promulgating regulations to effectuate the Act's provisions, including those pertaining to commercially reasonable and technically feasible age assurance and verifiable parental consent, and to support the Act's enforcement.[1] The OAG issued an advanced notice of proposed rulemaking (ANPRM) on August 1, 2024, inviting targeted and general public feedback and engagement.

On September 15, 2025, OAG issued a Notice of Proposed Rulemaking (NPRM), which reflected comments submitted in response to the ANPRM as well as OAG's own research, experience, and expertise in investigating harms to New Yorkers related to social media and other technologies, online privacy, and online safety. This research included extensive dialogue with key stakeholders, including affected industries and technology experts. The OAG invited all interested parties to submit comments responding to the NPRM.

The NPRM comment window closed on December 1, 2025. The OAG received 78 comments from various parties, including from academia, operators of online platforms, age assurance firms, advocacy organizations, trade and industry organizations, a local government agency, and general members of the public including self-identified New York parents, New York minors, and owners of New York small businesses. Many comments reflected deep engagement with the proposed rule and OAG greatly appreciates all comments received. This assessment contains OAG's full and complete responses to comments, generally organized by the underlying theme or section of the rule, as appropriate, to which a comment was directed.

After consideration of all comments received, OAG makes no substantial revisions to the rule.[2] The OAG considered each comment in finalizing the rule. The OAG relies on the Regulatory Impact Statement published on September 15, 2025. The revisions to the regulatory text do not reflect any change from the reasoning in the Regulatory Impact Statement published as part of the NPRM. This assessment of public comment notes the revisions made to conform

[1] G.B.L §§ 1501(1)(a)(b),(2),(4); 1505, 1506.
[2] See State Admin. Proc. Act §§ 102(9), 202(4-a).

with the Regulatory Impact Statement published as part of the NPRM, technical edits, and minor clarifications and corrections. The rule is adopted as proposed with such revisions as follows:

- Section 700.1(a) has been streamlined by removing the reference to a particular standard, while continuing to allow for any recognized industry standard.
- The definition of addictive online platform in section 700.1(d) more clearly states (but does not change) the period over which operators can measure user time.
- The definition of delete in section 700.1(p) is made consistent with section 700.7.
- The definition of monthly active user in section 700.1(y) clarifies that a user need only be considered a monthly active user of an online platform if their access to the platform includes access to an addictive feed.
- For parental consent, the requirement regarding notice in the 12 most commonly spoken languages in sections 700.1(ii), 700.2(e)(5)(i), and 700.3(e)(5)(i) is clarified to state that notices in those languages must be made available but need not be provided simultaneously in all 12 languages.
- "Statistically significant" is deleted from section 700.5(c)(1) for clarity as described in the Part II.D.7 herein.
- Sections 700.7(a) and (b) are modified to clarify in the regulatory text that data use must be limited to the purposes detailed in the rule and that retention of data is required for 5 rather than 10 years.
- Section 700.9(b) is modified to be consistent with G.B.L. § 1504, under which a covered operator cannot discriminate against any user, whether the user is a minor or adult, based on its required compliance with this law.
- Section 700.9(e) is added to be consistent with G.B.L. § 1501(7), and reiterates that the rule shall not be construed to limit an operator from restricting access to media the operator deems objectionable.

The OAG also corrects several typographical errors as follows:

- Section 700.1(l) contained incorrectly formatted references to ISO/IEC 27566-1 and IEEE 2089.1 and had subsections that were misnumbered. Those provisions are corrected.
- Section 700.1(bb) was missing a period at the end. That provision is corrected.
- Section 700.1(ii)(3) was missing the word "to" and had an incorrect internal reference. Those provisions are corrected.
- Section 700.2(e)(1)(ii) had an error in an internal reference, referring to subdivision (d) rather than the same subdivision. That provision is corrected. The same change is made in the corresponding provision of section 700.3(e)(1)(ii).
- The internal references in sections 700.2(e)(4) and 700.3(e)(4), though correct, were incorrectly formatted and are corrected.

- Section 700.2(e)(6)(ii) of the proposed regulatory text was both misnumbered as (i) and the internal reference was incorrect. That provision is corrected to reflect that operators complying with section 700.2(e)(6) must conduct annual review of the parental consent method. The same change is made in the corresponding provisions of section 700.3(e)(6)(ii).
- Section 700.3(e)(6) had an incorrectly formatted internal reference, while the corresponding reference in section 700.2(e)(6) was correct, and was missing a colon at the end of the first paragraph. That provision is corrected.
- Section 700.3(e)(6)(i) had an incorrect internal reference, while the corresponding reference in section 700.2(e)(6)(i) was correct. That provision is corrected.
- Incorrect formatting of internal references in section 700.4(b) are corrected.
- Section 700.9(d) had a superfluous “in” which has been deleted.

Public Comment Assessment

The OAG carefully reviewed and considered every comment submitted. Where commenters raised multiple distinct issues, the sections are further organized by theme to address those comments independently. Where appropriate, comments regarding particular provisions are combined and addressed together.

The OAG makes no other changes except as noted.

I. Comments addressing background, statutory authority, and legislative objectives

This Part I addresses substantial and material issues raised by commenters in response to the background, statutory authority, and legislative objectives sections of Regulatory Impact Statement.

Theme: Some commenters asserted current research does not conclusively demonstrate that addictive feeds and nighttime notifications cause mental health harms in minors.

Research amply demonstrates that addictive feeds and nighttime notifications cause mental health harms in minors, as summarized in Part II.B.2 of the NPRM. The majority of comments submitted to OAG, including comments submitted by organizations with relevant medical and scientific expertise, agreed.

Virtually all comments accorded with the NPRM on the point that minors' brains are still developing and thus are more vulnerable than those of adults to external influences. Multiple comments further supported the observation that addictive feeds and nighttime notifications undercut an individual's self-control, with more pronounced effects in minors because their brains are not fully developed. As a result, it is far more difficult for a minor to stop using addictive feeds and nighttime notifications on their own, even when the minor is well aware that these features are harming them. Research cited by commenters as well as the NPRM confirms this conclusion.

Only a few comments disputed the NPRM's research summary. For example, one commenter stated that no evidence shows these features cause harm. This is clearly contrary to available studies cited both in the NPRM and by some commenters. The same comment suggested that because "social media addiction" is not a recognized clinical condition, all studies demonstrating harms caused by addictive feeds and nighttime notifications can be dismissed. The OAG disagrees. Recognition as a clinical condition is not a precondition to the existence of harm. Moreover, as noted in the NPRM and multiple comments, harms including "problematic use" exist and have been observed.

Finally, a few comments acknowledged that current research shows addictive feeds and nighttime notifications cause mental health harms in minors while highlighting studies that demonstrate how other aspects of some online platforms may provide some benefits to some

minors.[3] The Act addresses the harms attributable to specific platform features while maintaining a covered minor's ability to access the rest of an online platform and the benefits that might be associated with such access. G.B.L. §§ 1501 and 1502 apply the parental consent requirement only to two features, addictive feeds and nighttime notifications, while G.B.L. § 1504 explicitly protects a covered minor from being blocked from accessing other parts of an online platform. As the legislative purpose of the Act indicates, the Act is structured to ensure that minors are protected from harmful platform features while still "obtain[ing] all the core benefits of social media."[4] In passing the Act, the Legislature thus struck a careful balance between shielding covered minors from harmful features and allowing them to continue to generally access online platforms. The final rule simply implements the Act.

Accordingly, OAG makes no changes in response to these comments.

Theme: Some comments recommended the final rule institute public education campaigns to increase media and digital literacy among covered minors and parents in lieu of requiring age assurance and parental consent to access addictive feeds and nighttime notifications.

A few comments proposed replacing the age assurance and parental consent requirements with various forms of media and digital literacy.[5] For example, they suggested classes in schools to teach minors how to safely browse the internet and avoid "inappropriate" websites and apps, and a public awareness campaign about existing parental control tools on platforms. In support of these proposals, one comment asserted without evidence that media and digital literacy education would be more effective at protecting minors than the Act's current requirements while posing fewer privacy risks.

As an initial matter, G.B.L. §§ 1501 and 1502 unambiguously require a covered operator to conduct age assurance and obtain verifiable parental consent before allowing a covered minor to access an addictive feed or nighttime notifications. Wholly replacing these requirements is beyond the scope of the final rule.

Moreover, the Legislature has determined that the Act, rather than the alternative proposals, are appropriate to effectively address the harms identified. As discussed in Parts II.B.1 and II.B.2 of the NPRM, the "addictive" quality of addictive feeds and nighttime notifications is unrelated to the subject matter or nature of the content in a feed. Consequently, lessons on identifying inappropriate content would be insufficient in reducing the harmful effects of these features. Additionally, awareness campaigns about parental controls require the availability of accessible and effective controls. Both parents and covered minors have observed

[3] Footnote 23 of the NPRM also discusses this issue.
[4] Stop Addictive Feeds Exploitation (SAFE) for Kids act, § 2 (Legislative Intent), enacting Article 45, §§ 1500-08, of the General Business Law (signed Chap. 120, June 20, 2024).
[5] Another commenter objected to section 700.3 of the rule as introducing a prohibition on nighttime notifications absent age assurance and verifiable parental consent, citing concerns about user privacy. This prohibition originates in the Act.

that many online platforms do not offer the types of controls or settings that let them effectively reduce the covered minor's exposure to these features.[6]

Finally, no comment has provided evidence demonstrating that media and digital literacy lessons effectively counteract the effect of addictive feeds and nighttime notifications on covered minors. As discussed in Part II.B.2 of the NPRM, ample evidence points the other way. A covered minor's brain is still maturing, including with respect to their capacity to properly utilize knowledge and make well-reasoned, informed decisions. Addictive feeds and nighttime notifications undermine the covered minor's ability to control their behavior, even if they know better.[7] Media and digital literacy lessons for the covered minor thus seem unlikely to be effective. As for parents, media and digital literacy lessons by themselves do not ensure that the parent has the chance to discuss risks and benefits with the covered minor before the covered minor accesses one of these features.

Accordingly, OAG makes no changes in response to these comments.

II. Comments addressing OAG's statement of the purpose, needs and benefits of the rule in the Regulatory Impact Statement published in the NPRM

This Part II of the Assessment of Public Comment addresses substantial and material issues raised by commenters in response to the provisions of the proposed rule. The OAG carefully reviewed and considered every comment submitted. Where commenters raised multiple distinct issues, the sections are further organized by theme. Where appropriate, comments regarding particular provisions are combined and addressed together.

A. Addictive Feed, Addictive Online Platform, Information Persistently Associated and Technical Information

Coverage of online platforms does not hinge solely on the definitions of addictive feed and addictive online platform. Under the proposed rule, not all online platforms with 20% or more of monthly active user time spent on addictive feeds are covered. Specifically, an online platform that serves fewer than 20,000 minors in the State of New York or that has fewer than 5 million global monthly active users is excluded from coverage as an exempt addictive online platform as defined in section 700.1(q).[8] Together, these definitions ensure that coverage is

[6] Multiple commenters identifying themselves as parents complained about this issue, while Part II.B.2 of the NPRM further discusses surveys of covered minors voicing the same concerns.

[7] One commenter cited an analogous study demonstrating that digital literacy lessons did not help minors to make better decisions regarding online ads. Jennifer L. Harris et al., EVIDENCE-BASED RECOMMENDATIONS TO MITIGATE HARMS FROM DIGITAL FOOD MARKETING TO CHILDREN AGES 2–17, 45 (2024), https://healthyeatingresearch.org/wp-content/uploads/2024/10/HER-Digital-Marketing-Report-2024.pdf. While the lessons helped minors to identify an ad as an ad, it did better equip minors to act on that knowledge, and did not reduce the influence of ads on minors' attitudes or desire for products shown in the ads.

[8] *See* sections 700.2(c), 700.3(c) of the rule.

tailored to those platforms that cause the harms the Legislature intended to target with the SAFE for Kids Act.

The OAG addresses all issues raised in the comments on these definitions and, after careful review and consideration, finalizes the definitions as proposed.

1. Addictive Feed: Section 700.1(c)

Theme: Commenters argued the definition of addictive feed must be more expansive to remedy the mental health harms caused by excessive social media use by minors.

One or more commenter asserted that the Act will be ineffective because it allows searches and feeds based on media a minor user follows or otherwise requests. They also asserted the Act will not effectively reduce excessive social media use because it does not limit the content minors will encounter. The OAG disagrees. As detailed in the legislative history, and in Part II of the NPRM, and as determined by the Legislature, algorithms based on data mined and gathered about a user are responsible for excessive use and lead to mental health harms in minors. Evidence does not support the same conclusion for searches and feeds composed of requested media.

Theme: Commenters requested exclusions from coverage based on various justifications.

Some commenters suggested exclusions from coverage arguing certain types of feeds are a limited component of online platforms. These commenters referenced the use of a feed that may meet the definition of an addictive feed but that they described as a supportive or ancillary component of the online platform. For example, some commenters suggested that a comment section could be set up as an addictive feed and that platforms should be excluded from coverage based solely on such a feed where it is a supportive component of the platform. Others argued for content- or industry-based exclusions. First, G.B.L. § 1500 defines both "addictive feed" and "addictive social media platform" without such exclusions; the rule is consistent with those statutory definitions. Additionally, the Act addresses feeds that are merely supportive components in the definition of "addictive social media platform" in that it only includes those online platforms for which an addictive feed is a significant part of the online platform. The final rule provides brightline guidance, as noted in Part III.A.4 of the NPRM, to confirm that only those platforms for which addictive feeds comprise 20 percent or more of time spent on the platform by monthly active users are covered. No platform using such a feed as a supportive component commented or offered evidence that a supportive element, like a comment section if set up as an addictive feed, would comprise such a high percentage of total user time on the platform.

Subtheme: Exclude navigational aspects such as home screens, menus, and search pages from "addictive feed"

One commenter suggested the definition of addictive feed should exclude navigational aspects of an online platform as those are not designed to maximize user time spent. The

definition of addictive online platform in section 700.1(d) requires that an addictive feed is a significant part of the platform. To be a significant part of an online platform, 20 percent or more of time spent on the platform by monthly active users must be spent on addictive feeds. Thus, a platform that uses an algorithm based on personal information about a user and a user's behavior for navigational aspects alone likely would not be covered; no platform stated it would be captured under this standard.

Another commenter suggested that changing the definition of addictive feed in section 700.1(c)(1) from media "shared or generated by users" to "shared and generated" by users would helpfully limit the definition of addictive feed to exclude platforms whose user-generated content consists only of comment sections and reviews. First, such a change would be inconsistent with G.B.L. § 1500(1), which specifically defines addictive feed to include "media shared or generated by users." Moreover, a comment or review section is not an addictive feed simply because it includes user-generated content or is presented in a particular order by an operator. An addictive feed requires personalization and while comments or reviews may reflect an order, such as most recent or most popular, the order would not be an addictive feed unless it were individualized to the user's profile or user data. Second, no online platform for which comments or reviews are the only user-generated or -shared data stated that they personalize the order of comments or reviews and more than 20 percent of their users' time is spent on feeds of comments and reviews. Finally, this change would not eliminate coverage of comment or review feeds because the media in question, namely the comments or reviews, in a user comment or review feed would usually be shared and generated by users.

Subtheme: Exclude certain types of feeds or platforms entirely

A number of commenters suggested industry or content-specific exclusions from the definition of addictive feed. Some commenters argued that online commercial transactions should explicitly be excluded, including the use of personalization for recommendations in e-commerce. Other commenters suggested educational platforms and content as well as workplace, health and wellness, and productivity-oriented content be excluded. Commenters argued that these types of platforms are not responsible for the mental health harms at issue.

As noted, G.B.L. § 1500(1) does not include content-based exclusions and the final rule does not add such exclusions. At the same time, consistent with the Legislature's directive, the rule carefully tailors the definition of addictive online platform to ensure only those platforms for which addictive feeds are a significant part of user time are required to comply with the law. Additionally, the rule's exclusion of platforms in sections 700.2(c) and 700.3(c) that have fewer than 20,000 minors in New York further tailors coverage to exclude certain platforms that are less likely to cause the mental health harms the Legislature targeted with the Act. Thus, the rule is unlikely to capture e-commerce, health and wellness, or workplace and productivity-oriented platforms that are limited both in the extent to which they use addictive feeds and tend to be more targeted to adult use.

Some commenters argued that platforms or content termed educational should be excluded from coverage. The OAG disagrees. A feed is an addictive feed only if it concerns a user's interactions with media generated or shared by other users—as opposed to media generated by the operator or platform. Educational platforms likely would not rely significantly on media generated by users. Additionally, as noted, the rule covers only those platforms in which addictive feeds are a significant part. Evidence of the harm caused by addictive feeds is abundant and commenters provided no evidence that addictive feeds as a significant part of platforms self-identified as educational would be different.

Theme: Commenters sought clarification on whether certain types of personalization by online platforms meet the definition of addictive feed.

One or more commenter suggested that section 700.1(c)(3) is not clear about whether "liking" media is akin to a user request or subscription, and thus, an allowable form of personalization that would not constitute an addictive feed. Another argued section 700.1(c)(2)(ii) prohibits personalization that is allowable as user-directed personalization under the Act. The OAG disagrees with both contentions.

First, "liking" or otherwise interacting with a piece of media cannot be interpreted as an "express and unambiguous user request[]" or a subscription to the media posted by a particular author, creator, or poster.[9] Thus, the use of such data would fall under the definition of addictive feed. Second, the rule hews closely to the statutory language and does not expand the definition of addictive feed. The commenter asserted that the Act includes a general exclusion for user-initiated content, which the commenter conflates with personalization based on a user's previous interactions. In fact, the rule borrows from G.B.L. §§ 1500(1)(c) & (d), which exclude media "the user expressly and unambiguously requested" from the definition of addictive feed.

Theme: Commenters sought clarity regarding whether operators may exclude harmful content and may apply trust, safety, and accessibility tools as part of their content moderation of feeds.

The OAG agrees with commenters that neither the Act nor the rule prevents operators from implementing trust, safety, and accessibility tools or from modifying the media a user receives to ensure they do not receive harmful or inappropriate content. The OAG thus modifies the rule by adding section 700.9(e) to incorporate G.B.L. § 1501(7), which states, "Nothing in this section shall be construed as preventing any action taken in good faith to restrict access to or availability of media that the covered operator considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected."

[9] *See* section 700.1(c)(3)(ii),(iv) of the rule.

2. Information Persistently Associated: Section 700.1(u)

Theme: One commenter suggested the definition of "information persistently associated" be modified to exclude certain types of "transient" data.

One comment proposed modifying the definition of "information persistently associated" in proposed section 700.1(u) to expressly exclude certain types of data that the comment described as "transient" in nature. The comment further proposed defining such data types by the purpose for which they are retained, with retention for "behavioral profiles" used in "content selection" being prohibited while retention for other purposes such as "functionality, analytics, or personalization" being permitted.

G.B.L. § 1500(1)(a) and its implementing provision of the rule, section 700.1(c), exclude from the definition of an "addictive feed" any instances where media is "recommended, selected, or prioritized for display" based on information that is not "persistently associated with the user or the user's device." As explained in Part III.A.21 of the NPRM, section 700.1(u) further clarifies the phrase "information…persistently associated" within this provision.

As proposed, section 700.1(u) contains a clear distinction between information that is "persistently" associated and information that is not "persistently" associated. The rule directs a covered operator to consider whether the association persists over time and in connection with a specific user or user's device. This definition captures the meaning of "persistent" while remaining flexible in anticipation of future technological developments that might be used to associate information with a user or a user's device. The comment categorizes certain data types as "transient" but then proposes allowing a covered operator to retain data depending on how the covered operator plans to use it—including if the operator plans to use it for personalization, which the commenter does not define. The OAG is not convinced, and the comment does not provide any explanation or evidence of how, an operator can guarantee that a given data type will always be "transient" and cannot be stored in some way. Nor does it explain why certain purposes should be permissible; for example, it does not differentiate between the "routine" personalization it proposes to allow and media selection that is clearly prohibited by the Act.

Instead, many of the commenter's concerns are addressed by section 700.1(u) as originally proposed. As noted in Part III.A.21 of the NPRM, a one-time, temporary use of an identifier does not qualify as "information persistently associated" with a user or a user's device. The NPRM provides several examples of one-time, temporary use of identifiers for content delivery (a type of "functionality") and changing link color after a user clicks on it (a type of temporary "personalization"). None of these examples would render a feed an "addictive feed" within the meaning of the Act and rule.

Accordingly, OAG makes no changes in response to this comment.

3. Technical Information Concerning a User's Device: Section 700.1(ff)

Theme: Commenters stated the definition of "technical information concerning a user's device" should explicitly address geolocation data.

Two comments suggested that section 700.1(ff) of the proposed rule be modified to expressly limit or prohibit geolocation data from qualifying as "technical information concerning a user's device." Both expressed concerns that a covered operator could use geolocation data to provide a covered minor with access to an "addictive feed" or "nighttime notifications" without obtaining verifiable parental consent.

G.B.L. § 1500(1)(b) excludes from the definition of "addictive feed" any instance where a covered operator recommends, selects, or prioritizes media based on "technical information concerning a user's device." Section 700.1(ff) further clarifies this phrase by outlining three prohibitions that prevent information from qualifying as "technical information concerning a user's device," including a prohibition against including "information linked, directly or indirectly, to the user's previous interactions with media generated or shared by other users" and a prohibition against "otherwise process[ing the information] for the purpose of providing an addictive feed or nighttime notifications."[10] These prohibitions apply equally to all data types, geolocation included. Thus, section 700.1(ff)(3) of the rule already prohibits the use of geolocation data to provide an addictive feed or nighttime notifications.[11]

Part III.A.21 of the NPRM discusses several examples of instances where a covered operator may recommend, select, or prioritize media based on "technical information concerning a user's device" that benefit a user and that would be excluded by the comments' proposal. For example, if a covered operator uses general geolocation data to apply policies based on New York laws, such as the Child Data Protection Act[12], that would be permitted pursuant to section 700.1(ff). Preventing a covered operator from doing so does not advance the goals of the Act and may interfere with the operation of other laws.

Accordingly, OAG makes no changes in response to these comments.

---

[10] One comment also expressed concern that geolocation data can be highly sensitive as it has the potential to identify an individual, or to at least pinpoint their location. The third prohibition in section 700.1(ff) expressly states that technical information "is not information linked to a user's identity." The OAG reiterates its caution to covered operators to carefully consider whether geolocation data is "linked" to the user's identity as outlined in Part III.A.31 of the NPRM. For the sake of clarity, if geolocation data identifies an individual or pinpoints their location to the degree that it is "linked" to a user's identity, then it is prohibited from qualifying as "technical information concerning a user's device" under section 700.1(ff)(1) of the rule. And regardless of whether the covered operator wishes to treat geolocation data as "technical information concerning a user's device," if the data is collected in connection with the covered operator's compliance with the Act, it is subject to the data protection safeguards in section 700.7 of the rule.

[11] The use of geolocation to determine whether a user is a covered user is separately addressed by sections 700.2(d)(1) and 700.3(d)(1), as discussed at Part D.13.

[12] *See* G.B.L. § 899-ll (defining scope of CDPA based on location of relevant conduct). Adopting the suggestion of one comment to limit the use of geolocation data to only compliance with the Act may undercut the ability of a covered operator to comply with not only the CDPA but also many other New York laws intended to protect minors, such as gambling laws.

4. Addictive Online Platform: Section 700.1(d)

Commenters generally agreed with OAG's proposal to determine whether an addictive feed is a significant part of an operator's platform based on time spent on the feed, citing the relationship of time spent to the harms the Legislature targets through the Act. One large platform emphasized its support in its comment, noting that time spent on the addictive feed is the best way to gauge which platforms are most likely to be addictive and, at the same time, allow minor users access to personalized feeds that are helpful and useful.

Theme: Commenters argued for exclusions and changes to the definition of addictive online platform, including the standard for determining whether an addictive feed is a significant part of an online platform.

Some commenters argued for a risk-based approach to determining whether an addictive feed is a significant part, recommending consideration of other factors, such as the audience composition, the design and purpose of the feed, whether the feed is the primary purpose or functionality of the platform, and the presence of other engagement-driving features, such as autoplay, streaks, or infinite scroll. The OAG does not believe that an entirely risk-based approach to coverage is practicable or that it would best serve the goals of the Act. At the same time, the Act and rule as a whole account for important factors without relying solely on a factor-based test.

The rule considers audience composition by exempting platforms that serve fewer than 20,000 minors in the State of New York. The definition of addictive feed accounts for the design of the feed, ensuring that only those feeds based either on information persistently associated with a user or a user's interaction with user-generated media are captured. As described in Part III.A.3 of the NPRM, the definition also includes several conditions, generally based on a user's affirmative actions, under which delivery of media is not an addictive feed even if it might otherwise meet the definition. The use of primary purpose as a factor to determine whether an addictive feed is a significant part of a platform would not adequately serve the intent of the Act. An operator may have a multifaceted platform with multiple purposes, each of which could be equally central to the platform while still including an addictive feed that leads to harms the Act seeks to address. Finally, while other engagement factors may also drive excessive engagement, the law targets addictive feeds based on evidence of their capacity to boost such excessive engagement and the resulting harm they cause.

As explained in Part III.A.4 of the NPRM, the Legislature allowed for "online services that provide such feeds as ancillary features or add-ons, or where users are on the feed for a relatively small portion of their time using the service" through its definition of addictive online platform.[13] At least one commenter argued that any presence of an addictive feed on an online

[13] NPRM at 36.

platform should trigger the protections of the Act because addictive feeds are so harmful. This, however, would not be consistent with the definition of addictive online platform.

Other commenters asserted that 20 percent of monthly active user time is arbitrarily low and would include platforms in which addictive feeds result in only ancillary or add-on engagement. Some suggested higher thresholds, with 50% of user time being the highest. The OAG disagrees. In devising the proposed rule, OAG considered the definition of "significant" as well as the Legislature's stated intent. The OAG searched publicly available information and specifically sought data and information regarding the 20 percent monthly active user threshold in Part III.A.4 of the NPRM, including whether the threshold would lead to coverage of platforms that are not responsible for the harms caused by addictive feeds. No commenter provided data or specific information to counter the proposal.

Taken together with exclusions for platforms with fewer than 20,000 minor users in New York State and for those with fewer than 5 million global users, OAG finds that 20 percent or more of monthly active user time appropriately targets platforms that risk the harms the Act intends to prevent. Notably, a standard under which an online platform would be covered only if the monthly active user time on an addictive feed is 50% or more would be less effective in mitigating the intended harms with no specific benefit articulated by commenters except that it would cover fewer platforms.

Commenters sought clarification about what would count as time on the feed and argued that certain types of content, even if part of an addictive feed, should not be included. While some commenters argued time spent watching or reading media in a feed is part of time spent on a feed, others argued "passive video clicks" and "likes" should not be included. To clarify, time spent on the feed includes all of the time a user dwells on a feed, whether to watch a video, read a post, or otherwise remark on media in the feed. The Act is concerned with how an addictive feed serves media to users in a manner that drives excessive user time and engagement. The Act and the rule are agnostic to the substance of the media; it is the nature of the engagement and time on the feed that cause mental health harms, as the Legislature found and as is supported by scientific evidence. Time spent on the feed does not, however, include a user's decision to click out of the feed into a different part of the same or different site. At the same time, operators cannot exclude time spent viewing media displayed on a feed where the user remains on the feed once they have completed or left the individual piece of media.

Commenters also argued that minors will migrate from online platforms that meet the 20% threshold and do not allow minors access to addictive feeds to platforms with addictive feeds that make up a smaller percentage of monthly active user time (and, thus, would allow minors access to addictive feeds without parental consent). The Act only requires compliance for those platforms for which the addictive feed is a significant part. This is a feature of the Act that balances the ability of operators to use addictive feeds as an incidental part of their platform with the need to protect minors from harmful excessive use due to addictive feeds. Moreover, to the extent this distinction leads to a significant migration of minors to an addictive

feed, the time spent on the addictive feed will increase, potentially to the point where the platform will be covered by the Act and its implementing rules.

Theme: The measurement of time spent on addictive feeds.

A few commenters argued that the rule created a rolling obligation to continually calculate whether monthly active users spend more than 20% or more of time on addictive feeds over the last six months. This is a misunderstanding of section 700.1(d), which says the monthly active user time can be "measured over any six-month period in the prior calendar year." No commenter argued that compliance with the rule as intended, whereby an online platform may choose any six-month period in the prior calendar year to determine whether it is a covered platform, is not feasible.

Part III.A.4 of the NPRM specifically states, "[a]s it is not clear that a particular six-month period would be more representative than another, OAG allows covered operators the flexibility to choose a six-month period in the prior calendar year."[14] However, OAG understands that the language might also be interpreted to require a rolling calculation. Accordingly, the rule as finalized is modified to clarify that time on addictive feeds may be "measured over any <u>one</u> six-month period <u>an online platform chooses to measure</u> in the prior calendar year" (additions to proposed rule underlined).

One or more commenters argued that smaller platforms composed of an addictive feed together with other components or pages that are not an addictive feed may not measure time spent on the different components of their platform. As an initial matter, time spent on different components of an online platform is an important metric for operators, and as described in Part IV.A of the NPRM, is often the way operators monetize online platforms, and is something online platforms can readily measure. Additionally, as explained herein and in Part IV.C.3 of the NPRM, the rule is clear that certain platforms are exempt based on their number of users or minor users under sections 700.2(c) and 700.3(c) of the rule. Accordingly, the OAG concludes it is reasonable for covered platforms to measure time spent on addictive feeds on their platforms and confirm whether they are covered platforms to the extent they are not exempt platforms.

Theme: Commenters questioned the terminology in the rule as inappropriate or exceeding OAG's authority.

Some commenters objected to the use of the term "addictive" in reference to the use of personalized feeds, arguing the term addictive has a specific meaning in medicine that does not apply to personalized feeds. The term "addictive" is used in the Act. While recognizing courts may interpret the Act and rule based on canons of statutory interpretation, neither the Legislature nor OAG must ascribe to the technical or medical meaning of a word.

[14] NPRM at 37.

Others argue that the definition of the term "addictive online platform" exceeds OAG's authority because the Act uses the term "addictive social media platform." With respect to OAG's authority to define the term "addictive online platform," while OAG is limited to the parameters and authority granted by the Legislature, that authority is based on statutory provisions that outline such authority themselves, and not the terms that are defined. The definition of addictive online platform in the proposed rule is consistent with the definition of addictive social media platform in the Act. The rule defines online platform, which is not defined in the Act, to simplify references to the different types of technology in which addictive feeds exist. The use of addictive online platform in the rule creates consistency among the terms. Accordingly, OAG makes no modifications based on these comments.

Theme: One commenter contended the definition of addictive online platform should exclude any platform on which a user spends 30 minutes a day or less.

One commenter suggested the definition of addictive online platform should exclude any platform on which a user spends 30 minutes a day or less. It is axiomatic that every online platform will have some users that spend less than 30 minutes per day or less on a platform. That some users may not engage in excessive use is not a reason to exempt the platform from the Act, nor does the statute provide a basis for such a distinction. Consistent with the statutory definition, OAG defines addictive online platform based on the significance of an addictive feed to a platform across all users.

B. Exempt Online Platform and Monthly Active User

1. Exempt Online Platform: Section 700.1(q)

Theme: Commenters argued for changes to the definition of exempt online platform.

A small number of comments addressed the definition of exempt online platform. For the reasons that follow, the definition is adopted as proposed.

One comment expressed concern that operators, particularly platforms that are small or early-stage, may not devote the resources necessary to determining whether their user base contains 5 million users or 20,000 covered minors and instead may simply assume that the rule does not apply, possibly even ignoring evidence to the contrary. This concern, while not entirely unfounded, does not necessitate a change to the proposed rule. Operators with users in New York State are obligated under the rule to conduct the requisite diligence to understand whether they qualify as exempt online platforms if their online platform includes an addictive feed as a significant part of its service and they do not wish to comply with the Act's requirements. If an operator incorrectly takes the position that the exemption applies without having sufficient basis to do so, that operator will be liable for any addictive feeds or nighttime notifications served to minor users. Further, as discussed in Part IV.A of the NPRM, online platforms that use addictive feeds as a significant part of their service generally measure their

growth and success by the number of active users, and often generate revenue through marketing based on the demographics of their platform.

Another comment expressed concern that the term "primary user base" is vague and may encourage platforms to construe the term in a self-serving manner, to avoid compliance. The comment did not suggest a definition for "primary user base" or an alternative term that could be used instead. The term "primary" is commonly understood to mean principal or first. This can refer to the population of users on a platform or the target platform audience. Whether the users of a platform are predominantly minors, or whether the intended principal audience of the platform is minors, should be known to any platform, even one that is newly created. Online platforms with addictive feeds as a significant part of their service by definition rely to a significant extent on user-generated content. Thus, they are likely to be planning for and tracking their intended and actual audiences. The OAG therefore declines to further define "primary user base."

Other comments asked OAG to require platforms qualifying as exempt online platforms to turn off addictive feeds where the platform knows or should know that a user is a minor, limiting the scope of the exemption to the age assurance requirement only. Following thorough consideration, OAG declines to adopt this request. The proposed rule exempts platforms qualifying as exempt online platforms from all requirements in sections 700.2(c) and 700.3(c), until such time as the exemption no longer applies. As explained in Part III.B.2 of the NPRM, the purpose of the exemption is to protect small or early-stage platforms from competitive harm while they are in a phase of development in which their platforms may not yet be yielding any profit or even any revenue at all. Requiring these platforms to apply an actual knowledge or "should know" standard for the age status of their users imposes obligations on the platforms that are inconsistent with the minimization of competitive harm that underlies the exemption. As explained in Part III.B.2 of the NPRM, the negative impact of the exemption is limited by the maximum of 20,000 covered minors and the "primary user base" carveout in the definition. Insofar as only small platforms with relatively few covered minors and a primary user base of adults are eligible to be exempt online platforms, the benefit of creating an alternative "know or should know" standard for these platforms does not outweigh the economic drawbacks.

Finally, one comment asked OAG to clarify that a covered operator reaching the 5 million-user limit may not avoid compliance by re-assuming exempt status in the event the covered operator then measures fewer than 5 million global monthly active users during the 180-day grace period. In the event a covered operator were to maintain a monthly active user base that fluctuates just above and below 5 million, this would create a compliance loophole, according to the comment. Sections 700.2(c) and 700.3(c) specify that a covered operator reaching 5 million global monthly active users has 180 days to come into compliance "from the first such instance;" thereafter, should the covered operator measure fewer than 5 million global monthly active users, it would no longer be required to comply until such time as it once again measured 5 million monthly active users, at which time it would have 30 additional days

to resume compliance. Whether or not the covered operator chooses to take advantage of the initial 180-day period to comply with the rule, that 180-day period is available for one time only; even if the covered operator resumes exempt status during the 180-day period, any future period to come into compliance will last only 30 days. Covered operators that are close to exceeding the 5 million global monthly active user-threshold at any time should plan accordingly.

While not expressly directed to the exempt online platform definition, a small number of comments expressed concern regarding the economic impact of the rule on small businesses. By including an exemption for covered operators with fewer than 5 million global monthly active users or 20,000 monthly active users who are covered minors, OAG intended to protect small businesses while still protecting minors and serving the legislative purpose of the Act. An explanation of these limits and their basis is set forth in Part III.B.2 and the economic analysis in Part IV.C.3 of the NPRM, which quantifies the impact to platforms of adopting commercially reasonable age assurance.

2. Monthly active user: Section 700.1(y)

The OAG received a small number of comments addressing the definition of monthly active user, from members of industry or groups representing industry perspectives. Some commenters argued that one minute is too insignificant to qualify a user as active. Others raised concerns about double-counting users logging on from different devices or using an online platform as both a "logged in" and "logged out" user. Others asked that not all types of user engagement be counted towards the one-minute threshold.

The monthly active user definition provides a measure for an operator to evaluate which platform users should be included in the monthly active user totals – specifically, any individual that visits an operator's platform and remains for at least one minute. The categorization of users as monthly active users enables operators to reach a conclusion as to whether the platform qualifies as an "addictive online platform" based on the amount of time the monthly active users spend on the operator's addictive feed versus other parts of the platform, and also allows covered operators to determine whether they meet the definition of exempt online platform, based upon having fewer than 5 million global monthly active users or 20,000 monthly active users who are covered minors. Following careful consideration of the comments addressing the monthly active user definition, the OAG adopts the definition as proposed but with one modification, for the reasons described below.

Theme: Commenters sought more flexibility and suggested alternative ways to define monthly active user.

A few commenters posited that the proposed monthly active user definition is not consistent with industry standards. These comments did not identify any alternative measure that constitutes an industry standard, nor did they recommend any particular standard to be used in the rule; instead, they recommended that platforms be afforded "flexibility" in

determining their own monthly active user definition. The OAG recognizes that variation exists in platforms' calculations of their user traffic; the proposed rule offered several examples of disparate standards used by various platforms,[15] and acknowledged in Part III.A.25 of the NPRM that platforms vary in reporting daily, weekly, or monthly users, among other differences in measurement. As stated in Part III.A.25 of the NPRM, the intent of the monthly active user definition is to be "as inclusive as or more inclusive than the majority of platforms when counting users." One commenter recognized this and expressed appreciation for OAG's effort to set a uniform standard that is inclusive of different approaches.

The OAG established a set standard to ensure fairness and consistency in both the implementation and enforcement of the rule. Allowing flexibility in the measurement of monthly active users could lead to platforms establishing standards that create inconsistent outcomes as to the application of the rule and its exemptions, and the adoption of a less stringent standard by some platforms could undermine the intent of the Legislature in seeking to protect minors using addictive online platforms. The OAG thus rejects the suggestion that it adopt a flexible standard to determine whether a user is a monthly active user.

A few commenters also suggested that low-quality user traffic be omitted from the definition of monthly active user. Insofar as "low-quality" traffic includes incidental or accidental visits lasting less than one minute or traffic driven by non-human users, both are already excluded under the current construction of the proposed rule. The OAG assumes that users visiting an operator's platform for less than one minute might not constitute intentional or "high-quality" user traffic and so omitted those visits from the monthly active user definition. And the definition applies only to "individuals," i.e., natural persons, meaning that any user traffic that can clearly be established as non-human must be excluded. Following consideration, OAG declines to further differentiate types of user engagement in the definition of monthly active user.

Finally, a few commenters expressed concerns regarding the counting of users and efforts to de-duplicate those counts. One commenter asked that OAG amend the definition to specify that only users logged in to a platform be included as potential monthly active users. The commenter expressed concern that including logged-out users might result in double-counting of users who are visiting the platform multiple times in a logged-out state or on different devices. Insofar as a platform is defined as an addictive online platform only if more than 20% of monthly active user time on the platform is spent on an addictive feed, should a platform decline to offer an addictive feed to logged-out users, counting those logged-out users in the definition of monthly active user is not consistent with the intent of the rule. Accordingly, the OAG will modify the definition of monthly active user to state that a monthly active user "accesses an online platform <u>in a manner that includes access to an addictive feed</u> and remains on the online platform for at least one minute" (new language underlined). Under this amended

[15] *See* NPRM at 37 n.53

definition, should an operator choose to offer addictive feeds to logged-out users, those users should be counted as monthly active users along with logged-in users.

Other commenters expressed general concern about the efforts required to de-duplicate users that are both logged in and logged out, or users that are logged in via multiple accounts or devices. As an initial matter, operators that clearly qualify as addictive online platforms and do not meet the exempt online platform definition do not need to keep an active count of monthly active users for purposes of determining whether the requirements of the rule apply. If an operator seeks to demonstrate that it does not meet the definition of addictive online platform, or qualifies as an exempt online platform, it will be incumbent upon the operator in counting monthly active users to minimize duplicative counting of users to the extent possible using data in its possession. That data is subject to all of the requirements in section 700.7 of the rule. Operators are not required to collect additional data for this purpose.

C. Nighttime Notifications

Theme: Commenters recommended expanding the definition of nighttime notifications to include more notifications.

Several commenters suggested expanding the proposed definition of nighttime notifications in section 700.1(z) of the rule, such as by expanding the time window or by removing the qualifier "concerning an addictive feed." Section 700.1(z) simply implements G.B.L. § 1502, which sets forth a prohibition on notifications "concerning an addictive feed" that occur "between the hours of 12 AM Eastern and 6 AM Eastern."

Accordingly, OAG makes no changes in response to these comments.

Theme: One commenter suggested the final rule include a separate definition for "notification."

One comment expressed concern that the term "notification" was unclear and suggested defining it separately from section 700.1(z). This comment provided examples of different types of notifications based on the platform's method of delivery. Other comments from organizations representing online platforms likely covered by the Act did not raise the same potential difficulties with compliance, even when commenting on sections of the rule related to nighttime notifications.

Additionally, G.B.L. § 1502, which is implemented by section 700.1(z), specifies that a notification must be "concerning an addictive feed." This qualifier combined with the time limits also set out in G.B.L. § 1502 provides a covered operator with sufficient notice of the types of notifications within scope of the rule. Accordingly, OAG makes no changes in response to this comment.

Theme: A commenter sought to clarify whether notifications originally scheduled to arrive during the time window set out by section 700.1(z) can be rescheduled and delivered outside of the window.

One comment asked for the final rule to clarify whether a notification that would have been sent between 12 AM Eastern and 6 AM Eastern can be rescheduled by a covered operator to be sent at another time. Part III.A.26 of the NPRM provides several examples to explain that notifications falling outside of the parameters set out by section 700.1(z) are unaffected. Similarly, a rescheduled notification that is received by a covered minor outside of the 12 AM Eastern-6 AM Eastern time window falls outside of the scope of section 700.1(z).

Accordingly, OAG makes no changes in response to this comment.

Theme: A commenter sought to clarify that a notification about conduct that falls within one of the exemptions outlined in section 700.1(c)(3) also falls outside of the definition of "nighttime notification" in section 700.1(z).

One comment proposed that section 700.1(z) of the rule be modified to expressly exempt notifications related to conduct falling within section 700.1(c)(3), which outlines conduct that does not constitute an addictive feed. This comment incorrectly interprets the proposed section 700.1(z) as overriding section 700.1(c)(3). The OAG again clarifies that only notifications concerning an addictive feed are prohibited without parental consent.

Part III.A.26 of the NPRM provides guidance to covered operators as to how to read the nighttime notification definition together with the exceptions to "addictive feed" in section 700.1(c)(3). Along the same lines and by way of non-limiting example, a notification concerning a piece of content that the covered operator provides in response to a search query by the user is not a "nighttime notification" so long as it directs the user to that piece of content and does not direct the user to access an addictive feed.

Accordingly, OAG makes no changes in response to this comment.

D. Age assurance: definitions, requirements, commercial reasonability and technical feasibility

This section addresses all comments related to the definitions regarding age assurance as well as the requirements for conducting age assurance in the proposed rule. It is organized by sections and themes, which combine the definitions and requirements, for ease of discussion.

1. Methods

The OAG received comments regarding the categories of age assurance methods specified in the rule. For the reasons stated herein, OAG finalizes those categories as proposed.

Theme: Commenters suggested the rule further expand or limit operator choice.

Several commenters praised the rule's enablement of operator choice as to the age assurance method or methods the operator offers to covered users. Commenters noted that granting this level of flexibility to operators allows them to create a tailored experience for users and is consistent with commercial reasonability.

At least one commenter sought to expand the three enumerated age assurance categories – age verification, age estimation, and age assurance – by adding a fourth category consisting of any commercially reasonable method. However, no comment identified specific age assurance methods excluded by the proposed rules. The OAG declines to adopt this additional category. While OAG intentionally designed the three age assurance categories to encompass a broad range of age assurance methods, the three categories represent and are inclusive of all effective age assurance methods available today or in the foreseeable future. Allowing a fourth category consisting of every commercially reasonable method negates the existing classification of methods and risks allowing methods that are not effective.

One commenter recommended that OAG require operators to submit their age assurance plan to OAG for annual approval. The OAG declines to adopt this recommendation, both because the certification requirements obviate the need for OAG to review and approve and because the requirements in the rule make clear the necessary elements of a covered operator's age assurance plan.

Theme: Commenters expressed views on self-declaration of minor and adult status.

More than one commenter, including commenters representing operators, praised the flexibility afforded by the proposal in the rule to allow minors to self-declare their age, with one commenter favorably describing this proposal as an example of risk-based age assurance. Another commenter cautioned that self-declaration as a minor should only be allowed in instances where there is no risk of an adult pretending to be a minor for reasons that harm minor users' safety. As stated in Part III.A.30 of the NPRM nothing in the rule is intended to interfere with operators' trust and safety policies or compliance with other applicable laws, and nothing in the rule prohibits operators from requiring age assurance for reasons unrelated to the rule.

Some commenters praised the recognition in the rule that self-declaration of adult status without additional validation is ineffective and will not meet the applicable accuracy thresholds. While no commenter posited that self-declaration of adult status should be sufficient in all instances, a few commenters advocated for limited use of adult status self-declaration. Specifically, one comment asked that operators be allowed to rely upon pre-existing user self-declarations of adult status while employing effective age assurance for new users. As described in Part III.D.3.b and elsewhere in the NPRM, effective age assurance is a necessary part of shielding minors from the mental health harms of addictive feeds and nighttime notifications because self-declaration of adult status is not effective. A significant portion of

minors lie about their age to access covered platforms. Allowing for pre-existing user self-declarations as evidence of adult status would simply reinforce the status quo.

Another commenter suggested that operators with small populations of minors should be allowed to rely on self-declaration of adult status in conjunction with selective application of effective age assurance methods at the operator's discretion. The commenter did not suggest that self-declaration of adult status should be assumed to be effective. Moreover, consistent with the commenter's request, the definition of exempt online platform in the rule allows for operators with fewer than 20,000 covered minors to be exempt from its requirements. Once a platform exceeds this threshold, effective age assurance is an important protection for all minors on a platform.

Finally, one commenter argued that operators should not be obligated to perform effective age assurance on users formerly self-declaring minor status and subsequently representing that they have reached adult status, claiming that this process will add administrative burden for operators. Recognizing that the age of a user's account is one factor that may be considered in an age inference method, OAG concludes that allowing users who have previously self-declared as a minor to later self-declare as an adult without corroboration by additional age assurance methods creates a high risk of method circumvention through false information. The OAG thus adopts the rule as proposed, under which self-declaration of adult status is never by itself an acceptable method of age assurance.

Theme: Commenters asserted the lack of perfectly accurate age assurance methods undermines the rule.

Some commenters criticized the age assurance methods contemplated by the rule by pointing out that no available age assurance method has perfect accuracy or presents a perfect set of circumstances for every user. The OAG acknowledges that no age assurance method today can determine or predict user age status with perfect accuracy and the rule does not require perfect accuracy. In addition, OAG notes that this has been true throughout history, including for methods widely accepted for in-person age assurance such as human inspection of government-issued identification (which can be falsified) and visual inspection of a person's appearance (which can be misleading). While age assurance methods are not perfect, effective age assurance is consistent with the requirements of the Act and its statutory purpose: protecting minor users from the harms caused by addictive feeds and nighttime notifications. By contrast, the status quo, in which age assurance is nonexistent or ineffective, affords little if any protection.

One comment asked OAG to mandate that every covered operator offer at least two age assurance methods to covered users. While OAG also recognizes that no single age assurance method creates the ideal experience for every user, the rule's allowance of operator choice of methods enables operators to optimize the user experience for their user populations and platforms. Further, as emphasized in Part III.D.2.b of the NPRM, OAG strongly encourages user

choice of age assurance methods and age assurance waterfalls, in which the least invasive methods are utilized first, to minimize user burden. The OAG declines, however, to mandate that every covered operator provide two or more age assurance methods to its covered users and concludes that the existing framework provides the best balance of operator burden and flexibility with user choice, including by mandating multiple age assurance methods if one method consists of providing government-issued identification.

Theme: One commenter argued that "false positive" and "false negative" should be replaced with alternative terms.

One comment recommended that OAG replace the terms "false positive" and "false negative with the terms "false accept" and "false reject," throughout the rule. The OAG declines to do so. "False positive" and "false negative" are terms that are recognized both in the scientific community and in global age assurance guidance laws and guidance. As defined in the rule, the terms are part of the framework by which operators must limit the number of covered minors falsely identified as adults and must measure and consider the number of adults falsely identified as minors. The OAG finds no basis to substitute the terms "false accept" and "false reject," which are not as commonly used or understood.

2. Age Estimation: Section 700.1(i)

The OAG received comments concerning age estimation from a variety of stakeholders. Comments from providers of age assurance methods expressed support for the ability of commercially available age estimation methods to meet the rule's requirements. Other comments expressed concern regarding aspects of age estimation. After extensive consideration of age estimation as a category of age assurance, OAG adopts both the definition of age estimation and its inclusion as an acceptable category of age assurance, as set forth in the proposed rule.

Theme: Some commenters argued that age estimation raises data privacy and security concerns.

Some commenters raised concerns about the biometric data required to perform age estimation and its implications for user privacy and data security. In advance of proposing these rules, OAG performed extensive analysis on the impact of age assurance on data privacy, as discussed further herein in response to comments addressing data security and privacy. Based on this analysis, OAG concluded that commercially available age estimation products can readily provide effective age assurance while protecting user privacy by minimizing, securely transmitting and storing, and promptly deleting the user data underlying the determination of the user's age status. After carefully reviewing the comments, OAG finds that the arguments commenters raised do not alter its conclusion that age estimation, when completed consistent with the requirements of the rule, can be conducted securely and maintain user privacy. The rule (at section 700.7(a)) mandates these privacy-preserving practices with respect to the data

collected to perform age estimation. Additionally, the rule's testing and certification requirements are designed to confirm that age assurance providers meet existing state-of-the-art data security requirements.

The OAG also notes that facial age estimation methods are already widely used by social media platforms, as detailed in Part III.D.2.g.ii of the NPRM. In addition, while commenters focused on facial age estimation (which differs from facial recognition), age estimation technology continues to evolve to include methods relying on data other than an image of a user's face, such as age estimation based on hand gestures. This technological progress will likely lead to further enhancements to privacy and security.

Theme: Commenters asserted age assurance may lead to disparate outcomes for different users.

Some commenters cited reports that some age estimation products have returned inconsistent accuracy rates for users when measured by race and gender. The OAG acknowledges the potential for racial and gender disparities in age assurance methods and carefully considered alternatives for ensuring equity in the application of age assurance methods. Some of the reports cited by commenters reflect older data, which has been updated in recent months and years following advances in commercially available age assurance products. The studies available make clear that age estimation results vary by product and are influenced by factors such as the training data used by the individual provider. Method improvement also is anticipated as the technology continues to advance. Some methods today are highly accurate when tested across different races and genders.

It is incumbent upon operators to select and implement age assurance methods that comply with applicable law, including laws designed to protect against disparate treatment, such as Human Rights Law § 296. Testing schemes must, accordingly, be designed to reflect any disparities among groups that may implicate applicable legal protections. As stated in Part III.E.2.a of the NPRM, "Covered operators should pay particular attention to discrepancies in both false positive and false negative rates to determine whether the age assurance methods offered have a disproportionately large negative effect on a basis prohibited by applicable law or otherwise treat protected groups differently."[16]

Theme: A commenter suggested operators should be required to provide at least one alternative to age estimation.

One commenter asked that the requirement in proposed section 700.4(c)(3), that operators must provide an alternative method to government-issued identification, be extended to age estimation, citing user privacy as a primary concern. The rule as finalized allows operators the flexibility to provide users choice among multiple, compliant age assurance methods, which ultimately allows operators to respond to the interests and needs of their

[16] NPRM at 95.

users. The OAG declines to mandate that an alternative method be offered by every operator alongside facial age estimation based on its determination that facial age estimation that complies with the data security and privacy requirements of the rule sufficiently protects user privacy. The rule requires robust data deletion and data security requirements to maximize user privacy and also mandates an appeals process for users seeking to prove adult status through an alternative method. The OAG also reminds operators considering whether to offer facial age estimation as the sole age assurance method that they are obligated to ensure at least one age assurance method meets both the accuracy minimum and the total accuracy minimum for every user, as demonstrated through the testing and certification process, and to deploy age assurance methods using only the settings or options for which the method received certification.

3. Age inference: Section 700.1(j)

Some comments addressed age inference as an age assurance method. The comments from age assurance providers generally supported age inference, with no major issues raised. As discussed further below, a small number of individual and advocacy comments raised questions and expressed concern regarding age inference, including its privacy implications and the relationship between age inference methods and existing data held by operators. The OAG adopts both the definition of age inference and its inclusion as an acceptable category of age assurance, as set forth in the proposed rule, and provides further clarification on the use of age inference by operators, herein.

Theme: Some commenters stated age inference should not be an acceptable age assurance method because it is based on operator collection of user data.

A small number of comments expressed opposition to age inference as an acceptable age assurance method based on the commenters' characterization of the rule as endorsing or requiring operators to collect additional data on users' platform behavior to conduct age inference. The rule does not, however, require or encourage operators to seek out additional data on user behavior to conduct age inference.

After conducting analysis of age inference technology, OAG concluded that many operators are already in possession of extensive user data that could be applied to an age inference method. In many circumstances, operators monetize this data for marketing, including through inferences regarding user demographics. Under the rule, operators may use this data, which they have already collected for other purposes, to conduct age inference for at least some portion of their user population. The rule provides operators the flexibility to respond to the interests and needs of their users and age inference allows operators to meet their obligations while minimizing both user burden and the additional collection of data. Moreover, age inference conducted using existing data does not relieve operators of their obligation to comply with applicable law, including with respect to commercial use of user data and related notices and consents. This also includes compliance with the enhanced data privacy protections

of the Child Data Protection Act for minors, which are triggered where an operator has actual knowledge that a user is a minor.

One commenter expressed concern about financial data being used by operators in age inference models. Following extensive consideration, OAG declines to expressly prohibit financial data from being used as part of age inference. The OAG recognizes that financial data can be sensitive but concludes that such data is used by some age assurance providers already and that section 700.7 adequately addresses the use and treatment of sensitive user data that is already possessed by an operator.

Theme: Commenters asserted age inference may not be reliable or requires lower minimum accuracy thresholds to be viable.

A few commenters argued that age inference based on analysis of user behavior on a platform may not be a reliable age assurance method. The OAG notes that age inference based on user behavior has only recently been deployed by operators as an age assurance method and where operators are developing proprietary algorithms to conduct age inference, the reliability of the technology is not transparent to outside evaluators. As such, the testing and certification requirements in the rule are designed to ensure that only effective age inference methods are relied upon to comply with the Act. In accordance with those requirements, age inference can only be deployed by operators as a compliant age assurance method if its efficacy is demonstrated via third-party testing.

One comment from an operator sought lower accuracy minimums for age inference as applied to operators' existing users, stating that under the current state of age inference technology, the proposed accuracy minimums are unreasonable. A second comment recommended that OAG forego accuracy minimums for age inferences and instead approve age inference methods on a case-by-case basis, arguing that doing so would encourage operators to use existing data for age inference. No operator submitted testing data demonstrating the efficacy of age inference in support of this or any comment or otherwise offered any basis, much less a compelling basis, for a different, lower set of accuracy minimums for age inference. In light of the availability of other commercially reasonable age assurance methods that meet the accuracy minimums in the rule, OAG finds that the accuracy minimums as finalized can reasonably be met by operators to comply with the rule.[17] OAG declines to set a separate, lower set of accuracy minimums specific to age inference or an ad hoc approval system for age inference methods; doing so would not serve the Act's purpose of protecting minors from addictive feeds.

Notably, commenters also did not address the flexibility of the rule through which operators can use multiple age assurance methods, jointly to meet the total accuracy minimum.

[17] Operators not required to comply with the rule, as defined in "exempt online platform," include operators with fewer than 5 million monthly active users or fewer than 20,000 monthly active users who are covered minors. *See* section 700.1(q).

Specifically, even if an operator's age inference method cannot meet the accuracy minimum requirement as to the operator's entire user population, it can still be included alongside other age assurance methods in the operator's age assurance program. Because all age assurance methods used by an operator must meet the accuracy minimum but only one method must meet the total accuracy minimum, age inference may be used where it is demonstrated to have a level of accuracy that meets the accuracy minimum for a sub-group of users – for example, users whose age is estimated to be substantially above or below 18. For the remaining sub-group of users for which age inference cannot determine age status to the required true positive rate (i.e., users for which age inference yields an inconclusive result as defined by the rule), the operator can advance those users to an alternative age assurance method. This practice is an example of an age assurance waterfall as described in Part III.D.2.b of the NPRM.

Relatedly, the testing benchmark requirement in section 700.5(b)(7) need only demonstrate compliance for any sub-group of users for which the age assurance method meets the required level of accuracy. Age inference based on usage data, as a relatively new method used for age assurance (as opposed to marketing or other internal purposes by operators), has the potential to improve to the point that it can be employed for all or mostly all users; the testing requirements will demonstrate if and when the appropriate benchmarks can be achieved. In light of the minimal user burden required for age inference based on existing usage data, this method may be a preferred option and the rule allows for it to be an option as to any part of the user population for which the accuracy requirements can be achieved.

4. Age Verification: Section 700.1(k)

The OAG received comments addressing age verification from a small number of individuals and advocacy groups, expressing concerns regarding the associated privacy and security risks. For the reasons set forth below and in the NPRM, OAG adopts the definition of age verification, its inclusion as an acceptable category of age assurance, and the requirements associated with the use of government-issued identification set forth in section 700.4(c), as proposed.

Theme: Some commenters asserted allowing for the use of age verification raises privacy and security concerns.

Some commenters praised the requirement in both the Act and the rule that every operator must offer at least one method other than government-issued identification unless the government-issued ID method is part of a zero-knowledge proof age assurance method. Commenters expressed support for users' ability to decline to provide government-issued ID while still being able to undergo age assurance. Other commenters expressed ongoing concern for the privacy implications of any collection of government-issued ID. At least one commenter asked that government-issued ID be fully prohibited as an age assurance method. The OAG is not persuaded by these comments, which fail to acknowledge the reduction of privacy risk to users from the data minimization and deletion requirements together with the certification

requirement in the rule. In light of the fact that most age assurance methods rely on some form of sensitive data, OAG concludes that adopting and enforcing strong data minimization and deletion requirements in the rule as they pertain to all data collected for age assurance is a more effective way to protect user privacy than prohibiting the use of any single form of sensitive user data for age assurance.

Theme: One commenter stated that allowing for the use of age verification leads to disparate outcomes because of unequal access to government-issued ID.

One commenter objected to the inclusion of age verification via government-issued ID as an acceptable form of age assurance because certain vulnerable groups have less access to government-issued ID, including racial minorities, immigrants, and people with disabilities. Both the Act and the rule recognize that not every user possesses a government-issued ID. Accordingly, section 700.4(c)(3) requires that all operators offer at least one method that does not require government-issued ID, and section 700.4(c)(2) requires that any individual declining to show government-issued ID for any reason must have the option to transition to the appeals process. That process in turn must offer an option to confirm the user's age other than through government-issued ID per section 700.6(a)(1). These procedural requirements do not distinguish between those users who choose not to provide a government-issued ID and those who do not have one, ensuring that both will have an avenue for age assurance while permitting operators to use government-issued ID as one potential option.

Theme: One commenter argued age verification via payment methods such as credit cards or deposit accounts should not be allowed under the rule.

One commenter sought a prohibition on age verification via payment methods such as credit cards, noting concerns related to financial data privacy and unequal access to credit cards or other financial products among users. The OAG does not find these arguments persuasive and declines to categorically prohibit credit cards or other financial products as a method of age assurance.

Preliminarily, the rules reflect OAG's finding that where an age assurance method meets the accuracy minimum including the method circumvention requirement, is commercially reasonable for an operator, and complies with the data privacy standards in the rule, blanket prohibition of such a method will limit operator flexibility and will not serve the goals of the Act. Commenters have not presented compelling evidence or argument that any method that meets those requirements should be prohibited.

With respect to age verification via credit card, the data minimization and deletion requirements in the rule were designed to protect user privacy, including by requiring deletion of data, such as a user's credit card-related data, if collected for age assurance purposes, immediately following the completion of age assurance. In light of this requirement, an operator's decision to allow age verification via credit card should not result in a compromise of

users' financial data privacy. The OAG notes, however, that it is not clear age verification via credit card can meet all of the rule's robust accuracy and data security requirements in its current form.

With respect to users' access to credit cards, OAG reiterates the importance of user choice in an operator's age assurance program and notes that operators have the flexibility to design an age assurance program that meets the needs and preferences of their users. The OAG also notes that any user who does not successfully complete the age assurance process for any reason, is treated as a minor by the operator as a result, and disputes that minor status can utilize the appeals process, which affords the user an additional opportunity to demonstrate age status using information available to the user.

5. Zero-Knowledge Proof Age Assurance: Section 700.1(jj)

The OAG received comments regarding the definition and inclusion of zero-knowledge proof age assurance as an acceptable category of age assurance method. The OAG adopts the definition of zero-knowledge proof age assurance as proposed and responds to the comments below.

Several commenters expressed support for the inclusion of zero-knowledge proof age assurance and praised the category as among the most privacy-preserving of all age assurance methods. Other commenters cautioned that although zero-knowledge proof age assurance methods enable effective age assurance without collection of user data by operators, those methods may still involve data collection by a third-party and associated privacy and security risks. The OAG agrees with both points and notes that zero-knowledge proof age assurance methods must comply with the data minimization and deletion requirements in the rule. The OAG further notes that, as set forth in section 700.9(a), operators remain responsible for compliance with the rule where operators elect to engage or otherwise rely on a third-party.

Theme: One commenter suggested zero-knowledge proof age assurance should eventually be mandatory.

One commenter advocated for OAG to require, at such time as zero-knowledge proof age assurance methods are sufficiently commercially available, that all operators adopt them in lieu of other age assurance methods. The OAG declines to adopt this recommendation. The rule does not mandate any one age assurance method or category but rather provides operators with flexibility to design the optimal age assurance program for their platform and users in accordance with the rule's requirements. While zero-knowledge proof age assurance methods are already being adopted by some software platforms in accordance with global regulatory requirements, whether zero-knowledge proof age assurance is commercially reasonable and technically feasible for compliance with the rule at a current or future point in time may depend upon a variety of factors including factors specific to the operator, such as the operator's user interface.

As set forth in section 700.4(g), OAG expects operators to periodically evaluate the age assurance methods selected and to adjust those methods based upon the commercially reasonable options at the time. Criteria against which operators must evaluate their chosen methods include "accuracy, method circumvention, and user burden;" the extent to which user data privacy is placed at risk should be included in any analysis of user burden. It is entirely possible that in the foreseeable future, zero-knowledge proof age assurance will become the industry standard and operators should act accordingly in adopting those methods where they otherwise comply with the rule and are commercially feasible.

Theme: A commenter suggested the zero-knowledge proof method definition should be amended to add an express "double-blind" requirement.

One commenter sought a change to the definition of zero-knowledge proof age assurance, asking OAG to expressly state that only "double-blind" methods of zero-knowledge proof age assurance, in which no single third-party has identifying information regarding both the user and the platform the user is seeking to access, be allowed under section 700.4(c)(3). The proposed definition states that the method must allow an individual "to demonstrate age status using verified data without revealing additional information to the operator or any third-party beyond the validity of the individual's age status." As stated in this definition, the method must not allow any third-party facilitator to learn the identity of the operator making the request for confirmation of a user's age status as this would be "additional information" regarding the user. Similarly, the operator must not learn information about the user beyond the user's age status. In this manner, an allowable zero-knowledge proof age assurance method is maximally privacy-preserving. Because the proposed rule already specifies the parameters of allowable zero-knowledge proof age assurance and further describes these requirements in Part III.A.35 of the NPRM, OAG declines to amend the definition of zero-knowledge proof age assurance to further clarify its requirements.

6. Accuracy Minimum and Total Accuracy Minimum: Sections 700.1(b) and (gg)

The OAG received comments regarding the "accuracy minimum" definition as a measure of efficacy for an age assurance method. Some commenters, including from the age assurance industry, expressed support for the specificity of the allowable false positive rates and the proposed rule's approach to accuracy based on narrow age ranges, with more allowance of false positives for users whose actual age is closer to the target age of 18. Other commenters did not support the proposed rule's approach or offered alternatives for measuring efficacy. For the reasons stated herein, OAG finalizes the definition of accuracy minimum as proposed.

Theme: Some comments suggested the final rule should have laxer accuracy minimums or a standard of general reasonableness for age assurance accuracy for greater commercial reasonability and lower adult burden.

Some comments generally criticized the accuracy minimums as too stringent, requiring too few false positive age assurance outcomes, which commenters surmised would create excessive cost for operators and increase the risk of enforcement. Of those comments, a few suggested that the minimums be replaced by a general reasonableness standard.

The comments asserted the minimums would lead to a meaningful economic burden without providing any data to support the argument that the accuracy minimums as proposed would not be commercially reasonable for operators. As described at length in Part IV of the NPRM, the analysis conducted by OAG demonstrates that, in fact, age assurance costs will minimally burden operators. To further protect against economic burden, the rule proposes that exempt online platforms need not comply with the rule until such time as the operator achieves the minimum number of monthly active users or covered minor monthly active users specified in section 700.1(q). No comments provided data or alternative analyses to substantively contradict OAG's analysis, including the analysis of costs associated with age assurance or the exemption thresholds. The OAG thus finds no basis to adjust the parameters of the accuracy minimum definition due to purported economic burden.

With respect to enforcement risk, the comments raising this concern did not explain their rationale beyond asserting that operators would not be able to meet the requirements in the accuracy minimum and as such would risk adverse enforcement action. But the comments did not provide any support for the argument that the false positive maximums in the accuracy minimum definition are not achievable through commercially reasonable and technically feasible age assurance methods. In fact, as discussed in Part III.D.3 in the NPRM, OAG extensively analyzed the efficacy of age assurance methods, established the age categories and corresponding false positive maximums directly from this analysis, and concluded that these requirements are achievable by operators using commercially reasonable and technically feasible age assurance methods.

With respect to the suggestion that a general reasonableness standard would be a preferable alternative to the accuracy minimum requirement as proposed, this proposal lacked any detail as to how this standard would meet the statutory mandate of protecting minor users, including how OAG could measure efficacy or protect against operators taking insufficient steps to accurately identify minor users. Particularly in light of the current and historical state of age assurance on addictive platforms as outlined in Part III.D.1.a of the NPRM, OAG has concluded that objective standards are needed to define "reasonable" efforts by operators.

Some commenters argued that the accuracy minimum definition as proposed would lead to excessive burden on adult users, who will be asked to undergo age assurance to demonstrate their adult status. Based on OAG's analysis of age assurance technology, OAG anticipates that some adults may be asked to undergo age assurance. The extent of burden on adults will depend upon the age assurance method selected by the operator. For example, operators already in possession of sufficient user data may be able to use age inference as one method and this method may eliminate the need for many adults to undergo burden in

connection with age assurance. The false positive maximums in the accuracy minimum definition also minimize adult burden to the extent possible while upholding the statutory objective of protecting minor users; this is why the false positive maximum for 17-year-olds is higher than for younger minor users. For the reasons set forth in the NPRM and herein, OAG thus adopts the proposed framework as maximizing the balance between accurately identifying minor users and minimizing adult burden.

Theme: One commenter argued different, lower accuracy minimums for older minor users may not be appropriate or justified.

One commenter questioned whether the variation in allowable false positive rates, in particular the higher false positive rates allowed for 16- and 17-year-olds, is justified. The commenter did not provide data or analysis to contradict OAG's preliminary findings in the NPRM. As described in Parts III.D.3 and III.D.4 of the NPRM, in setting the allowable false positive rates, OAG extensively analyzed available data related to the accuracy of commercially available age assurance methods across the full spectrum of user ages. The OAG proposed the maximum rates by balancing the need to protect minors from addictive feeds with the commercial reasonability and technical feasibility of age assurance methods available to operators and the user burden associated with various age assurance methods. The allowable false positive rates reflect the efficacy of commercially available age assurance methods that operators can adopt.

Another commenter expressed concern that establishing allowable false positive rates may encourage operators to forego age assurance methods with false positive rates that are lower than the allowable maximums. As noted in Part III.D.3.l of the NPRM, under section 700.4(g), operators also have an ongoing obligation to "act reasonably and in good faith to adopt more effective age assurance methods consistent with related industry and technological developments." Together, the two requirements balance the benefit to regulated entities of bright-line rules with the evolving nature of the age assurance industry, which in recent years has continuously improved the efficacy of existing methods and made new age assurance methods commercially available.

Theme: Commenters opined on the propriety and effectiveness of required age categories and accuracy thresholds.

The OAG received a few comments on the five age categories established in the accuracy minimum definition (consisting of ages 0-7, 8-13, 14-15, 16, and 17) and false positive maximums associated with each category. Some commenters praised the framework and the underlying acknowledgement, discussed in Part III.D.3.d of the NPRM, that accurately determining adult status through age assurance becomes more difficult as users approach adulthood. Commenters recognized that the graduated framework and age categories afford maximum protection to minor users while minimizing adult burden.

Other comments challenged OAG's justification for the accuracy benchmarks assigned to each age category. In each case, commenters' broad assertion that OAG did not sufficiently justify the age-specific accuracy requirements was not supported by any substantive arguments or countervailing data. In fact, as described in Part III.D.3 of the NPRM, OAG selected the age categories and the accompanying accuracy requirements following analysis of accuracy data for a variety of age assurance methods. This taxonomy optimizes the balance between protecting minors from addictive feeds and minimizing adult burden through a broad range of commercially reasonable and technically feasible age assurance methods available to operators.

One commenter suggested that the number of age categories be reduced to a smaller number of broader age ranges to reduce the data collected from young users for testing purposes. The OAG declines to adopt this recommendation. Reducing and broadening the age categories will not advance the purpose of the Act as doing so will reduce the overall accuracy of the maximum false positive rates that are achieved by using commercially reasonable age assurance. Further, the testing and certification of age assurance methods will require those methods to be tested against minor users of all ages, regardless of the number of age categories included. Any incremental reduction of testing data resulting from a reduction in age categories does not outweigh the drawbacks described above.

Theme: Commenters addressed the method circumvention threshold.

A few comments received by OAG also addressed the accuracy threshold for method circumvention. Each of these comments was submitted by groups representing operators. The comments claimed that a 98% method circumvention detection rate was not an achievable minimum absent excessive operator burden. The comments asked that the detection rate be reduced although none of the comments proposed an alternative. Notably, none of the comments from age assurance providers or groups representing them contended that 98% method circumvention detection was not achievable. OAG considered a range of available information in setting the threshold and none of the comments provided any additional data to support the argument that a lower method detection threshold is warranted. Absent any such data, and because detection of method circumvention is critical to the overall efficacy of an age assurance method, OAG declines to lower the method circumvention accuracy threshold.

Theme: Commenters provided feedback on total accuracy minimum definition and relationship to accuracy minimum.

A few comments from the age assurance industry and one municipal agency provided positive feedback on the combined requirement of the accuracy minimum and total accuracy minimum, as well as the relationship between the two minimums. The commenters noted that the interplay of the minimums reflects a sophisticated understanding of age assurance technology and allows operators to craft an age assurance program that maximizes efficacy and minimizes user burden.

Other comments expressed confusion, or reflected a misunderstanding, regarding how the accuracy minimum and total accuracy minimum interact in an operator's age assurance program. For example, one comment criticized the collective minimums as prohibiting methods that are effective but not able to meet the accuracy benchmarks for all users. As described in Part III.D.3.e of the NPRM, OAG established the accuracy minimum and total accuracy minimum as companion benchmarks to allow operators to utilize multiple age assurance methods that address different portions of their user population. For example, if an age assurance method addresses only a subset of users but meets the accuracy minimum standards for those users, an operator can utilize that method for those users. At the same time, the operator must provide at least one method that meets the requirements in the rule as applied to every user; this obligation is reflected in the total accuracy minimum definition and requirement. The operator may choose one method that meets both the accuracy minimum and total accuracy minimum requirements or may combine multiple methods to meet those requirements. The OAG anticipates that operators will make different choices to best serve the needs of their business and users.

Theme: Some commenters argued the rule should include a standard for false negatives.

Some comments suggested that the final rule include maximum allowable false negative rates in the accuracy minimum definition, stating that including both false positive and false negative maximums would more comprehensively limit any disparate impact of age assurance on protected groups. One comment suggested that the two rates be combined as a single percentage of incorrect outcomes. The OAG carefully considered the appropriate role of false negative rates. Section 700.5(b), as finalized, requires, as part of annual testing and certification, the measurement of false negative rates, both in aggregate and disaggregated by age categories 18, 19-20, 21-25, and 26-30, along with false positive rates in aggregate and disaggregated by the age categories in the accuracy minimum. The OAG is not convinced that further specifying false negative rates or any other alternative would better facilitate equity in the application of age assurance methods.

With respect to including false negative rates in the accuracy minimum definition, OAG declined to propose false negative maximums following extensive analysis of age assurance technology and the commercial incentives for operators to minimize false negatives within the range of commercially reasonable and technically feasible age assurance methods available. Commenters' concerns that operators may choose age assurance methods with high false negative rates for cost savings purposes overlooks the economic incentives to continue furnishing users with addictive feeds, based on the relationship between engagement maximization and per-user revenue.

Commenters' suggestion to incorporate specific false negative requirements is not persuasive. As proposed, the rule allows operators some flexibility to balance user burden against factors such as overall accuracy and cost. At the same time, the proposal includes

safeguards to limit the negative impact on users of false negative outcomes in several ways. First, the requirement that false negative rates be annually tested provides operators with detailed visibility into the percentage of their users potentially impacted by false negative outcomes. Second, section 700.4(g) requires that operators periodically examine their chosen age assurance methods against other available age assurance products and act reasonably and in good faith to adopt methods with lower false positive and false negative rates. Third, the rule requires that operators provide individual users impacted by a false negative outcome with an avenue for redress through the appeals process set forth in section 700.6.

For all of the reasons above and in the NPRM, the OAG adopts the definition of accuracy minimum as proposed.

7. Testing and certification

The OAG received comments regarding the testing and certification requirements for age assurance methods. Some comments, including from the age assurance industry and the advocacy community, expressed general support for testing and the related framework and requirements laid out in the rule. Some comments from representatives of operators criticized the testing requirements as financially burdensome or unjustified. Other comments sought clarification or changes to the testing conditions required in section 700.5. And a few comments requested that testing results be made public. After careful consideration, OAG adopts the testing and certification requirements in section 700.5 as proposed, with minor amendments to the regulatory text as set forth below.

Comments from both the advocacy community and the age assurance industry generally provided favorable feedback regarding the certification requirement for age assurance methods as an important protection of method integrity. Commenters specifically praised the requirement that testing providers be accredited and the adoption of internationally recognized industry standards such as ISO 27566-1 as uniform testing benchmarks.

Theme: One commenter questioned statutory authority for a certification requirement in the rule.

One comment posited that the annual certification requirement, and in particular the requirement that testing providers be accredited, exceeds OAG's statutory authority by imposing a licensing regime on operators. The OAG disagrees. The certification requirement sets a standard to ensure age assurance is effective and safe, as expressly authorized by G.B.L. § 1501(2)(b), which directs OAG, in setting standards for commercially reasonable and technically feasible age assurance, to consider the "effectiveness of available age determination techniques" and "the impact of the age determination techniques on the covered users' safety," among other things. Specifically, the annual certification requirement confirms that age assurance methods are consistently effective in meeting the required accuracy minimums in a dynamic online environment, as well as the data minimization and security requirements. The

rule does not create a licensing regime: it requires no license for operators or third-party providers of age assurance methods, nor does it establish a licensing authority or related requirements. Given the nature of the online age assurance process and the rule's deletion requirements for live user data, certification and testing are the most efficient methods for ensuring that operators are not, intentionally or inadvertently, employing age assurance methods that are not sufficiently effective.

Similarly, the requirement that testing providers be accredited employs an objective and broadly recognized standard to confirm that the testing provider is both adequately equipped to perform the required testing and free from any bias or affiliations that might impact the integrity of the testing results. The rules do not empower any government entity to assert licensing authority over a testing provider but rather require use of the well-established system of accreditation via organizations such as the American National Standards Institute, or an equivalent body.

Theme: Some commenters asserted testing and certification may be burdensome operationally and financially.

Some comments from representatives of operators expressed concern regarding the perceived burdens associated with annual testing by an accredited third party. Some commenters claimed that annual testing will present financial and operational burdens for operators, particularly for smaller platforms. One commenter relatedly asked that the frequency of certification be extended from one to three years. None of the commenters submitted any data or economic analysis to support their argument regarding financial burden.

While OAG acknowledges that testing involves some operational burden, that burden is outweighed by the statutory purpose of protecting minors through effective age assurance methods. The alternative to demonstrative efficacy through testing is to audit age assurance outcomes provided for live users, which would require the extended retention of live user data, creating privacy and security challenges. It also is important to recognize that, while operators remain responsible for ensuring that the requirements of the rule are met, the testing obligation attaches to specific age assurance methods rather than an operator's overall age assurance program. Thus, a third-party age assurance provider furnishing multiple operators with an age assurance product could undergo compliant annual testing and that testing may constitute compliance with each of the operator's obligations under section 700.5 as to that method (subject to compliance with section 700.5(e) as well as operator diligence and good faith as described further below). Given that age assurance providers may be impacted even more directly by the testing and certification obligations in the rule, it is instructive that comments from the age assurance industry uniformly supported these requirements.

With respect to purported financial burden, the economic analysis in Part IV.B of the NPRM makes clear that the baseline costs of testing and certification as factored into age assurance adoption and maintenance costs are not overly burdensome to covered, non-exempt

platforms. Additionally, if an operator chooses to offer age assurance via a third-party provider, that provider may absorb some of the costs of testing and certification (which are specific to each age assurance method), potentially resulting in efficiencies of scale. Should an operator develop its own age assurance method, that operator would be directly responsible for the costs of testing and certification of that method, but may experience associated cost savings in the elimination of third-party usage costs. Further, such an option is not necessary as commercially reasonable and technically feasible age assurance methods are available to operators from third parties. In particular, OAG does not consider such incremental financial burden to be a sufficient reason to extend the time period for certification from one to three years, in light of the fact that both operators and age assurance methods have historically rapidly evolved and changed to meet market trends and user demand, and that no operator has provided data to support the conclusion that annual testing and certification are commercially infeasible.

One comment argued the accreditation requirement for testing providers effectively excludes entities that are not accredited but that the commenter perceived to be capable of performing testing, such as academic institutions and non-profit organizations. The OAG received no comment from any academic institution or non-profit organization expressing interest in performing age assurance testing and the commenter did not explain why such institutions would not be capable of obtaining accreditation. In setting the testing and certification requirements, OAG explored the associated operational needs for testing providers, which include specialized knowledge and equipment specific to age assurance testing. Even an institution that is highly qualified in many areas may lack the specific proficiency or tools needed to perform the testing required by the rule. Should such institutions in fact be capable of performing the testing and incentivized to do so on behalf of an operator, obtaining accreditation to establish this competency should not be an undue burden. Further, nothing in the rule prevents operators or age assurance providers from working with any entity to perform general testing. Notwithstanding these conclusions, in an effort to maximize the ability of qualified testing companies that are recognized by accreditation bodies such as the American National Standards Institute or an international equivalent to perform age assurance testing and certification, OAG removes the specific reference to ISO/IEC 17065 from the definition of “Accredited Third-Party" in 700.1(a), instead relying on the accreditation bodies to use such accreditation standards as are appropriate.

Some comments asked that OAG allow operators to conduct their own testing or certification to satisfy the requirements of section 700.5. The comments provided no details as to how the capability of operators to perform this testing or certification could be measured, how operators could avoid the perception of bias in conducting their own testing or certification, or how such a system would prevent evasion of the requirements by ineffective or purposely non-compliant operators. Because the testing and certification obligations in section 700.5 are the primary means by which OAG will establish operator compliance with the rule,

OAG rejects the option of direct operator testing or certification as insufficient to achieve this purpose.

In proposing the rule, and as addressed in the NPRM, OAG considered and rejected alternatives such as regular audits performed by OAG, increased operator reporting obligations to OAG, or loosening the data deletion requirements to enable a retrospective re-creation of age assurance results for covered users. But no alternative presented an efficient solution that serves the statutory purposes of ensuring operators employ effective age assurance and preserving users' privacy, while minimizing burden on operators and conserving government resources. As such, OAG adopts the annual certification requirement and associated accreditation requirement for testing providers, as proposed.

Theme: Some commenters suggested the final rule require publication of certification results.

A few comments requested that OAG require the publication of the results of section 700.5 testing by operators, claiming that making the data available to the public would facilitate public understanding of the efficacy of age assurance, including by other policymakers. While OAG generally encourages the transparency of age assurance testing data, following consideration, OAG declines to mandate the publication of all testing that occurs in connection with section 700.5 compliance. The OAG notes, however, that nothing in the rule prevents operators and age assurance providers from publishing or otherwise sharing testing results so long as those results comport with the data privacy and security requirements in the rule.

Theme: Commenters sought clarification on the extent to which operators can rely on testing providers for compliance with the rules' age assurance requirement.

A small number of comments sought clarification regarding the ability of operators to rely on the testing results produced by accredited testing providers. One comment suggested that OAG provide a safe harbor to operators engaging in good-faith implementation of age assurance. The OAG anticipates that operators will rely on the testing results but also expects operators to take consistent measures to ensure the accuracy and integrity of the test results.

As contemplated by the rule, testing providers will use industry-recognized testing standards and specialized equipment and knowledge to validate the efficacy of an age assurance method along with related requirements such as data minimization and deletion. Operators are not expected to replicate the testing process or to question the technical or specialized aspects of the testing methods. This does not equate to a total safe harbor or abdication of responsibility regarding testing results, however. The OAG expects operators to take actions such as conducting diligence on the historical performance and reputation of testing companies before selecting a testing provider, providing truthful, accurate and complete information to the testing provider, and questioning any aspects of the testing process or results that raise concerns regarding accuracy or integrity.

Additionally, OAG notes that, as set forth in section 700.5(e), testing will only validate an operator's use of an age assurance method if the variable settings and options deployed for covered users are the same settings and options for which certification was granted. The obligation to ensure this consistency remains the responsibility of the operator.

Theme: Commenters provided feedback regarding testing requirements for age assurance.

The OAG received numerous comments, including from the age assurance industry and one testing provider, commending OAG's decision to incorporate two internationally recognized testing standards in the definition of "certification." The commenters expressed support for these standards as testing benchmarks.

One comment from an operator representative criticized the rule as lacking additional specifications regarding testing such as specific methodologies and validated datasets. The commenter asked OAG to provide these details. The OAG declines to provide additional requirements specific to testing. Because the rule allows operators to adopt a broad range of age assurance methods, it is anticipated that testing requirements may vary considerably based upon the age assurance method being tested. This includes new age assurance methods for which no testing standard may initially exist. Whether an age assurance method meets the requirements for certification also will depend upon the options and settings chosen by the operator in implementing the age assurance method. These conditions create a large and dynamic number of testing variables; as such, the testing process will not be well-served by mandating a single set of testing methodologies or datasets.

The OAG has adopted the ISO 27566-1and IEEE 2089.1 testing standards for age assurance, which are designed to apply to a broad range of age assurance methods. More specific methodologies and datasets must be determined by the accredited testing providers with input from operators. Should established standards be unavailable for or incompatible with testing of a new age assurance method, section 700.5(f) allows operators and accredited testing providers to develop protocols that are consistent with the requirements in the rule and to retain records of the protocols and results that can be examined later by OAG as needed.

One comment proposed that OAG mandate the inclusion of specific testing information in the report prepared by the testing provider, such that the testing results could be independently replicated. While OAG declines to adopt this specific mandate, section 700.5(b) requires that the report include "testing protocols used and all results," including several specific categories of results, and OAG expects that the level of detail in the report will provide adequate detail to allow OAG to engage in follow-up inquiries as needed.

Finally, one comment asked that OAG allow operators to use benchmarks from the facial age estimation study conducted by the National Institute of Standards and Technology (NIST), *see* NIST IR 8525, as an allowable alternative to the use of ISO 27566-1 or IEEE 2089.1. The OAG declines to expressly adopt the testing standards used by NIST, which rely upon data not

available to the general public and which were not expressly designed for reproduction by private testing providers. The OAG recognizes, however, that accredited testing providers may choose to adopt testing methods reflected in NIST IR 8525, for the testing of facial age estimation methods.

Theme: One commenter suggested the final rule clarify certain testing conditions.

The OAG received one comment that raised questions regarding section 700.5(c)(1), which sets certain specifications for sample size calculation for testing. The comment suggested OAG omit several aspects of the section and set specific percentages for both the confidence level and margin of error allowable in testing results. Following consideration of this comment, OAG adopts the language change recommendation in part, declines to adopt exact percentages for confidence level and margin of error, and modifies section 700.5(c)(1) to clarify requirements for sample size.

As discussed in the previous section, testing methods and conditions will be based on numerous factors such as the age assurance method being tested and, as applicable, one or more variable settings and options implemented by operators. The sample sizes employed in testing must always yield reliable results, as stated in section 700.5(c)(1). The requirement that those results have a "high confidence level and a low margin of error" reflects the common understanding in data science of the narrow percentage range acceptable to achieve a "high" confidence level and a "low" margin of error. The OAG expects that the accredited testing provider will assign the appropriate percentages and will make those decisions available in the testing report.

The OAG declines to mandate specific percentages for the confidence level or margin of error necessary to achieve reliable results. This decision is based on the recognition that testing must include samples that represent both an aggregate population and various sub-populations, including specific age categories and such sub-populations as are needed to ensure the age assurance method satisfies the operator's obligations under applicable law. Mandating a single percentage for confidence level and margin of error across all tests of every sub-population could create testing conditions that are infeasible for testing providers. Following extensive consideration, OAG concludes that the specific confidence level and margin of error percentages for each test performed are best determined by the testing provider, with input from the operator, and may vary by test based upon the identified sub-populations to be tested.

Relatedly, OAG included the population of the State of New York as a baseline for operators and testing companies to make a number of determinations, including overall sample size, demographic categories that may be necessary to include as sub-populations, and the appropriate confidence level and margin of error percentages to assign to those sub-populations to achieve reliable results, based upon the corresponding population in New York State. After considering the comment, OAG declines to remove this benchmark for sample size calculation.

Following consideration, OAG agrees with the commenter that inclusion of the term "statistically significant" is redundant, as reliable testing results with a high confidence level and low margin of error are, by their nature, statistically significant. The OAG therefore strikes the language "and statistically significant" from section 700.5(c)(1).

8. Testing of method circumvention

The OAG received two comments addressing the testing of method circumvention detection in connection with certification that an age assurance method meets the accuracy minimum and total accuracy minimum. The first comment, from an age assurance provider, sought additional clarification regarding the types of testing required to comply with section 700.5(b)(4). That section requires testing of method circumvention detection "consistent with a nationally or internationally recognized standard, or if none is available, including a variety of attack vectors weighted to reflect the most prevalent risks."

The types of method circumvention tested will be specific to the age assurance method, as a user's circumvention attempts for one type of age assurance method may be inherently different than for another. But regardless of method type, all age assurance methods should effectively detect the circumvention methods most likely to be employed by users of addictive online platforms. This includes attack methods that are available to the average user, reflecting low or possibly medium sophistication, budget, and timeframe. More sophisticated circumvention methods should be included in the testing where evidence of past use exists but are likely to make up a relatively small proportion of the overall testing data set. The type and proportion of method circumvention types represented in the testing data should be based upon the best information available, and records reflecting the decisions and justifications for the make-up of the testing data should be retained in accordance with section 700.5(d).

The second comment recommended that, due to the differences in testing conditions described in the previous paragraph, the testing of method circumvention be subject to a qualitative rather than a quantitative standard. After careful consideration of this recommendation, OAG declines to adopt it. As expressed in the previous paragraph, the testing data for method circumvention detection will be customized to reflect both the specific age assurance method being tested and the nature of the attacks most commonly experienced by that method in connection with users of addictive online platforms. Once the testing data has been established, the performance of the age assurance method against that data can and should be measured on a quantifiable basis to ensure the method maintains a high accuracy rate.

The comment also expressed concern that a quantifiable testing standard that measures the detection of users' attempts to mask their location using a VPN or similar technology could encourage operators to engage in privacy-invasive methods to boost detection accuracy. But testing the detection of a user's location is not required by section 700.5 because determining that location is a separate obligation of the operator that temporally precedes the direction of a

user to an age assurance method and is unrelated to the efficacy of the age assurance method in detecting method circumvention. For these reasons, OAG maintains that a quantitative threshold is the most appropriate measure of method circumvention detection.

9. Inconclusive Age Assurance Outcome: Section 700.1(t)

A small number of commenters sought changes to, or a clarification of, the definition of inconclusive age assurance outcome and its relationship to accuracy minimums. The OAG adopts the definition of inconclusive age assurance outcome as proposed and responds to the comments below.

Theme: Commenters made inquiries and provided feedback regarding the relationship between false negatives resulting from a buffer age and the definition of inclusive age assurance outcome.

One commenter sought clarification regarding the definition of inconclusive age assurance outcome and specifically whether it applies in instances when an operator intentionally selects an age above 18 as the target age to decrease the false positive rate for minor users, sometimes referred to as a "challenge" or "buffer" age. As explained in Part III.A.20 of the NPRM, the definition of an inconclusive age assurance outcome is limited to instances in which, following receipt of all required information, the age assurance method does not function as intended, such as in instances when the data provided is of unusually low quality, when the age assurance method is tuned to be too sensitive to data quality, or when the method is not functioning as it should for technical reasons.

An intentional decision by the operator to create a buffer age to decrease an age assurance method's false positive rate, where that decision leads to the method's inability to confirm adult status for an individual below the buffer age, is creating an intended outcome and accordingly should not be treated as an inconclusive age assurance outcome. However, it also is not categorized as a false positive. Rather, the determination by an age assurance method that an adult user has not met the buffer age should be considered a false negative outcome. Although the rule does not set a threshold for false negatives, in testing, these false negatives must be reported under the rule. Operators are incentivized not to adopt a system that results in too many false negatives as it creates user friction for adults misidentified as minors. In instances when a user contests they are a minor and the user is identified by the age assurance method as falling within the buffer age range, the operator may either allow the user to choose an alternative age assurance method – or, if such a method is not available or is declined by the user, to allow the user to advance to the appeals process to demonstrate adult status.

Theme: Commenters raised questions regarding the effect of inconclusive age assurance outcomes on accuracy minimum requirements.

One commenter expressed concern that allowing outcomes to be categorized as inconclusive age assurance outcomes may enable operators to consistently deny access to users

with hardware that generates lower quality data or may generally mask poorly functioning age assurance methods.

While OAG recognizes the commenter's concern regarding evasion of the required accuracy minimums, it ultimately rejects this argument as unpersuasive for several reasons. First, the argument overlooks operators' primary incentive, which is to attract and maintain users. To the extent operators want to discourage certain types of users from their platforms, OAG does not have reason to believe age assurance that has been tested and certified is likely to allow for targeted exclusion of certain users. Relatedly, operators have an incentive to select age assurance methods that function as intended and optimize those methods for the maximum number of users, to minimize cost and user friction. The argument further discounts operators' economic incentive to identify users demonstrating adult status, due to revenue models built on engagement maximization and fueled by addictive feeds and nighttime notifications.

Second, the testing and certification requirements in the rule mandate that testing reports include "rates of inconclusive age assurance outcomes and the reason for each age assurance outcome," (at section 700.5(b)(2)), which will create transparency as to the frequency and cause of this result. Third, while data quality is a factor in the ability of an age assurance method to function as intended, commercially reasonable and technically feasible age assurance methods are capable of accommodating a wide range of data quality and can provide users with instructions on optimizing that quality. To the extent a user cannot furnish sufficient quality data, that user may exercise the appeals process to demonstrate their age status through alternative means.

Another commenter asked OAG to confirm that operators may assume a covered user's adult status if all offered age assurance methods yield an inconclusive age assurance outcome and there is no actual knowledge of minor status. As specified in G.B.L. § 1501(d) and in section 700.4(b)(ii), OAG confirms that an operator may assume adult status but notes that the operator must comply with all requirements in 700.4(b).

Theme: Commenters made inquiries regarding conflicting age assurance outcomes.

One commenter asked OAG to clarify the obligations of an operator in a scenario in which the same covered user completes two different offered age assurance methods and those methods yield opposing results. The rule provides sufficient direction to operators regarding scenarios in which conflicting age assurance method outcomes may occur. As acknowledged by the comment, conflicting age assurance outcomes are unlikely to occur in the course of the standard age assurance process, including because the completion by a covered user of multiple age assurance methods yielding conclusive results will be a rare occurrence. In such instances, as stated in section 700.4(a)(2), subject to an operator's good faith determination that a covered user has adult status pursuant to sections 700.6(a) & (d), a determination of minor

status by a compliant age assurance method conveys actual knowledge of that minor status to an operator.

10. Impact of age assurance on actual knowledge of adult status

One comment argued that the concept of "age status" in the rule exceeds operators' obligations under the Act, which the commenter characterizes as requiring only that an operator take action based on actual knowledge that a user is a minor. Another commenter asked that OAG substitute an actual knowledge standard for the age assurance requirements in the rule. These comments misconstrue or overlook the mandate in the Act that operators use "commercially reasonable and technically feasible methods to determine that the covered user is not a covered minor."[18] Operators are obligated under the Act not only to act on information in their possession regarding the minor status of the user, but to ascertain whether a covered user is a minor using commercially reasonable and technically feasible age assurance. The concept of "age status" in the rule operationalizes this requirement as part of its age assurance framework. The OAG therefore declines to modify the final rule with respect to the age assurance requirements in section 700.4 or the definition or use of "age status."

The same comment criticized operators' obligation to respond to reports of method circumvention by users and to take reasonable measures to avoid users' intentional concealment of location, framing these requirements as a constructive knowledge obligation that exceeds operators' statutory obligations under the Act. The OAG disagrees. G.B.L. § 1501(c) requires OAG to "identify the appropriate levels of accuracy" for age assurance and the detrimental impact that method circumvention and location concealment necessarily have consequences for the accuracy of age assurance methods, and thus, it is well within OAG's authority to account for them in satisfying that statutory mandate.

G.B.L. § 1501 also authorizes OAG to establish "commercially reasonable and technically feasible methods for covered operators to determine if a covered user is a covered minor," and G.B.L. § 1505 authorizes "such rules and regulations as are necessary to effectuate and enforce the provisions of this article." In so doing, the Act directs OAG to consider the efficacy of the age assurance methods. As explained in Part III.D.3.f of the NPRM, combatting method circumvention is an element of any effective age assurance method. New circumvention methods emerge on a regular basis, particularly with the improvement of AI technology, and information regarding successful circumvention methods can rapidly proliferate online. If unchecked, a new circumvention method that is not being detected by age assurance can undermine an age assurance method's efficacy and erode public trust in that method. This scenario can occur even if an age assurance method has regularly undergone annual testing and certification.

[18] G.B.L. § 1501(a).

The requirement in section 700.4(d)(3) that an operator conduct a good faith investigation of reports of new or previously undetected forms of method circumvention thus ensures that age assurance methods remain effective and that the accuracy minimums are actually being met when the age assurance methods are operating in real life. This is not a constructive knowledge requirement; rather, section 700.4(d)(3) requires operators to respond to reports or material changes in aggregate data with a good faith investigation as to their validity, and to act upon valid evidence of systemic circumvention.

As an alternative, OAG considered increasing the frequency of age assurance testing and certification requirements. However, this would increase burden and expense and is a less targeted approach and, thus, may not demonstrably improve outcomes. Allowing operators to determine when action is needed following an investigation is the more balanced, flexible solution that also protects the efficacy and integrity of age assurance. Accordingly, OAG adopts section 700.4(d)(3) as proposed.

With respect to individual users, section 700.4(d)(2) obligates operators to respond to reports that a user has engaged in method circumvention leading to an alleged false positive outcome. The OAG recognizes that commercially reasonable and technically feasible age assurance methods are not foolproof and that some users will successfully mislead an age assurance method into concluding that they have adult status. Section 700.4(d)(2) creates a duty to follow up on reports rather than ignore them. Once again, this is the more balanced and feasible alternative for minimizing minor user harm resulting from false positive age assurance outcomes, versus requiring that all age assurance methods never or virtually never allow false positive outcomes. The OAG thus adopts section 700.4(d)(2) as proposed.

Finally, sections 700.2(d)(2) and 700.3(d)(2) obligate operators, in determining whether a user is a covered user to which the Act's protections apply, to "take reasonable steps to investigate and detect covered user efforts to conceal or misrepresent their location." Many platforms already possess information regarding a user's location. Further, users' employment of technology such as VPNs to avoid location-specific requirements is often readily apparent to operators via basic technical signals. The rule obligates operators to take "reasonable steps" to use available resources to determine whether a user is a covered user or whether more information is needed to make the determination. This is a balanced and reasonable approach in light of the fact that minor users not identified as covered minors will receive none of the protections afforded by the Act. For these reasons, OAG adopts sections 700.2(d)(2) and 700.3(d)(2) as proposed.

Theme: Commenters raised questions regarding joint use of an account by adults and minors.

One comment questioned the extent to which operators should rely on age assurance as conveying actual knowledge of adult status when presented with conflicting evidence. As an example of a complex user scenario, the comment described an account used by both adults and minors, such as a social media account associated with a youth sports team. Recognizing

that such an example likely represents a small percentage of the overall user population, OAG clarifies below the requirements of the rule as it relates to this and similar examples.

As set forth in section 700.4(b), to treat a covered user as an adult, an operator must successfully complete age assurance for the user and either receive a confirmation of adult status or an inconclusive outcome across all methods. Additionally, section 700.4(a)(4) states that actual knowledge of minor age status can be based on an operator's "good faith determination based on other, reliable evidence or knowledge that the covered user is a minor." Accordingly, if an operator receives confirmation via age assurance of a user's adult status, and later receives credible information that the account is being used by a minor, either in addition to or instead of the adult user, the operator likely has sufficient evidence to determine that the account is associated with a covered minor and classify the account as such. This data may include data used by the operator for "marketing, content selection, or other commercial purposes" as cited in section 700.4(a)(3).

11. Appeals process: Section 700.6

The OAG received a number of comments regarding the appeals process as proposed in section 700.6. Several commenters praised the inclusion of an appeals process as an important element of a fair and equitable age assurance program. Some commenters sought changes to the requirements of section 700.6, based on their rationale that the framework in the rule is either too permissive or too strict. For the reasons described below and in the NPRM, OAG adopts section 700.6 as proposed.

Theme: Commenters made suggestions for amendments to the appeals process framework.

Some comments expressed concern that the framework for the appeals process laid out in section 700.6 affords too much leeway to operators to deny addictive feed access to adult users or to require users to provide government-issued ID. The OAG disagrees. Section 700.6(a)(1) obligates operators to offer, as part of the appeals process, at least one method other than government-issued identification; an operator with an appeals process that only offers this method on appeal would be in violation of the rule.

Additionally, recognizing that operators are financially incentivized to identify adults where possible but must protect against users falsely claiming adult status through the appeals process, the parameters proposed in section 700.6 provide the best balance of allowing operators to craft the appeals process best-suited for the needs of their users while holding those operators accountable for their appeal adjudications by requiring a timely appeal determination (at section 700.6(c)) and a written summary of the appeal decision including an explanation of its basis (per section 700.6(a)(4)).

Various comments recommended OAG include additional requirements as purported improvements to the process, including a mandate that appeals determinations be implemented immediately and that the appeals process be offered in the 12 most commonly

spoken languages in the State of New York consistent with Executive Law § 202-a and G.B.L. § 1506. The OAG declines to add these provisions. While section 700.6(d) expressly enables operators to change a user's age status from minor to adult based upon the appeal process and OAG expects that such a change will be implemented expeditiously, including because operators are financially incentivized to maximize adult users once adult age status is confirmed, OAG declines to mandate this change within a particular time period as operators' systems may vary in their ability to process the change. The OAG also declines to implement language requirements for the appeals process, which is consistent with the rule's framework for the underlying age assurance process. The OAG notes the requirement in section 700.6(b) that the appeals process be "clear, conspicuous, and accessible." Offering the appeals process in multiple languages may be necessary for that process to be accessible, depending upon the operator's user population; operators should consider this obligation in crafting their appeals process.

Following consideration of commenter recommendations for the addition of other requirements in the appeals process, including but not limited to mandatory human review, an independent ombudsman, mandatory web accessibility standards, and the inclusion of specific details in appeal records, OAG declines to adopt these measures, finding insufficient evidence to demonstrate that they would add user benefits beyond the current mandates of the appeals process in the rule that would offset the additional burden on operators.

Theme: Commenters suggested alternatives to the proposed timeframe for providing an appeal decision.

The OAG received one comment from a group representing operators, asking that the time for first response to an appeal be extended from 10 business days to 45 calendar days, claiming, without providing specific citations, that this period is allowed under most consumer statutes. The OAG also received one comment asking that the time for the full appeal adjudication be limited to 72 hours. The OAG declines to adopt either of these requests.

Section 700.6(c) specifies that a user appealing a minor age status determination receive an initial response within 10 business days and that a final determination be sent to the user "expeditiously" upon the receipt of all requested information. Following consideration of the comments, OAG concludes that this framework ensures users will not be subject to undue delay but also recognizes that operators may not be able to advance the appeals process while waiting for user-provided data. The OAG declines to extend the time for first response, including because the failure of the initial age assurance method or methods is a factor that, to some extent, is within the control of the operator; if the method or methods are ineffective, the operator thus should address user concerns expeditiously.

The proposed framework balances the prevention of user burden with commercial reasonability and operator agency to design an effective yet user-friendly appeals process. It is important to note that, consistent with section 700.9(b), at no time should users lose access to their accounts while the appeals process is ongoing.

Theme: One commenter argued records should be kept of the results of appeals and the results should be publicly reported.

One comment requested that OAG mandate operators provide detailed public reporting of appeal determinations. The OAG declines to do so. Absent a clear indication that the appeals process is not creating fair outcomes, OAG does not automatically conclude that greater public transparency is needed with respect to operator appeals process and, in fact, sees some risk that a more transparent process may become more vulnerable to users looking to misrepresent their age status. The OAG notes, however, that the data retention requirements in section 700.7(b)(1) include data on determinations made by the operator via the appeals process. This requirement will allow OAG to take such actions as are necessary to ensure compliance with the rule.

Theme: A commenter sought to confirm data minimization requirements for the appeals process.

One comment sought confirmation that data collected during the appeals process is subject to the same minimization and deletion requirements in section 700.7(a). The OAG confirms that the requirements in section 700.7 apply equally to data obtained and used in the appeals process, which is part of age assurance.

12. Third-party providers

A few comments addressed the status of third-party age assurance providers, seeking clarification regarding the providers' direct legal obligations under the rule. Two comments recommended that third-party providers be held directly responsible for the data in their possession should an adverse event occur such as a data breach. One comment expressed concerns that an absence of express liability for third-party age assurance providers creates a bad incentive structure for those providers with respect to the requirements of the rule.

Section 700.9(a) makes clear that, although operators are free to use third parties to provide age assurance methods, the operator remains responsible for all requirements in the rule satisfied by third parties. That said, third-party age assurance providers may also have legal obligations and face liability under other applicable laws such as data breach, privacy, and general consumer protection laws. Such obligations may also be reflected in the applicable agreements between third-party age assurance providers and operators.

With respect to third-party provider incentives, holding operators responsible for acts by third-parties upon which they rely for compliance will incentivize those operators to choose third-party age assurance providers that are capable of adhering to all the applicable requirements in the rule and to maintain oversight over those providers to ensure the requirements are met. This in turn may incentivize third-party providers to act responsibly as well.

Accordingly, OAG makes no changes in response to these comments.

13. User location

The OAG received comments regarding use of a user's location data in connection with an operator's obligation to determine whether a user is a covered user. Some commenters supported the use of data in operators' possession to determine user location or recommended OAG adopt specific additional technical requirements to ascertain a user's location. Other comments argued that the rule already requires operators to access too much user data, to the detriment of user privacy. Several commenters recognized VPNs as a known method for users to avoid accurate detection of their location, while one commenter requested that OAG take no action to discourage VPN use for legitimate security reasons. For the reasons described below and in the NPRM, OAG adopts the aspects of the rule related to user location as proposed.

Theme: Commenters provided feedback on operator use of user data to confirm location.

One commenter expressed support for operators' use of user location data in their possession to determine whether the Act applies to a user. Other commenters expressed concern regarding this provision, conflating it with a requirement that operators collect additional data regarding user location.

Sections 700.2(d)(1) and 700.3(d)(1) require that, in determining whether a user is a covered user, operators should "take into account all reliable information accessible by the covered operator regarding the user's location including technical information concerning a user's device and covered user data the covered operator possesses or accesses for marketing, content selection, or other commercial purposes." Many leading operators have publicly acknowledged tracking the location of user devices and as such already have access to many months or years of user location data. Even where user devices are not actively tracked by operators, those operators may still have high-quality location signals from users, including self-declared location that pre-dates the age assurance requirement and data obtained by operators for commercial or marketing purposes. Notably, this section does not instruct operators to collect additional data regarding user location. In this way, the rule balances user privacy with the reality that many operators are already aware of user location and must act on that information.

Theme: Commenters made suggestions regarding potential concealment of user location via VPNs.

Several commenters noted the known use of VPNs to conceal user location as an obstacle to the implementation of effective age assurance by operators. Some commenters surmised that use of VPNs by users undermines the statutory mandate to implement effective age assurance for covered users. Other commenters cautioned against requiring operators to adopt invasive geo-location requirements to defeat user location concealment via VPN. The OAG acknowledges users' concerns regarding VPNs as valid but nonetheless adopts as proposed

the provisions in sections 700.2(d) and 700.3(d) of the rule that address operators' obligations regarding user location data in determining whether a user is a covered user.

The OAG performed extensive analysis of VPNs prior to publishing the proposed rule. While OAG acknowledges that VPNs may obscure user location in some instances, the assertion that VPNs render age assurance ineffective overlooks a number of factors, most notably operators' pre-existing possession and use of reliable user location data. The availability of this data limits the ability of a user to obscure their location via newly implemented VPN use for the purpose of avoiding age assurance.

Additionally, while some users may use VPNs to avoid undergoing age assurance, prolonged use of VPNs in connection with a frequently visited platform, particularly one requiring a user to log in, is not always feasible for users. It is also the case that VPNs are often detectable. In recognition of operators' ability to detect user VPN use as one signal relevant to determination of user location, sections 700.2(d)(2) and 700.3(d)(2) require operators to "take reasonable steps to investigate and detect covered user efforts to conceal or misrepresent their location and, in such instances, employ reasonable methods utilizing available data to determine whether the user is a covered user." A user's VPN use may or may not raise questions for the operator regarding the user's location, but it is one factor that operators must consider in determining whether a user is a covered user.

The OAG does not intend to discourage the use of VPNs for legitimate security reasons. Sections 700.2(d) and 700.3(d) make clear, however, that operators may not rely entirely on a one-time IP address for a user as definitive proof of the user's location while ignoring signs that a VPN is in use or historical user location data in the operator's possession. Operators are obligated to take all such factors into account in concluding whether a user is a covered user.

14. Alternatives to age assurance

Some commenters proposed alternatives to platform-specific age assurance. Following consideration, the OAG rejects these alternatives for the reasons below.

Theme: Commenters argued the final rule should allow for app-based and device-based age assurance.

Some commenters advocated for app-based or device-based age assurance as an alternative to holding operators responsible for the conduct of age assurance. The OAG received a number of comments advocating for the age assurance framework in H.R. 10364, the federal App Store Accountability Act[19] – many, though not all, of these consisted of similar arguments and phrasing. A separate group of commenters, including individuals, advocates, one academic institution, and one municipal agency, noted the user privacy benefits of age information maintained directly on a user's device.

[19] H.R. 10364, App Store Accountability Act, 118th Cong. (2024).

In keeping with the statutory mandate of the Act, OAG declines to transfer responsibility for age assurance from operators to app store providers or device manufacturers. At the same time, OAG notes that nothing in the rule prevents operators from accessing and relying on a signal from either an app store or a device regarding a user's age status as it would from any third party. The flexibility to decide how age assurance is conducted does not, however, absolve the operator from the requirements of the Act and rule if the operator chooses to rely on a third party. Specifically, the operator remains responsible for ensuring the method comports with all requirements in the rule, including the accuracy and certification requirements. The OAG further notes that an app-based or device-based signal indicating minor age status may be treated by the operator as a self-declaration of minor age status pursuant to section 700.4(a)(1).

Theme: Commenters argued more readily accessible parental and user controls would obviate the need for age assurance.

A small number of users, primarily individuals along with one operator representative, advocated for OAG to forego age assurance in favor of increased parental and user controls such as the ability of a parent to disable all feeds offered by an operator or to whitelist specific apps and websites. While nothing in the rule prohibits the implementation of additional parental or user controls, none serves as a substitute for age assurance in achieving the statutory requirements of the Act. Additionally, OAG notes the comment of one academic institution that found parental controls to be generally ineffective in protecting minor users from dangerous features like addictive feeds or nighttime notifications.

Theme: Commenters proposed other alternatives to age assurance.

A handful of comments proposed alternatives to age assurance that would not comport with the statutory directive in the Act; as such, OAG declines to adopt them. These alternatives include content-based restrictions on platforms, broadening the Act's requirements to all online platforms, requiring covered operators to turn off addictive feeds and nighttime notifications by default and employ age assurance as a predicate to restore the features, and applying the restrictions in sections 700.2 and 700.3 to all users, not just minors.

15. Timing of age assurance implementation

One comment requested clarification regarding the timeline on which operators are responsible for providing age assurance that meets the obligations in the rule and implementing the section 700.2 and 700.3 requirements for covered minors. In accordance with the Act and as set forth in section 700.11, all aspects of compliance with the rule, including age assurance, must take place within 180 days of the rule's final publication in the State Register.

E. User and Covered User

1. Covered User: Section 700.1(o)

Theme: Some commenters suggested the proposed definition should be limited to only logged-in users or should only include logged-out users or users without accounts if such users can be reasonably identified as unique individuals.

A few commenters suggested only logged-in users or users that can otherwise be identified as unique should be considered covered users. The definition of covered user in the rule tracks the definition in G.B.L § 1500(4), which does not distinguish between the users that can and cannot be identified as individuals. Moreover, allowing operators to provide users with addictive feeds and nighttime notifications regardless of their age status so long as they are not logged in would incentivize covered online platforms to shift users to logged out experiences, which would be contrary to the goals of the Act. Accordingly, OAG does not modify the definition of covered user.

Theme: One commenter stated the requirement that a covered operator use reliable, accessible information to determine whether a user is a covered user under sections 700.2(d) and 700.3(d) should be expanded to create the same standard for determining whether a user is a covered minor.

One commenter suggested the addition of a requirement to sections 700.2(d) and 700.3(d) to ensure covered operators cannot plead ignorance of reliable evidence of minor status they have and use for other purposes. The OAG agrees substantively with the commenter. The rule accomplishes the same goal through a combination of provisions in section 700.4, namely sections 700.4(a)(3),(4), and 700.4(d). Accordingly, OAG declines to modify sections 700.2(d) and 700.3(d).

2. User: Section 700.1(hh)

Theme: One commenter contended the proposed definition of user is broader than the definition in the Act.

One commenter contends that the definition of "user" in section 700.1(hh) is broader than the definition in the Act. The commenter asserts that the statutory definition implies the only relevant users are "end-users" of a platform, and that this would exclude contributors to a platform, with the presumption that some or all contributors are not "end-users." The OAG disagrees.

The definition of covered user in G.B.L. § 1500(4) is "a user of a website, online service, online application, or mobile application in New York, not acting as an operator, or agent or affiliate of the operator, of such website, online service, online application, or mobile application, or any portion thereof." Under a reasonable reading of this provision an operator or agent or affiliate of the operator acting as such would be a "covered user" barring the explicit exclusion. The language, "not acting as an operator . . ." would otherwise be superfluous. The term user can thus reasonably include all uses of the website, including contributing media. Moreover, interpreting "interactions with media shared or generated by users" in the definition

of an addictive feed reasonably includes third-party contributors as users. Thus, OAG adopts this definition as proposed.

F. Verifiable parental consent

Proposed sections 700.2(e) and 700.3(e) of the rule outline identical standards for verifiable parental consent to access an addictive feed and nighttime notifications, respectively. Commenters generally addressed both, so for efficiency, OAG has consolidated its response unless otherwise noted.

To clarify the potential misunderstanding of some commenters as to the process outlined in the Act and rule: as proposed and now finalized, under sections 700.2(a) and 700.3(a), an operator may only provide an addictive feed or nighttime notifications to a covered minor at the behest of the minor with consent from the parent. The Act does not require parents to affirmatively change the settings of an addictive online platform to apply the protections to these features. Instead, an operator cannot provide a minor with these features by default; the operator must obtain parental consent to provide them.

Theme: Some commenters argued the rule creates a requirement for verifiable parental consent for a covered minor to access an online platform.

The final rule does not require parental consent for a minor to access any and all parts of an addictive online platform. Consistent with G.B.L. §§ 1501(1) and 1502, the rule imposes requirements for verifiable parental consent only with respect to two specific features: addictive feeds and nighttime notifications. G.B.L. § 1504, implemented by section 700.9(b), clarifies that a covered operator cannot comply by simply denying access to the platform to those covered minors who do not want or cannot get parental consent. Instead, covered operators that serve covered minors must provide them with an otherwise equal experience that does not include an addictive feed or nighttime notifications.

The Act also does not mandate that a covered operator provide a parental consent process. Part III.I of the NPRM clarifies that denying covered minors who do not receive parental consent access to the entire platform would violate the rule.

One commenter questioned whether age assurance and a verifiable parental consent request can precede a covered minor's attempt to access an addictive feed or nighttime notifications. Another suggested that age assurance and verifiable parental consent should only be permissible when a covered minor affirmatively attempts to access those features. As explained in Part III.I of the NPRM using the example of account creation, the covered operator has the option to conduct age assurance and parental consent either at account set up or when a user attempts to access the covered features. Either way, the operator must still comply with G.B.L. § 1504 and the corresponding section 700.9(b) of the rule. A covered operator cannot deny a covered minor access to an online platform simply because that covered minor does not wish to undergo age assurance or to request parental consent. A covered operator may offer its

users the option to skip age assurance and verifiable parental consent and to immediately access a version of the platform without addictive feeds or nighttime notifications.

The OAG makes no changes in response to these comments.

Theme: Some commenters contended the final rule should not require verifiable parental consent for certain higher-risk groups of covered minors.

Two commenters proposed that the final rule exempt certain groups of covered minors.[20] The commenters suggested that certain covered minors were potentially at higher risk of not being able to secure an individual who meets the requirements to provide verifiable parental consent.

The OAG is sensitive to the health and safety of covered minors. The Act, G.B.L. §§ 1501 and 1502, is clear in requiring verifiable parental consent to allow a covered minor to access an addictive feed or nighttime notifications without exception for any subset of covered minors.

Moreover, OAG does not believe any such exception is necessary. As discussed in Part III.A.28 of the NPRM, existing New York law provides an expansive definition of "parent" when determining who may grant consent on behalf of a minor. These laws govern sensitive areas, such as healthcare, where individuals traditionally deemed a "parent" (e.g., biological parents) may be unavailable or otherwise unqualified.[21] And an individual "in parental relationship" simply must be lawfully caring for the covered minor.[22] The final rule adopts this formulation and, thus, accommodates minors living outside of traditional households.[23]

Theme: Two commenters argued that the final rule should not require verifiable parental consent for minors aged 13-17 because older minors are capable of independent decision-making.

G.B.L. §§ 1501 and 1502 require verifiable parental consent to allow covered minors, with "minor" being defined as an individual under age 18, to access an addictive feed or nighttime notifications.[24] Neither section contemplates any exception based on the age of the covered minor. Consistent with Part II.B.2 of the NPRM and many commenters responding to both the ANPRM and NPRM, minors, including those aged 13-17, are more vulnerable than adults to the mental health harms caused by addictive feeds and nighttime notifications

[20] Suggestions included homeless, runaway, emancipated, and unaccompanied minors, as well as minors in foster care.

[21] For example, as some commenters have suggested, abusive parents.

[22] *See, e.g.,* Educ. L. § 2(10) (defining "in parental relation" as "parents, guardians or other persons, whether one or more, lawfully having the care, custody or control of such child . . . .").

[23] Further, in case multiple individuals or minors are potentially identified as a parent to the covered minor, sections 700.2(e)(5)(iii) and 700.3(e)(5)(iii)'s requirement that the method "be reasonably calculated to ensure that the individual providing consent is a parent" allows a covered operator to design policies and processes to address the situation.

[24] This definition does not prevent operators from complying with federal laws like the Children's Online Privacy Protection Act (COPPA), as discussed on page 47 and in Part III.B.4 of the NPRM.

because their neural paths are still developing.[8] Accordingly, OAG makes no changes in response to this comment.

Theme: Commenters weighed the efficacy of a verifiable parental consent requirement in deterring covered minors from accessing an addictive feed or nighttime notifications.

Many commenters supported the limits and optionality offered by the verifiable parental consent requirement. Some commenters suggested it would be ineffective because parents would grant consent without fully reflecting on the decision or would be pressured by operators or minors.

The Act allows operators to choose to implement verifiable parental consent. "Valid consent" as defined in section 700.1(ii) does not permit coercive practices, dark patterns, or other undue pressure by operators to obtain consent.[25] "Dark patterns" are design elements that are intended to "trick or manipulate users into making choices they would not otherwise have made and that may cause harm."[26] With respect to the covered minor, the final rule implements the Act's parental consent requirement,[27] which ultimately facilitates communication between minors and parents.

Accordingly, OAG makes no changes in response to this comment.

1. Valid Consent: Section 700.1(ii)

Theme: **Commenters requested an express allowance for covered operators to "bundle" a request for consent to an addictive feed or nighttime notifications with other requests.**

Some commenters proposed amending section 700.1(ii) of the rule to remove subsection two, which requires that consent be "specific"—presented separately from any other request by the covered operator—out of concern that this subsection was overly prescriptive, stifles innovation in consent mechanisms, and may make it harder for a parent or covered minor to grant consent. As explained in Part III.A.34 of the NPRM, OAG has aligned the definition of "valid consent" with general principles of consent recognized in several areas of law and multiple jurisdictions, as well as considering the best approach for providing a parent or covered minor with clear choices. Consent technology generally is flourishing, as observed in Part III.B.4.a of the NPRM, while wide adoption of these principles continues.

---

[25] *See* Part III.A.34 of the NPRM.

[26] Fed. Trade Comm'n, *Staff Report: Bringing Dark Patterns to Light* 2 (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20- %20FINAL.pdf. Research outlined in Part II.B of the NPRM also demonstrates that addictive feeds and nighttime notifications are designed to undermine a minor's self-control and thus their ability to make reasoned decisions about their use of these features.

[27] Additionally, as noted in Part II.2.B.2 of the NPRM, even reduced exposure to these features resulted in improved mental health for individuals.

Moreover, as noted by other commenters, allowing a covered operator to bundle requests for consent with other requests can result in "dark patterns" and otherwise undermine an individual's ability to grant valid consent.[28] As one commenter responding to the ANPRM observed, prioritizing how quickly or efficiently an individual completes an online consent flow often works against the interests of the individual and may not result in truly informed decision-making.

Accordingly, OAG makes no changes in response to these comments.

Theme: **Commenters weighed in on the requirement in section 700.1(ii)(3) and whether it arguably requires that requests for consent be simultaneously displayed in multiple languages.**

One commenter interpreted proposed section 700.1(ii)(3) to require a covered operator to not only translate notices into the 12 required languages, but to simultaneously display all language versions to a user. This part of the subsection is adapted with very minor wording changes from G.B.L. § 1506(1). The OAG does not interpret the Act as requiring, nor did it intend for the rule to require simultaneous notice in 12 languages. As discussed in Part III.A.34 of the NPRM, the objective is to ensure that an individual is presented with any notices in terms they can easily understand. This principle extends to the language of the notice, recognizing, as do many other New York laws, that New York State is home to diverse communities. A simultaneous display of the same notice is unnecessary as long as the notice is available in the required languages and easily accessible to a user.[29]

To clarify the requirement, OAG adopts a minor wording change to section 700.1(ii)(3) of the final rule by substituting the word "provided" in the second sentence with "made available." This change also more closely aligns this subsection with G.B.L. § 1506(1).

2. Subsections of 700.2(e) and 700.3(e)

Theme: One commenter suggested the final rule provide express instructions on how a covered operator should address a change in a covered minor's parent to a new individual.

Commenters generally supported the flexibility provided by the proposed definition of "parent" in section 700.1(cc) of the rule, both for implementation by covered operators and in addressing non-traditional household arrangements. One commenter suggested that the final

[28] *See* Fed. Trade Comm'n, *Staff Report: Bringing Dark Patterns to Light* at14-18.

[29] The OAG also directs covered operators to Part III.A.31 of the NPRM, which discusses how an operator may filter content based on a user's language setting under the definition of "technical information concerning a user's device."

rule include instructions on how a covered operator should address situations where a covered minor's identified parent may change.[30]

The OAG is sensitive to the realities of non-traditional households, and as explained in Parts III.A.28 and III.B.4.b of the NPRM, so too is the final rule. The definition of "parent" contemplates that more than one individual may qualify as a "parent" to a covered minor and have the right to grant consent on behalf of that minor. Sections 700.2(e)(2) and 700.3(e)(2) ensure that a parent has access to a simple mechanism to withdraw consent at any time, and sections 700.2(e)(5)(iii) and 700.3(e)(5)(iii) apply a flexible standard to guide a covered operator on how to determine whether an individual is a "parent" to the covered minor. These provisions, along with the "parent" definition, allow a covered operator to have policies and processes for addressing the various circumstances under which a covered operator identifies an individual as a "parent."

Multiple approaches to such situations are possible and the appeals process outlined in section 700.6 may be an appropriate method of resolution in some cases. However, OAG concludes that requiring specific outcomes and accounting for all potential cases related to questions about an individual's status as a "parent" through rulemaking is not necessary for creating an effective verifiable parental consent mechanism, nor would it be practical and thus, OAG declines to do so.

Accordingly, OAG makes no changes in response to this comment.

Theme: Some commenters suggested sections 700.2(e)(1) and 700.3(e)(1) should not involve covered minors in the process of requesting consent from parents.

Several commenters supported the verifiable parental consent process outlined in the rule as both consistent with the Act and a sensible approach that allows covered minors to be part of the decision-making process. Commenters supported the rule's approach because it ensures that parents and covered minors discuss how to appropriately use online platforms, which encourages the development of autonomy and digital literacy in a minor. By expressly providing the covered minor with a choice about accessing an addictive feed or nighttime notifications, these provisions help families to collaboratively make informed decisions.

A few commenters[31] argued the rule should be modified to allow operators to seek parental consent without a request or consent from the minor. The OAG disagrees. Without this requirement, a covered operator can limit access to its platform to only those minors who are willing to have a parent contacted for consent. The suggested change would not only require

[30] The proposal focused on section 700.2(e)(2) of the rule. However, as the issue ultimately turns on the potential of multiple individuals to satisfy the definition of "parent" under the final rule, OAG discusses the comment in relation to both sections.

[31] In addition to several comments submitted by organizations, nine commenters submitted what appears to be a form comment, which raised substantively identical objections against this approach. The OAG addresses all such comments here.

the minor to provide the operator with contact and other information about a parent, it would also reveal minors' use of a covered platform to a parent and would prompt the parent to grant access to addictive feeds and nighttime notifications even where the minor did not wish to access them. Accordingly, the OAG finalizes these sections as proposed.

Theme: According to some commenters, the rule's verifiable parental consent process conflicts with the Act or other laws.

Some commenters argued the verifiable parental consent process outlined in the rule conflicts with the Act or other statutes. The OAG disagrees.

Some commenters suggested the final rule is inconsistent with the Children's Online Privacy Protection Act ("COPPA"). The OAG disagrees. As explained in Part III.B.4.a.ii of the NPRM, sections 700.2(e)(6) and 700.3(e)(6) of the rule address any potential overlap with COPPA, which only exists for individuals who are under the age of 13.[32] Specifically, for individuals under the age of 13, the FTC expressly allows several methods of consent in which a child participates in the process, such as the "email-plus" method where a child enters a parent's email before a request is sent to the parent.[33] If the child does not enter the parent's email, the request for parental consent cannot be sent. To the extent some covered operators may be required to comply with both laws, Part III.B.4.b in the NPRM addresses how they may do so consistently and the comments do not alter that analysis.

A few commenters asserted that the rule's verifiable parental consent process should be consistent with the Family Educational Rights and Privacy Act and its implementing regulations (collectively, FERPA). These commenters did not provide any examples of an operator who potentially has to comply with both laws or explain why the processes should be consistent. In any case, OAG also considered FERPA when drafting the final rule[34] and concludes requiring FERPA's consent process, which governs sensitive, personally identifiable information and has specific signature requirements, would not best serve the context of access to addictive feeds and nighttime notifications. Moreover, OAG expects far fewer covered operators will need to comply with both FERPA and the Act, compared to COPPA.

One commenter argued that involving covered minors in the verifiable parental consent process contradicts the Act itself. The OAG disagrees. G.B.L. §§ 1501(1) and 1502 require the covered operator to obtain verifiable parental consent only if a covered minor wishes to access an addictive feed or nighttime notifications. Under sections 700.2(b) and 700.3(b), the covered operator is not required to provide these features to covered minors at all. Moreover, the Act's preamble makes it clear that the Legislature did not intend to grant unilateral control of a covered minor's activities on an online platform to the parent, stating that the Act "still

[32] Unlike the Act, COPPA does not apply to individuals aged 13-17. *Compare* 15 U.S.C. §§ 6501(1) *with* G.B.L. § 1500(6).
[33] 16 C.F.R. §§ 312.5(b)(2)(viii), 312.5(c).
[34] *See* Part III.A.28 of the NPRM.

permit[s] minors to view non-addictive feeds and any content available on [the] platform." Similarly, G.B.L. §§ 1501(6) and 1503 clarify that except as expressly specified, it is not intended to give parents "any additional or special access to or control over the data or accounts of their child." Accordingly, the final rule allows a covered minor to confirm whether or not they wish to access an addictive feed or nighttime notifications in the first place, and accordingly to decide whether to trigger the parental consent process.

Theme: Some commenters argued a parental consent process that does not involve minors is easier and better.

Some comments suggested removing the covered minor from the verifiable parental consent process because it would make it as "easy" as possible for a covered operator to obtain consent from the parent. One commenter further suggested a parent who has denied a request for consent should be able to independently initiate a new request in order to change their earlier choice. But these proposals would allow the parent to make changes to a covered minor's account without the covered minor's knowledge or confirmation that they even wish to access these two features.

One commenter suggested without evidence that a covered minor may be unreasonably afraid to confirm a covered operator can contact their parent. As discussed in Part IV.D.2 of the NPRM, research demonstrates that many minors would welcome more tools allowing them to manage platform features, including the two at issue, and already discuss their use of online platforms with parents. Moreover, even if these proposals were adopted, in many cases the covered operator may still need to ask the covered minor for their parents' contact information in order to send the parent a request. To the extent a covered minor fears having a covered operator contact their parent, the rule allows them to avoid it by forgoing an addictive feed and nighttime notifications.

Some commenters expressed concerns that sections 700.2(e) and 700.3(e) would be burdensome because a family would have to go through the process for "every" online platform and "every" feature that the covered minor wishes to use. Individualized consent is a key component of the Act and critical to the minor user's agency in deciding whether to request parental consent as well as the parent's ability to grant or deny that consent. Sections 700.2(b) and 700.3(b) of the rule also allow a covered operator to choose to not implement any method of verifiable parental consent. A covered operator may remove access to addictive feeds and nighttime notifications for all minors, and some covered operators likely will opt for this approach over implementing methods of verifiable parental consent. This will reduce the number of addictive online platforms requiring a covered minor and a parent to undergo any method of verifiable parental consent.

Accordingly, OAG makes no changes in response to these comments.

Theme: Some commenters suggested that parental consent to access an addictive feed or nighttime notifications should not be indefinite, consent should have to be re-affirmed by the parent or expire after a defined time period.

Some commenters expressed concern that a grant of parental consent may be indefinitely valid and would not allow parents to withdraw their consent as they see fit. That is not the case. Sections 700.2(e)(2) and 700.3(e)(2) require a covered operator to offer a mechanism to withdraw consent at any time. Such a mechanism must be as easy to use as the mechanism used to grant consent.[35] The OAG emphasizes to covered operators that making it difficult for a parent to access the mechanism to withdraw consent, or otherwise employing dark patterns to draw less attention to it compared to the mechanism to grant consent, is a violation of the final rule and the Act.[36]

One commenter expressed the opposite concern: if a parent had previously refused consent, both parents and covered minors would be disadvantaged if a covered operator was not permitted to send parents annual reminders that they can change their mind. Again, OAG concludes that sections 700.2(e)(3) and 700.3(e)(3) reflect an approach that best balances respect for a parent's wishes and safety of the mental health of children with the covered operator's interest in obtaining consent. The covered operator can provide a mechanism for changing the consent decision, but cannot press the parent[37] without the affirmative involvement of a minor who would like to send another request to the parent.

Accordingly, OAG makes no changes in response to these comments.

Theme: Commenters provided feedback on the notice required by sections 700.2(e)(4) and 700.3(e)(4).

While several commenters suggested that sections 700.2(e)(4) and 700.3(e)(4) of the rule be modified or expanded, commenters differed as to their proposed changes.[38]

Some commenters proposed that these sections require a covered operator to include additional information, such as further information regarding the risks posed by a specific platform feature or general information on the covered operator's data collection practices. The OAG supports transparency, and the rule does not prevent a covered operator from providing this information, including during the verifiable parental consent process. In addition, to the

[35] This also addresses the suggestion of one commenter, who proposed that the final rule ensure any grant of consent is fully revocable

[36] Parts III.A.34 and III.B.4.b of the NPRM also discuss in more detail the prohibited use of "dark patterns" in subverting a parent's (or a covered minor's) ability to grant valid consent.

[37] The OAG also reminds covered operators that abusive use of reminders, also known as "nagging," has been recognized as a "dark pattern" by the FTC. Fed. Trade Comm'n, *Staff Report: Bringing Dark Patterns to Light* at 14-16, 18.

[38] One commenter suggested that a "plain language" requirement be applied to the notice. This requirement is included in sections 700.2(e)(4)(iii) and 700.3(e)(4)(iii) of the rule, as well as incorporated into the definition of "valid consent" in section 700.1(ii)(3).

extent that any information is required under other laws applicable to a covered operator, section 700.7(e) ensures that a covered operator must continue to comply with such laws.[39]

However, OAG declines to require this additional information in the notice specified by sections 700.2(e)(4) and 700.3(e)(4). With respect to information about specific platform features or the risks associated with them, as explained in Part III.B.4.b.i of the NPRM, the notice requirements target the basic information a covered minor or a parent can use to make a decision about accessing an addictive feed or nighttime notifications. Disclosures for valid consent must balance substance that may be useful with individuals' ability to understand, retain, and process the most relevant information. Also, as observed by other commenters, overwhelming a covered minor or parent with extraneous information in a single notice is a well-recognized "dark pattern" that often undermines their ability to grant valid consent.[40]

The same is true with respect to disclosures related to a covered operator's data collection practices during the verifiable parental consent process. Here, OAG also emphasizes that a covered operator may not rely solely on the notice required under sections 700.2(e)(4) and 700.3(e)(4) to satisfy its obligations under the data protection safeguards in section 700.7(a) of the final rule. For example, a covered operator cannot simply state in the notice that it collects certain data types for verifiable parental consent and then claim this disclosure is sufficient to meet its obligation to collect the minimum types of data necessary under section 700.7(a)(1). The covered operator must conduct an analysis of what data types are and are not necessary to operate a method of verifiable parental consent, and then limit its collection to the necessary types.

Finally, a few commenters suggested that the translation requirement in sections 700.2(e)(5)(i) and 700.3(e)(5)(i) be relaxed to lighten the burden on covered operators. These subsections simply restate G.B.L. § 1506. However, to clarify how a covered operator may satisfy this obligation and ensure consistency with the equivalent requirement in the rule's definition of "valid consent," OAG adopts a minor language change in the final rule by substituting the word "providing" with "making available." The OAG provides further clarification on the translation requirement in its response to comments regarding section 700.1(ii)(3).

Except for this non-material substitution for clarity, OAG makes no changes in response to these comments.

Theme: Commenters suggested the final rule should allow for diverse methods of verifiable parental consent.

Some commenters supported a rule that was not limited to specific methods of obtaining verifiable parental consent, but that allowed a covered operator to flexibly consider a

[39] For example, a covered operator may need to consider if it should provide a separate notice under the requirements of the Child Data Protection Act for any data collection about a covered minor that is not "strictly necessary." G.B.L. § 899-ff(2).

[40] Fed. Trade Comm'n, *Staff Report: Bringing Dark Patterns to Light* at 22-23.

range of methods based on its specific user base and online platform, as well as technological innovation. Sections 700.2(e)(5) and 700.3(e)(5) of the final rule take this approach, outlining general requirements that a method must account for and allowing for the development of new methods. Several comments, including commenters with expertise in parental consent technology, commended the rule as embracing the diverse range of methods already available, and in particular, approvingly cited sections 700.2(e)(5)(vi)-(vii) and 700.3(e)(5)(vi)-(vii) for not limiting parents to methods where they must present government identification or make an account.

Accordingly, OAG makes no changes in response to these comments.

Theme: One commenter stated the final rule should not require age assurance to be performed on the parent.

One commenter argued that the age assurance requirement in sections 700.2(e)(5)(i) and 700.3(e)(5)(i) exceeds OAG's authority under the Act and creates privacy and security risks for parents. G.B.L. § 1501(4) gives OAG discretion to draft rules regarding methods of verifiable parental consent. The Act does not limit OAG to specific methods of determining whether an individual is in parental relation to the covered minor and OAG finds that determining the individual's age status using a highly effective method, while not sufficient on its own, is a relevant data point for ruling out individuals falsely representing themselves as having a parental relationship with a minor. The Act imposes no constraints on using age assurance as part of verifiable parental consent, and G.B.L. §§ 1501(a) and 1502 specifically identify age assurance as a way to determine who is over and under the age of 18.

With respect to privacy and security risks, section 700.7(a) of the final rule imposes stringent data protection safeguards on all data collection under the rule, including data collection related to age assurance as part of verifiable parental consent. The OAG addresses this issue in more detail in its response to comments on section 700.7(a).

Accordingly, OAG makes no changes in response to these comments.

Theme: One commenter argued the final rule should expressly prohibit the use of biometric data or payment card information in a verifiable parental consent method.

One comment singled out parental consent methods using biometric data or payment card data as creating unique privacy and security risks and proposed banning such methods in the final rule. The OAG is sensitive to privacy and security risks to individuals. Sections 700.2(e)(5)(iv) and 700.3(e)(5)(iv) of the rule specifically require a covered operator to make "reasonable efforts" regarding privacy and safety as part of implementing an acceptable verifiable parental consent method. The rule further addresses these risks for all parental consent methods by requiring strict data protection safeguards under section 700.7(a). If a method of verifiable parental consent cannot meet these standards, the covered operator may not use that method. To the extent biometric or payment card data can be used in compliance

with the safeguards required by the rule, OAG concludes they are potential methods a covered operator may choose. Thus, OAG declines to list these as specific prohibited methods.[41] The commenter also was concerned that permitting methods based on payment card information would unfairly discriminate against individuals, typically low-income or undocumented, who do not have access to credit cards, debit cards, or bank accounts. Should such a method involve charging an irreversible fee to a covered minor or a parent, it violates sections 700.9(b) of the rule and G.B.L. § 1504, similar to examples discussed in Part III.I of the NPRM. To the extent that a method relying on payment card information does not require an irreversible fee and the covered operator determines it complies with all other requirements of the rule, the covered operator may still conclude that not all of its users can access this method. But this is true of any method a covered operator may consider. The OAG encourages covered operators to consider "waterfall" approaches that combine several methods to reduce burdens on users while providing them with options, similar to what is discussed in Part III.D.2.b of the NPRM. Additionally, sections 700.9(b) of the rule and G.B.L. § 1504 do not permit the covered operator to deny an individual general access to an online platform simply because that individual does not complete the verifiable parental consent process and section 700.6 requires an appeals process to prove adult status.

Accordingly, OAG makes no changes in response to these comments.

Theme: Commenters suggested the final rule should be more prescriptive about the requirements for methods of verifiable parental consent.

Commenters suggested that the final rule include more prescriptive requirements for methods of verifiable parental consent, centering largely around sections 700.2(e)(5)(iii)-(v) and 700.3(e)(5)(iii)-(v). Several comments proposed more detailed requirements for the types of proof a covered operator would need to collect and retain regarding parental consent, pointing to section 700.7(b) as a potential model.

The OAG reviewed the suggestions carefully and concludes that the requirements and standards finalized balance accountability and clarity with flexibility for covered operators and the evolution of consent technology. As noted herein, OAG recognizes the variety of circumstances surrounding adults in parental relation to children. The standards in sections 700.2(e)(5)(iii)-(v) and 700.3(e)(5)(iii)-(v) allow for covered operators to best develop a parental consent method appropriate for their minor user population while still ensuring robust protection of covered minors.

[41] Use of payment card information has been recognized by the FTC as an acceptable method of verifiable parental consent when complying with COPPA. 16 C.F.R. § 312.5(b)(2)(ii). As discussed at length in Part III.B.4.b.iii of the NPRM, a covered operator may consider FTC-approved methods of verifiable parental consent for use under the Act but must determine whether the method can also satisfy the limited additional requirements of sections 700.2(e)(6) and 700.3(e)(6) of the rule.

Additionally, the OAG declines to add a certification requirement for verifiable parental consent methods and, thus, it is not necessary to include explicit record retention requirements specific to parental consent other than the age assurance portion of the method. For any age assurance, including age assurance conducted for purposes of parental consent, covered operators must comply with the recordkeeping requirements in section 700.7(b). As a general matter, the covered operator carries the burden of proving that it is complying with the Act and the final rule, including proving that it has taken "reasonable efforts" to protect the covered users' and parents' privacy and safety under sections 700.2(e)(5)(iv) and 700.3(e)(5)(iv), and that it collected valid consent from a parent.[42] If a covered operator is unable to provide such proof and still chooses to provide a covered minor with access to an addictive feed or nighttime notifications, the covered operator has not satisfied its obligations.

Accordingly, OAG makes no changes in response to these comments.

Theme: Commenters suggested the final rule should be more specific around what types of proof are acceptable to demonstrate that an individual is a "parent."

Two commenters[43] expressed concern that the standard outlined in the rule, namely sections 700.2(e)(5)(iii) and 700.3(e)(5)(iii), is not specific enough to be easily implementable. However, commenters representing parental consent technology companies expressed confidence that this standard is both implementable and already reflected the capabilities of existing technology. A commenter representing technology companies potentially subject to the Act also supported the rule's flexible approach to defining "parent."

The "reasonably calculated" standard for determining a parent is identical to the standard outlined in the COPPA Rule as far back as 1999.[44] Operators have been able to implement this standard and no commenter has submitted direct evidence that a covered operator cannot successfully adopt it for the purposes of the Act.

Accordingly, OAG makes no changes in response to these comments.

---

[42] Several commenters also suggested that the rule specify the types of data that a covered operator should retain with respect to the non-age assurance portion of a verifiable parental consent method. Given the diversity of potential methods and of potential relationships acceptable under the rule's definition of "parent," the rule allows the covered operator to determine which types of data should be collected and retained as proof of valid consent by the parent. Giving covered operators this flexibility also helps ensure that the rule supports innovation and development of new verifiable parental consent methods, as discussed in Part III.B.4.ii of the NPRM. However, OAG reminds covered operators that at all times they must comply with section 700.7(a) of the rule, including the data minimization requirement.

[43] Comments addressing age assurance methods as applied in the parental consent context are addressed in together with other comments addressing age assurance.

[44] 64 Fed. Reg. 59888, 59914 (Nov. 3, 1999). No version of the COPPA Rule has taken the approach suggested by commenters. 16 C.F.R. § 312.5(b)(1); *see also* Fed. Trade Comm'n, *Complying with COPPA: Frequently Asked Questions*, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions (section I.4 observing that the specific methods of verifiable parental consent listed in 16 C.F.R. § 312.5(b)(2) is "non-exhaustive").

Theme: A commenter urged clarification in the final rule about whether a parent can be required to create an account to complete verifiable parental consent if the parent has declined to provide government identification as part of the process.

One commenter sought clarification regarding whether sections 700.2(e)(5)(vi)-(vii) and 700.3(e)(5)(vi)-(vii) of the rule should be read as separate, independent requirements, or should be read as alternatives. The use of the conjunctive "and" between these subsections indicates that covered operators should read them as separate and independent. A covered operator cannot force a parent to create an account to complete verifiable parental consent, regardless of what other methods of verifiable parental consent are offered by the covered operator.

Theme: Some commenters suggested the final rule adopt the verifiable parental consent methods approved by the FTC for complying with COPPA as appropriate for all covered minors.

Some commenters proposed merging sections 700.2(e)(5)-(6) and 700.3(e)(5)-(6) to create a single unitary standard for verifiable parental consent based on the list of specific verifiable parental consent methods approved by the FTC in 16 C.F.R. § 312.5(b)(2). Commenters argued that such a standard would be less burdensome for covered operators. Other comments support the rule's approach, which addresses the use of these methods for covered minors under the age of 13 in sections 700.2(e)(6) and 700.3(e)(6) and further permits covered operators to consider whether these methods may satisfy the requirements in the rule, but does not limit them to these methods. Commenters supporting the final rule noted that several of the methods approved by the FTC are outdated and may be more vulnerable to circumvention than newer methods.

G.B.L. § 1507(2) expressly addresses covered operators who must comply with COPPA. However, COPPA applies only to children under the age of 13[45] and does not address verifiable parental consent (or any other issue) for covered minors aged 13-17, as the Act does. A unitary standard does not benefit covered operators who are not currently required to comply with COPPA.

Furthermore, Part III.B.4.b.iii of the NPRM carefully considered the FTC's treatment of verifiable parental consent methods for both covered minors under the age of 13 and aged 13-17, including the relative burden on covered operators who must comply with both laws, the likelihood that the FTC accounted for differences presented by older covered minors, circumvention concerns, and the best way to encourage technical innovation. The NPRM offers detailed guidance to covered operators as to how they can adapt existing COPPA-verifiable

[45] 15 U.S.C. § 6501(1) (defining "child" as "an individual under the age of 13").

parental consent methods with only incremental effort to comply with the rule.[46] Comments submitted did not point to other issues specific to compliance with both COPPA and the rule.

Accordingly, OAG makes no changes in response to these comments.

Theme: Commenters addressed timing of the review of verifiable parental consent methods.

Several comments supported the rule's annual review cycle. Some commenters proposed adjusting sections 700.2(e)(7) and 700.3(e)(7) of the rule to allow a covered operator to review verifiable parental consent methods on an alternative cycle, primarily to alleviate compliance burdens. Some proposed a three-year cycle, while others proposed the use of "risk-based" approach.

As an initial matter, a "risk-based" approach does not provide clarity to covered operators about when they should review their verifiable parental consent methods. As discussed in Part III.B.4.b.iv of the NPRM, regularly timed reviews help a covered operator ensure that their chosen method continues to comply with the rule and accounts for technological developments. Given significant leaps in technology that can occur over the course of one year, OAG concludes the one-year cycle balances compliance burden with the goals of the Act.

Moreover, the requirement does not mean that a covered operator will need to invest resources in updating the method each year, only that a covered operator must assess whether or not such an investment is needed. Covered operators regularly review their products and services for many different reasons including, but not limited to, legal compliance, so OAG does not expect this requirement to impose a significant burden, as discussed in its economic analysis in Part IV.D of the NPRM. No commenter has provided concrete evidence, such as increased costs specific to the annual review requirement, in support of their contention.

Commenters suggesting a longer review cycle, such as three years, have not provided any evidence that these longer cycles will ensure a covered operator timely updates its methods in accordance with the requirements of the rule. Again, given the pace of technological innovation, OAG is concerned—as are other commenters—that a longer review cycle would detrimentally affect the privacy and safety of covered users and parents, among other potential negative effects.

Accordingly, OAG makes no changes in response to these comments.

G. Data use and protection: Section 700.7

[46] One commenter requested that OAG clarify how the rule applies to a specific COPPA verifiable parental consent method, commonly known as the "email plus" method, which the commenter asserts is particularly prone to circumvention. Footnotes 83 and 84 of the NPRM address this method in context of circumvention issues. In addition, OAG reminds covered operators that to utilize sections 700.2(e)(6) and 700.3(e)(6) of the rule, they must expressly consider circumvention, fraud, or misuse issues under subsection (ii).

1. General privacy risks

The OAG received comments expressing concerns about privacy risks related to the collection, analysis and deletion of data attendant to the performance of age assurance and parental consent. For the reasons below, OAG adopts the standards in the proposed rule for the collection, analysis and deletion of data, because they are sufficiently robust to address the concerns raised, and proposes a small number of minor changes for clarity.

Theme: Commenters raised general privacy concerns.

A number of commenters noted that in spite of the privacy protections in the rule, any collection of data carries privacy and security risks; these commenters took the position that age assurance and parental consent review are inherently objectionable due to these inevitable risks, regardless of the extent to which the risks are minimized. None of the commenters suggested alternative measures to address this generalized concern.

As noted in the Act's preamble, the Legislature recognized that balancing the concerns of various stakeholders, such as covered operators and users, with the goals of the Act is a complex and technical matter. Accordingly, it delegated authority to OAG to promulgate regulations that consider these concerns and apply a flexible, informed approach to resolving them. In turn, OAG issued an ANPRM that, among other topics, solicited comments on data privacy and security in connection with the Act. It carefully considered all responses in drafting the proposed rule, which imposes strong data use and protection safeguards on all information collected in connection with the Act.

The OAG acknowledges the fact that data collection creates risks but declines to change the requirement that operators collect information necessary to conduct age assurance or review parental consent. To minimize data-related risks, the rule mandates practices including the requirement that operators collect no more data than is necessary to perform the required function and delete that data as soon as the function has been completed. If a covered operator violates any of these subsections, it risks investigation and enforcement.

Theme: Some commenters sought privacy standards for each age assurance method.

The OAG received two comments urging that the final rule include an explicit directive that operators use the highest available privacy standards for each age assurance method they provide. The comments argued that this added directive would further emphasize the importance of data protections in the rule.

The proposed rule contains numerous provisions that protect data privacy. For example, proposed section 700.7(a) mandates that all data collected for compliance with the rule "shall be the minimum necessary to comply" (700.7(a)(1)), "shall not be used for any other purpose" (700.7(a)(2)), "shall be collected and stored using industry-standard data security measures," (700.7(a)(3)), and "must be immediately deleted" following the minimum time needed to

comply with the rule (700.7(a)(4)). These obligations apply regardless of the age assurance method or methods used by the operator. The OAG recognizes that operators' platforms vary considerably in the nature of the user experience and interactions with different aspects of the platform. Applying uniform, privacy-preserving standards allows operators to customize their age assurance program while establishing a consistently high standard that protects all users. After carefully considering the points raised in the comments, OAG does not believe it adds privacy protection to further direct operators to adopt method-specific privacy standards, and doing so may reduce the clarity of the rule's directives regarding privacy and security.

Theme: One commenter suggested privacy and security provisions in section 700.7 should apply to third parties.

One commenter expressed concern that section 700.7 does not expressly require third-party vendors to maintain the same privacy standards as operators. The comment asked that OAG create binding and enforceable obligations directly on third parties that handle user data.

The scope of the Act and OAG's statutory mandate does not include direct enforcement authority with respect to third parties. However, the rule addresses third-party actions concerning data where the third parties are acting at the behest of the operator. Specifically, while section 700.7 does not expressly reference third-party vendors acting on behalf of operators, section 700.9(a) makes clear that "all requirements herein apply equally to covered operators that elect to engage or otherwise rely upon any third-party to comply with this Part." It is, therefore, incumbent on operators to ensure any third-party entities acting on their behalf adhere to all obligations in the rule, including the data-related obligations in section 700.7. Should a third-party vendor fail to meet the obligations in section 700.7, OAG will consider that failure to be the same violation as if the act or omission were committed by the operator.

Theme: Comments addressed the scope of section 700.7 and its application to data collected by operators.

Some comments suggest that section 700.7 as proposed, including the general data use and protection principles outlined in section 700.7(a), only applies to age assurance data. Consequently, they raise concerns that other information collected in connection with the Act, such as non-age assurance parental consent data, is entirely unprotected.

Section 700.7 as originally proposed was not so limited, referring consistently to data collected in connection with "this Part," where "Part" refers to the entire rule and not to merely the sections on age assurance. This section is intended to implement a data use and protection framework for all information collected in connection with the Act. To further remove any ambiguity, OAG adopts two clarifications.

One, it modifies section 700.7(a), which previously specified that it applied to "data collected for the purpose of complying with this Part," to specify that it applies to "data

collected for the purpose of complying with any section of this Part." As noted, "Part" refers to the rule as a whole.

Two, OAG modifies references to "this Part" in subsections (a), (b), and (d) of section 700.7(a) to instead refer to "the applicable section of this Part." This modification helps clarify that a covered operator should consider how each general data use and protection principle functions in light of the section of the proposed rule under which it is collecting information.

Theme: Commenters suggested the final rule include a minimum necessary standard and require self-declaration as part of that standard.

A small number of comments made requests related to the requirement in 700.7(a) that data collected to comply with the rule "shall be the minimum necessary to comply with this Part; . . . ." Commenters asked that this language be further clarified or amended to mandate or prohibit actions by operators in the interest of data protection. One commenter representing operators requested that a "reasonableness" qualifier be added to the standard to give operators more flexibility to collect data in their discretion. Following careful consideration of these comments, for the reasons below, OAG adopts the "minimum necessary" standard as proposed and declines to mandate further action by operators.

One comment urged OAG to adopt, as part of the "minimum necessary" standard in 700.7(a), the requirement that all operators request self-declaration of age status prior to engaging in any additional age assurance method. According to the comment, this additional requirement would allow all minors the opportunity to avoid engaging in further age assurance by self-declaring minor age status, in accordance with section 700.4(a)(1).

After consideration of this request, OAG declines to mandate the sequencing of age assurance methods, recognizing that the most appropriate, effective, and fraud-preventative age assurance method for a user may depend upon the individual platform or the individual user. For example, some operators may choose to employ age inference as an initial age assurance method, using data already in the operator's possession, without contemporaneous notice to the user. For other users, the timing of an operator's request for self-declaration may be impacted by minimizing user friction or fraud prevention measures.

While OAG will not mandate particular assurance methods or a sequence in which multiple methods should be employed, instead allowing operators to make this determination in accordance with the obligations in the rule, OAG does expect operators to take the "minimum necessary" standard in 700.7(a)(1) into account in designing and executing an age assurance program. Absent extenuating factors, operators should choose and prioritize age assurance methods that require the minimum amount of data to determine a user's age status.

Theme: Commenters suggested that an operator should not be able to maintain the estimated age of users.

One commenter asked OAG to reconsider section 700.7(c), which allows an operator to collect and retain a covered user's estimated age "solely to determine age status for purposes of this Part with the covered user's valid consent." The comment expressed concern that retention of estimated age data could increase data security risks and posited that estimated age is not necessary for determination of age status.

In determining exceptions to the data minimization and deletion requirements of section 700.7(a), OAG carefully considered the corresponding benefits and risks of limited data retention. While data minimization is an important feature of the rule, in limited instances some data retention is allowed or required where the benefits outweigh the risks. With respect to a minor user's estimated age, OAG does not require the collection or retention of this information but does allow it for minor users. The OAG concluded that the security risks from this data retention are relatively low – importantly, estimated age or age range does not pose the same security risks as a user's birthday, which is not within the scope of the data deletion exception in section 700.7(c). The OAG also took into consideration the requirements in section 700.7(a)(3) that such data be stored "using industry-standard data security measures."

Retaining a minor's estimated age or age range benefits both operators and users by allowing operators to estimate when a minor user might reasonably attain adult status. Because operators are obligated, under to section 700.4(d)(4), to provide minor users with a process to update their age status upon reaching the age of 18, which then requires the operator to complete age assurance for that user, the knowledge that a user is or is not likely to reach adult status within a certain time period allows operators to craft appropriate communications with the user and prevents minor users from being asked to update their age status with unnecessary frequency. Should the covered user prefer that the operator not retain their estimated age, the covered user can deny or rescind consent for such retention. Based on these factors, OAG adopts the limited retention of estimated age data set forth in section 700.7(c).

Theme: Commenters addressed visibility of user behavior by ID issuers and third-party data owners.

A few commenters asked OAG to mandate that the issuer of any credentials that serve as confirmation of age status, such as an agency issuing government-issued identification, be prohibited from learning the identity of the operator requesting confirmation of a user's age status via those credentials. The comments seek to prohibit such issuers from developing a cache of information regarding the user's online activities. The OAG declines to issue such a blanket mandate as doing so may limit the commercially reasonable and technically feasible age assurance options available to operators. But OAG notes a few factors that mitigate risk to user privacy. First, presentation of government-issued identification by a user does not require the operator to confirm the identification with its issuer unless it is necessary to ensure the method meets the applicable accuracy thresholds. Second, users who are concerned about any risks

associated with the identification issuer will have the option to choose an offered method other than government-issued identification, unless the ID verification is a zero-knowledge proof age assurance method, in which case identification issuers will not know the identity of the requesting platform. Third, section 700.7(e) states that a covered operator "must comply with all other applicable data protection and security laws," including laws governing accurate disclosures regarding the operator's transmission of user data.

The OAG also considered comments that raised data privacy concerns related to the sharing of user identity data with third-party data owners such as banks or credit card issuers in conducting age assurance, and one comment raising similar concerns related to operators obtaining user age status data from other operators or the same third-party source as other operators. The OAG concludes that these concerns are adequately addressed by the data protection, data minimization, and operator liability requirements in section 700.7 and declines to modify those requirements.

Theme: One commenter argued to add a reasonability qualifier for "minimum necessary" data collection.

The OAG received one comment stating that the language of 700.7(a), requiring that data collected be the "minimum necessary," be modified to add a reasonableness qualifier. In support of this point, the comment cited a limited number of state privacy laws, which use the phrase "minimum reasonably necessary" to describe an allowed scope of data collection. The comment argued that the current phrasing would allow OAG to penalize commercially reasonable data collection, offering as examples device information, language settings, and time zone data; the comment did not explain why this information would not be considered the "minimum necessary" to comply with the rule.[47]

Unlike a data privacy law, which addresses a wide range of potential data that may be collected for various purposes, the Act and the requirements of the rule address only a narrow scope of data collection by the operator to complete age assurance and parental consent. The data needed for these actions is specific to the age assurance and parental consent methods chosen by the operator. The single comment that raised this issue failed to establish categories of data that would be "reasonably necessary" to comply with the rule and yet not "necessary" per 700.7(a) or otherwise addressed by the rule. Given the importance of data minimization, the rule is intended to provide the clearest possible guidance to operators regarding the scope of acceptable data collection. It is not in the interest of operators or users to introduce ambiguity regarding the categories of data operators may acceptably collect. For this reason, OAG adopts the "minimum necessary" standard as proposed.

[47] Some of the data cited in the comment also may qualify as "technical information concerning the user's device," which is exempted from the definition of an "addictive feed." *See* section 700.1(c)(3)(i).

2. Delete: Section 700.1(p)

Theme: A commenter sought clarification that the definition of "delete" does not permit a covered operator to indefinitely retain data sets derived from information collected from a user in connection with the Act.

One commenter interpreted proposed section 700.1(p) of the rule to permit a covered operator to collect information from a user, create a new data set from the initial information, and delete the initial information without deleting the second, derived data set. This commenter suggested that the second data set would not be subject to either section 700.1(p) or to the general data protection requirements in section 700.7, because of the use of the word "or" between "remove" and "de-identify" in the proposed section 700.1(p). Multiple comments reviewing the same section interpreted it to mean the opposite, namely, that the "or" allows a covered operator to either permanently delete or remove data or to de-identify it, so if a covered operator wishes to retain any information, its only choice is to first de-identify it.

The OAG clarifies, consistent with the multiple comments referenced, that the word "or" as used in section 700.1(p) must be interpreted to prohibit evading the deletion requirement of the Act by creating a copy of data initially collected under the Act. G.B.L. §§ 1501(3) and (5) require a covered operator to "immediately delete" information collected in connection with age assurance or verifiable parental consent conducted under the Act, except as necessary to comply with state or federal law. Section 700.1(p) clarifies the meaning of "delete" in these provisions by offering one of three permanent approaches to covered operators: 1) destroy data; 2) remove data; or 3) de-identify data. Here, the conjunctive "or" acts to make the options mutually exclusive. Deriving a new data set does not fit into any of the three, and accordingly, a covered operator cannot circumvent section 700.1(p) by creating a new data set.

Moreover, section 700.7 of the rule applies to all data collected under the Act[48], and its subsection (a)(2) permits data to only be used for the purpose of complying with the Act. If a covered operator takes information initially collected under the Act and derives a second data set from this initial data, the process of deriving the second data set is subject to this purpose limitation, the same as any other use of the initial information by the covered operator. If a covered operator intends to use the derived data set for any purpose not related to the Act, then creating the derived data set is a violation of section 700.7(a)(2). It is not necessary for the rule to draw a distinction between information initially collected from a user and data that is later derived from the initial information. Creating a distinction is likely to confuse the covered

[48] The comment also interprets the rule to limit a covered operator's data deletion obligations to only information initially collected as part of age assurance. However, the deletion obligations in G.B.L. § 1501(3),(5) are not so limited. Accordingly, section 700.7(a)(4) of the rule, which implements these provisions, applies the same data protection principles to all data collected in connection with the Act, regardless of when it was collected or for what purpose.

operator into believing that different standards apply to each data set when in both cases, the covered operator must comply with the Act and final rule.

Accordingly, OAG makes no changes in response to these comments.

Theme: Some commenters stated the definition of "delete" should not include de-identification because including it is beyond the scope of the Act.

Some comments[49] objected to including "de-identification" as part of the definition of "delete" in section 700.1(p), arguing that allowing for "de-identification" is contrary to G.B.L. §§ 1501(3) and (5), because it does not require that all information collected from a user be permanently deleted.

G.B.L. § 1500 does not provide a definition for "delete." As used in subsections three and five of G.B.L. § 1501, this word is directly applied to data collected in connection with the age assurance and parental consent processes mandated by the Act.[50] Subsections two and four of this same section of the Act grant OAG authority to promulgate regulations specifying appropriate methods for carrying out these processes. Disposal of data is part of these processes and providing an explicit definition of "delete" in the final rule is well within the authority delegated to OAG.

The proposed definition also comports with the general objectives of the Act, which describes in its preamble how the Act's safeguards shall be implemented in a "commercially feasible and technically reasonable" manner.[51] Comments responding to both the ANPRM and NPRM noted that requiring data destruction or removal in all cases may prevent a covered operator from complying in good faith with the Act, as well as from responding to genuine user issues. Allowing a covered operator to retain de-identified data, but only after meeting stringent standards to protect user privacy, balances such operational concerns with user interests. Moreover, as explained in Part III.A.16 of the NPRM, it is widely acknowledged that commercially reasonable and technically feasible standards of online and digital data deletion commonly include de-identification.[52] This process is also recognized as a method of de-linking data from an individual in many state privacy laws.

---

[49] In contrast, one comment apparently misread section 700.1(p) to require immediate and "irretrievable destruction" of all copies of data and raised concerns that this would interfere with legitimate operational needs. "De-identification" as permitted under section 700.1(p) is plainly an alternative, and the comment fails to address why de-identification would be insufficient for any operational concerns that might require a covered operator to not immediately delete data.

[50] The OAG also notes that these subsections expressly contemplate that a covered operator may need to retain information "where necessary" to comply with federal and state laws, further supporting the proposed section 700.1(p).

[51] *E.g.* G.B.L. § 1501(2).

[52] One comment suggested that sections 700.5 and 700.7 of the rule obviate any practical need to include de-identification in section 700.1(p), since a covered operator need only retain data collected from its users under these sections. However, data collection under 700.7 clearly contemplates a process whereby the initial data collected likely does identify an individual or device, but is reduced to only a limited amount of retained data to

Accordingly, OAG makes no changes in responses to these comments.

Theme: Some commenters argued the definition of "delete" should exclude de-identification because de-identified information is at risk of being subjected to re-identification processes.

Some commenters objected to the inclusion of "de-identification" in section 700.1(p) because of the risk that de-identified information can be processed in the future to re-identify the user from whom it was collected. These comments cited several examples where a purportedly de-identified data set had been subjected to re-identification processes and the identity of individuals had been extracted from the data set. Other comments did not find the inclusion of "de-identification" to appreciably threaten the privacy of individuals, noting that this definition is paired with strong data protection and security safeguards in other provisions of the final rule.

The OAG acknowledges commenters' concerns. However, inadequately de-identified data, as in references cited by commenters,[53] likely fail to satisfy the rule's requirements. As discussed in Part III.A.16 of the NPRM, section 700.1(p) does not permit any type of purported de-identification process[54], but outlines specific, stringent standards that must be met to qualify as "de-identification" within the meaning of the rule, including that the covered operator must take "reasonable measures" to ensure de-identified information cannot be "re-linked with an individual or device" and to ensure that any recipients of such information take similar measures. In addition, a covered operator itself cannot attempt to re-identify or re-link the de-identified information. If a covered operator cannot meet these standards, then the covered operator has not met the definition of delete under the rule.

The OAG also notes that a covered operator has an ongoing obligation to ensure any de-identification process it uses meets the requirements of the rule. For example, if a covered

---

"document the operation" of an age assurance method, as discussed in Part III.G.2. While section 700.7(b) does not explicitly require that retained data be de-identified, a covered operator may de-identify this data in accordance with section 700.1(p), and indeed, is encouraged to do so (to the extent it is consistent with sections 700.5 and 700.7) under the data minimization principle embodied in section 700.7(a). These sections thus work together to encourage a covered operator to safeguard an individual's data. As for section 700.5, it addresses data collected in connection with the rule's mandatory certification process, which will not contain data collected from a covered operator's users and which is thus irrelevant to the concerns motivating G.B.L. §§ 1501(3),(5).

[53] Daniel C. Barth-Jones, *The 'Re-Identification' of Governor William Weld's Medical Information: A Critical Re-examination of Health Data Identification Risks and Privacy Protections, Then and Now*, Research Report (July 2012), https://ssrn.com/abstract=2076397 (examining re-identification using a publicly-available data set); de Montjoye, Yves-Alexandre, César A. Hidalgo, Michel Verleysen, and Vincent D. Blondel, *Unique in the Crowd: The Privacy Bounds of Human Mobility*, 3 Scientific Reports 1376 (2013) (examining re-identification using publicly-available data sets), https://doi.org/10.1038/srep01376.

[54] One comment cited to FTC guidance outlining how a specific technique called "hashing" does not de-link data from an individual or a device. Fed Trade Comm'n, *Technology Blog: No, hashing still doesn't make your data anonymous* (July 24, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/07/no-hashing-still-doesnt-make-your-data-anonymous. The standards outlined in this guidance for de-identification are consistent with section 700.1(p) of the rule, and OAG agrees that "hashing" as a standalone technique does not satisfy the rule's requirements.

operator is alerted that a purportedly de-identified data set can be re-identified, the covered operator should investigate and consider whether it needs to improve its existing measures against re-identification. Ignoring such a report would not be taking "reasonable measures to ensure that the de-linked information cannot be re-linked with an individual or device," and may prompt an OAG investigation.[55]

Additionally, the rule does not permit de-identified information, even if it meets all requirements, to be indefinitely retained or to be repurposed. Section 700.7 of the rule imposes several data protection safeguards, including data minimization principles, that apply to all data collected in connection with the Act. Similarly, subsection five of section 700.1(p) as originally proposed only permitted de-identified information to be retained as long as "necessary" to meet a relevant purpose under the rule and would not permit the information to be used for any other purpose. For clarity, OAG is modifying section 700.1(p) to state that de-identified information can only be held for the "minimum time necessary," which more closely aligns with the general data minimization principle embodied in section 700.7(a) and makes it clearer that the data protection standards outlined in section 700.7(a) continue to apply to de-identified information.

Except as stated, OAG makes no other changes in response to these comments.

Theme: Commenters suggested the definition of "delete" list specific methods besides de-identification.

Several comments proposed modifying section 700.1(p) to list additional specific methods to include in the definition of deletion, such as cryptographic erasure,[56] segregation from operational or commercial uses, and overwriting with random data. With one exception[57], the cited methods all appear to permit the retention of some data after processing. The comments did not provide supporting evidence to demonstrate all of these methods are widely accepted, either by covered operators or by recognition in relevant laws such as state privacy

[55] The OAG has a long and active record of investigating improper data collection and handling practices under both New York and federal laws. *E.g.*, OAG, *Press Release: Attorney General James and Multistate Coalition Secure $5.1 Million from Education Software Company for Failing to Protect Students' Data* (Nov. 6, 2025), https://ag.ny.gov/press-release/2025/attorney-general-james-and-multistate-coalition-secure-51-million-education, OAG, *Press Release: AG James: Google And Youtube To Pay Record Figure For Illegally Tracking And Collecting Personal Information From Children* (Sept. 4, 2019), https://ag.ny.gov/press-release/2019/ag-james-google-and-youtube-pay-record-figure-illegally-tracking-and-collecting.

[56] Commenters disagree on the nature of cryptographic erasure, with one comment asserting that this technique would not qualify as either deletion/removal or de-identification under section 700.1(p) as proposed and another describing this technique as a type of permanent deletion/removal of data, although data is still retained after the process is completed.

[57] One comment also proposed listing the physical destruction of storage media. This method already falls within the "permanently destroy [or] remove" language of section 700.1(p).

laws addressing deletion rights.[58] One comment also proposed that section 700.1(p) should limit covered operators to only methods of "deletion" expressly specified in the rule.

Section 700.1(p) provides a functional definition of "delete" that is not tied to methodology.[59] This approach provides a flexible rule that ensures the protections of the Act are not rendered moot by technological advances. Limiting a covered operator to specific methods could in the long run undermine the data protections of the rule.[60] For example, the security of cryptographic erasure depends on the type of encryption used, as older forms may be broken even without access to the encryption key.[61] Conversely, not listing a specific method does not mean that a covered operator is prohibited from using it, but only that the covered operator must first determine whether a given method meets the standards of section 700.1(p). Taking cryptographic erasure again as an example, if the covered operator can demonstrate that its implementation of the technique currently ensures information is removed from the covered operator's systems so that it cannot be retrieved and cannot be accessed or used without authorization, then the covered operator is complying with the rule.

Accordingly, OAG makes no changes in responses to these comments.

Theme: One commenter suggested that the definition of "delete" should clarify the deadline by which a covered operator must delete data collected under the Act.

One comment proposed amending section 700.1(p) to further clarify deletion deadlines, such as requiring deletion no later than 24 hours after completion of age assurance, requiring deletion "without unnecessary delay," and requiring the covered operator to meet the shortest deadline where feasible.

When referring to deletion, the Act consistently uses the word "immediately."[62] This obligation is implemented not only by section 700.1(p) but also by section 700.7(a)(4). "Immediately" is a commonly understood word that conveys a sense of urgency.

---

[58] In contrast and as noted in the NPRM, "de-identification" is recognized in the comprehensive privacy laws of multiple states. NPRM Part III.A.16, at 43-44, and n.58.

[59] "De-identification" is expressly mentioned, but again, the approach of the rule is to outline standards that any purported de-identification method must meet rather than endorsing specific types of de-identification.

[60] For the same reason, OAG declines to make changes here in response to a comment that proposed prohibiting covered operators from relying on de-identification with respect to biometric data, on the basis that this type of data is impossible to de-identify. If it is indeed impossible for biometric data to meet the de-identification standards outlined in the final rule, then the rule already prevents a covered operator from relying on de-identification for compliance.

[61] Nat'l Inst. of Standards and Tech., TRANSITIONING THE USE OF CRYPTOGRAPHIC ALGORITHMS AND KEY LENGTHS 2-4 (Oct. 2024) (discussing how older encryption keys become vulnerable to attack as computing power improves and how development of quantum computing may impact current encryption technology), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar3.ipd.pdf. *See also* Google, *Quantum Frontiers May Be Closer Than They Appear* (Mar. 26, 2026), https://blog.google/innovation-and-ai/technology/safety-security/cryptography-migration-timeline/.

[62] G.B.L. § 1501(3),(5).

In addition, the proposed section 700.7(a)(4) stated that at most, a covered operator may retain data for the "minimum time required" to comply with the rule, setting an outward bound. Consistent with the intent of the proposed rule, OAG has modified this language to clarify that a covered operator may retain data for the minimum time "necessary to comply with the applicable section" of the rule. This clarifies that the provision allows a covered operator to determine an appropriate data retention time so long as the retained data is only used for complying with a section of the rule and is immediately deleted once the covered operator has fulfilled its compliance obligations. The OAG considered setting a time period such as 24 hours, but concludes that the language finalized best protects New Yorkers' data while retaining necessary flexibility consistent with the Act.

3. Data retention

Some comments raised issues related to the retention of data and related considerations. For the reasons described below, OAG adopts the data retention provisions of section 700.7 as proposed, with the exception of the data retention period established in 700.7(b), which will be limited to five years in the final rule.

Theme: Commenters provided feedback regarding data to be retained in compliance with other laws.

One comment raised a concern about the language of 700.7(b)(5), which requires that data be maintained "where necessary for compliance with any applicable provisions of State law or federal law or regulation." The comment asked that this language be clarified and potentially narrowed to avoid any perception that it requires retention of user data that otherwise would be deleted pursuant to section 700.7(a)(4). The comment did not cite any provisions of state or federal law that create ambiguity when considered along with the language of section 700.7(b)(5).

The purpose of 700.7(b)(5) is inherently limited; the language makes clear only that data should be retained where "necessary" under other applicable state or federal laws, meaning that the rule does not pre-empt existing state and federal data retention obligations. The rule does not seek to enhance or expand upon any such obligations. Operators that are subject to overlapping regulations thus can interpret their respective obligations appropriately.

Accordingly, OAG adopts section 700.7(b)(5) in the final rule as proposed.

Theme: Some commenters requested a shorter duration for the data retention period.

A few comments from both industry and the advocacy community expressed concerns with the length of the 10-year data retention period set in section 700.7(b). These comments questioned the necessity for such a lengthy retention period, particularly in light of the security risks that accompany any retention of data.

The primary purpose of the data retention required in section 700.7(b) is to create transparency and accountability in the execution of operators' age assurance programs. Should there be reason to suspect that an operator is not complying with the requirements in the rule, the data maintained pursuant to section 700.7(b) will allow for an investigation of the operator's practices. The security risks related to this data are low insofar as the data retained does not include any personal user data; instead, the retained data must be anonymized and, in many instances, aggregated.

Notwithstanding the foregoing, after consideration of the comments received, OAG concludes that the 10-year retention period in section 700.7(b) is not necessary to ensure the potential for a thorough investigation of an operator's compliance with the rule. This is in part because OAG expects operators' age assurance programs to be dynamic and evolving to adapt to changes in age assurance technology and their own platforms. In light of the expected adaptations and changes in operators' age assurance programs, practices that took place 10 years earlier may be less relevant in evaluating the current or even recent historical state of an age assurance program. Taking into consideration all points raised in the comments, most notably the security concerns inherent to any data retention, OAG amends section 700.7(b) of the proposed rule to require a five-year retention period for all data enumerated therein. The OAG notes that this change does not impact the 10-year retention period in section 700.5(d), which pertains to test results, reports, and certifications, none of which are expected to include user data and thus do not create analogous risks to user data privacy.

Theme: One commenter suggested the final rule limit government access to retained data.

One comment argued that the collection of data to comply with the rule risks such data being provided by operators to government entities, either voluntarily or in response to compelled process, creating risks for certain user communities. The comment asked OAG to prohibit operators from creating searchable user databases based upon data collected for age assurance purposes. The comment further suggested that OAG expressly prohibit operators from voluntarily disclosing age assurance data to government entities or create a prior notice obligation to OAG.

The OAG carefully considered this comment and the risks it outlined. Section 700.7(f) makes clear that the data retention obligations in the rule should not be construed to "allow a covered operator to use data retained pursuant to this section, whether alone or together with other data, in order to identify an individual user." In addition, data collected must "not be used for any purpose other than to comply with this Part" (section 700.7(a)(2)) and all data "shall be held for the minimum time required to comply with this Part and thereafter must be immediately deleted" (section 700.7(a)(4)). The OAG concludes that these provisions, taken together, already prohibit operators from using age assurance data to create searchable databases as described in the comment.

With respect to operator disclosure of age assurance data in response to government requests, creating obligations related to such actions exceeds the scope of OAG's statutory rulemaking authority. However, section 700.7(e) requires operators to comply with all applicable data protection and security laws, which may include requirements related to data requests by government entities.

Theme: A commenter suggested the final rule specify U.S. location of retained data storage.

One comment asked OAG to mandate that data collected to comply with the rule be stored only on servers located in the United States, citing data concerns related to international data storage, particularly in countries with looser security standards or additional security risks. While OAG declines to implement this requirement, OAG notes that section 700.7(a)(3) obligates operators to encrypt all age assurance data both in transit and at rest, and to store that data "using industry-standard data security measures." The OAG also expects that much of the data collected for age assurance will be stored only for a short time prior to being deleted pursuant to 700.7(a)(4), further reducing the risks related to that data storage. Taking these and other considerations into account, OAG concludes that the existing security obligations in the rule are sufficient without further mandating that age assurance-related data be stored only in the United States.

H. Remedies: Section 700.8

The OAG received one comment that generally supported the available remedies as described in section 700.8 and a few comments that provided criticisms or suggestions to amend those remedies. Of note, the proposed rule closely tracks the remedies provided by the Legislature in the Act, G.B.L. § 1508. For this reason, and because all of the suggested changes would require OAG to exceed its statutory authority, OAG adopts section 700.8 as proposed.

One comment recommended that the remedies available to OAG for enforcement of the rule be graduated so that repeat offenders are subject to harsher penalties by design. The OAG declines to adopt this recommendation as codifying such a provision goes beyond OAG's statutory authority. The OAG notes, however, that in a legal action for non-compliance with the rule, OAG may consider factors such as the nature of the offense and the operator's history of non-compliance in seeking specific remedies.

One comment asked that the rule include a private right of action for individuals harmed by violations of the rule, as well as whistleblower protections for individuals providing evidence of violations. The OAG declines to adopt these remedies, which go beyond the remedies provided by the Act. Another comment asked that penalties for non-compliance with the rule that are recovered by OAG be directed to a fund supporting children's behavioral health. Again, OAG declines to codify this request as doing so would exceed OAG's rulemaking authority conferred by the Legislature.

Finally, one commenter expressed concern that OAG's ability to enforce the rule and underlying law through the remedies enumerated in G.B.L. § 1508 give rise to a risk that enforcement will be used as a tool to evoke government censorship. The commenter did not specify how such censorship would flow from enforcement of the rule and did not request any changes to the rule that would alleviate or lessen this concern. As stated above, OAG has not materially expanded upon or changed the remedies included in G.B.L. § 1508 by the Legislature and to do so would exceed OAG's statutory authority. The OAG thus declines to make changes to the proposed rule in response to this comment.

I. Miscellaneous: Section 700.9

Theme: Commenters suggested ways to ensure covered minors can still access content on covered platforms.

Commenters proposed exempting certain types of content or subject areas to ensure that the Act and rule do not prevent covered minors from accessing content. This is unnecessary. As discussed in Part III.I of the NPRM, G.B.L. § 1504, which is implemented by section 700.9(b) of the rule, prohibits a covered operator from blocking a covered minor's access to content solely because the covered minor has not been permitted to access an addictive feed or nighttime notifications under the Act. G.B.L. § 1500(1)(a)-(h) also exempts from the definition of "addictive feed" various other platform features that a covered minor can use to access content, such as search features.

Accordingly, OAG makes no changes in response to this comment.

Theme: Commenters suggested the final rule should not prevent adults who do not wish to undergo age assurance and parents who do not wish to use a method of verifiable parental consent from accessing online platforms.

Some commenters expressed concern that the rule prevents adults from accessing any part of an online platform if the adult does not wish to undergo age assurance. Similarly, one comment suggested that the rule prevents parents (or their covered minors) from accessing any part of an online platform if the parent does not wish to use a method of verifiable parental consent because the parent is concerned about having to undergo age assurance as required under sections 700.2(e)(5)(i) and 700.3(e)(5)(i) of the rule.

Sections 700.2(a) and 700.3(a) of the rule, which mirror G.B.L. §§ 1501(1) and 1502, state that they apply to addictive feeds and nighttime notifications, two specific types of platform features. They do not apply generally to an online platform, or to other features of the platform, and an individual must undergo age assurance only if they wish to access one of the specified features.

Furthermore, as discussed in Part III.I of the NPRM, G.B.L. § 1504 and its implementing section 700.9(b) of the rule include protections to ensure a covered operator does not use the Act or rule as a pretext to generally deny an individual access to an addictive online platform.

Consequently, if an individual declines to undergo any offered age assurance method including methods offered as part of the appeals process, all that a covered operator must do is deny them access to an addictive feed and to nighttime notifications. A covered operator may not deny this individual access to the rest of the online platform on the basis that the rule requires them to do so.

Accordingly, OAG makes no changes in response to this comment.

Theme: One commenter argued section 700.9(b) of the rule is contrary to the Act and prevents a covered operator from complying in good faith with the Act.

One commenter asserted that proposed section 700.9(b) of the rule conflicts with the Act because it bars a covered operator from taking the very steps required by the Act, namely, preventing a covered minor from accessing an addictive feed or nighttime notifications absent parental consent. This section substantively reproduces the text of G.B.L. § 1504 but also clarifies that actions necessary to comply with sections 700.2 and 700.3 are not prohibited by section 700.9(b) because they are required for a covered operator to comply with the Act. How a covered operator may comply with this section in conjunction with the rest of the rule is extensively discussed in Part III.I of the NPRM.

Accordingly, OAG makes no changes in response to this comment.

Theme: One commenter suggested the final rule should expressly prohibit a covered operator from engaging in specific discriminatory practices against users.

One comment proposed that the rule elaborate on proposed section 700.9(b) by expressly prohibiting certain practices, such as charging covered minors or parents a fee (or increasing the amount of existing fees). Another comment, although addressing section 700.7 of the rule, similarly proposed that the rule expressly prohibit a covered operator from charging for the appeals process. Section 700.7 merely separates out the requirements for an appeals process for readability. Since the appeals process remains part of the age assurance process outlined under the rule, section 700.9(b) still applies to a covered operator's actions under section 700.7 and OAG addresses these comments together.

Part III.I of the NPRM explicitly addressed fee-charging by a covered operator in connection with the Act and explained when OAG would consider this to violate the rule and G.B.L. § 1504. Thus, an express prohibition of specific practices is unnecessary. In addition, OAG is concerned that an express list of prohibited practices may mislead a covered operator into thinking that only practices on the list are forbidden when this section of the rule is intended to be broadly applicable. The OAG reminds covered operators that they should carefully consider section 700.9(b) when designing their compliance plans, since a violation of this section will be investigated no differently than a violation of any other section of the rule.

To further clarify that section 700.9(b) applies equally to all covered operator actions in connection with the rule, OAG is modifying the text to state "covered users and parents" instead

of “covered minors and parents” throughout this section. This modification also aligns more closely with the original text of G.B.L. § 1504.

J. Effective date

G.B.L. § 1508(5) sets the effective date of the Act as the 180th day after OAG promulgates rules implementing the Act. Proposed section 700.11 of the rule adopts the same effective date.

One comment proposed that the rule include a “sunset” provision establishing a three-year cycle wherein the rule would expire unless the Legislature conducts an assessment and affirmatively acts to re-authorize it. The comment also proposed mandating research studies on the effects of the Act and rule and their effectiveness in reducing mental health harms in minors, as well as a safe harbor to protect previously compliant covered operators in the event of the rule’s expiration. Per the comment, such measures would ensure that the rule implements the Act while minimally infringing on individual rights and accounting for novel technological and social developments.

This proposal directly contradicts G.B.L. § 1508(5), which clearly outlines all requirements for the Act to take effect. It is also unnecessary for ensuring that the final rule is regularly reviewed and updated, since State Admin. Proc. § 207 already establishes such standards for agency rule-making.

Accordingly, OAG makes no changes in response to this comment.

K. First Amendment

Some commenters argued that the Act and, and thus, these implementing rules impermissibly regulate speech or expressive activity in violation of the First Amendment. The OAG concludes that neither the law nor the rules violate the First Amendment. When a legislative enactment is challenged on constitutional grounds, there is both an exceedingly strong presumption of constitutionality and a presumption that the Legislature has investigated for and found facts necessary to support the legislation.[63] Moreover, as noted by other commenters, the Act and the rules address specific features, namely addictive feeds and nighttime notifications, not protected speech. The Legislature has determined these features are harmful to minors and their regulation does not unduly or disproportionately burden any person’s ability to express or access protected speech.

Theme: Some commenters asserted the Act and rules violate the First Amendment by directly regulating addictive feeds, which they argue are protected expression.

[63] *White v. Cuomo*, 38 N.Y.3d 209, 217 (2022) (quotations omitted) (citing *I.L.F.Y. Co. v. Temporary State Housing Rent Comm’n.,* 10 N.Y.2d 263, 269 (1961); *Lincoln Bldg. Assoc. v. Barr,* 1 N.Y.2d 413, 415 (1956), addressing state and federal constitutional questions).

Some commenters argued that the Act directly regulates expressive activity by limiting access to addictive feeds for minors and burdening access for adults. These commenters argue that addictive feeds constitute protected speech or expression, and, thus, the law and rule are subject to heightened or strict scrutiny. One commenter argues that the Act unlawfully distinguishes between speakers because it applies only to platforms that provide addictive feeds with user-generated or user-posted media but does not apply to feeds consisting of media generated or posted by an operator.

A predicate to any First Amendment claim is a showing that the challenged state action regulates speech or expressive conduct.[64] Here, consistent with the Supreme Court's decision in *Moody v. NetChoice, LLC*, 603 U.S. 707, 725 (2024), there is no basis to conclude that the prohibition of addictive feeds for minors regulates speech or expressive conduct. Addictive feeds are features of an online platform, not expression protected by the First Amendment. Addictive feeds consist of "engagement optimization" algorithms applied to user-generated media that lead to the addictive behavioral patterns that the Legislature concluded are harmful to children. As discussed at length in Part II.B.1 of the NPRM, these algorithms are focused on engagement and do not reflect any particular message, idea, or expression. Accordingly, the First Amendment is not implicated by the Act and rule's limits on addictive feeds.

Theme: Some commenters argued that age assurance unduly burdens adults' access to media on addictive online platforms in violation of the First Amendment.

A few commenters argued that requiring age assurance violates the First Amendment because it prevents adults from freely exercising their right to speak on the internet and from accessing speech. One commenter also argued that the law would not allow adults to remain anonymous in the media they post or access. Some commenters argued that age assurance triggers heightened scrutiny because it imposes a disproportionate burden on individuals exercising their First Amendment rights. One commenter noted that the false positive rates allowable under the accuracy minimums, especially for older minors, may be so high as to render the law underinclusive under heightened scrutiny.

First, as explained herein, addictive feeds are not protected speech or expressive activity. Thus, no First Amendment protection attaches to them. Second, these comments are based on the false premise that the law and rules set up an "age gate" for access to all platform services, i.e., age assurance must be conducted to access any aspect of a platform if the platform has an addictive feed as a significant part. Neither the Act nor the rules require an online platform to conduct age assurance in order for a user to either access media created or posted by other users or to post or share media. Operators need not limit user access on a covered online platform to comply with the law. The law is triggered only if a user has access to an addictive feed or nighttime notifications. The media that would be in any such feed can remain readily available to any user by any means other than an addictive feed, including search, subscription,

[64] See *Mastrovincenzo v. City of New York*, 435 F.3d 78, 91 (2d Cir. 2006).

a chronological feed, a feed of curated media, or through another user sharing that material. An operator can continue to allow any user of an online platform to post, search for, and be provided an array or feed of media that has been posted or shared.

Third, OAG disagrees with commenters' assertion that requiring adults to undergo age assurance to access addictive feeds and nighttime notifications is unduly burdensome. Commenters do not provide convincing evidence that any age assurance method consistent with the requirements of the final rule will either require significant investment to implement or overburden adult users in violation of the First Amendment. Those contentions are undermined by the economic analysis conducted by OAG, the exemption of certain platforms in the final rule, and the widespread and increasing use of a variety of age assurance methods and technologies around the world, which is thoroughly documented in Part III.D.2.g.i of the NPRM.[65]

Additionally, even if the law as implemented by the rules "burdened" adult access to media with age assurance, such burden would be incidental and subject to intermediate scrutiny under the Supreme Court's decision in *Free Speech Coalition, Inc. v. Paxton*, 606 U.S. 461 (2025), a standard today's age assurance technology would readily meet. For example, age assurance can be conducted anonymously and the law neither suggests nor requires disclosure of a user's identity.

Theme: Some commenters argued that the law and rules are not appropriately tailored to address minors' mental health harms.

A few commenters also argued that regardless of the standard applied, the law and implementing rules are not adequately tailored to address the stated harm of negative mental health outcomes for minors. Some argued the definition of addictive feed is underinclusive because other aspects of social media cause mental health harms as well. One commenter argued that feeds based on content a user subscribes to, follows, or searches for will also cause excessive use. Another commenter argued the law is not adequately tailored because it translates to a requirement that online platforms provide a strictly chronological feed that includes material deemed harmful to minors.

The OAG disagrees. In Part II.B of the NPRM, the OAG fastidiously summarized the evolution, purpose, and technology behind addictive feeds as well as the scientific evidence supporting the conclusion that addictive feeds cause significant mental health harms suffered

[65] As just a few additional examples occurring since the publishing of the proposed rule, the government of Australia implemented an age assurance requirement as part of a prohibition of social media accounts for users under the age of 16, which went into effect in December 2025, *see* https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions, the government of Brazil enacted detailed rules requiring effective age assurance methods by providers of online products and services, *see* Digital Statute for Children and Adolescents, Law No. 15.211/2025; Decree No. 12.881/2026 (Braz.), and the government of Canada published a national standard instructing online platforms on acceptable age assurance methods, *see* First National Standard of Canada for Age Assurance Technologies, CAN/DGSI 127:2025 (Can.).

by minors. The rule targets addictive feeds, the cause of these mental health harms, without limiting access to media. No commenter presented evidence that display of media based on content followed, subscribed to or searched for by users alone would be sufficient to cause the same harms while Part II.B.1 of the NPRM explains the mechanisms in addictive feeds that lead to excessive use. Finally, neither the rule nor the law requires strict chronological feeds or the display of unfiltered media. Instead, the law targets personalization as defined in addictive feeds but does not otherwise limit operators from choosing an order by which to display media. The OAG also clarifies that neither the law nor the rules prohibit the removal or prioritization of content based on the media's quality or subject matter. Nor does either prevent online platforms from enforcing their preferred content moderation policies, including those that prevent the display of harmful or objectionable speech. G.B.L. § 1501(7), adopted nearly verbatim in final rule section 700.9(e), clarifies online platforms' ability to adopt and enforce such policies.

Theme: A few commenters argued that the ban on nighttime notifications violates the First Amendment.

A small number of commenters argued that the ban on nighttime notifications violates the First Amendment because it is underinclusive and targets certain platforms while allowing for nighttime notifications by others.

Like addictive feeds, the nighttime notifications are automated features and, as discussed in Part II.B.1 of the NPRM, are focused on reengagement or bringing the user back to the addictive feed rather than communicating a message. Accordingly, the law, on its face, does not regulate the "message[s]" or "ideas" expressed by anyone and does not distinguish among different types of speakers. [66]

L. Other comments

In addition to the comments discussed in other sections, comments made proposals regarding subject matter not addressed by the Act.[67] One comment proposed that the rule explicitly address potential conflicts between the rule and data protection laws enacted by municipalities and other local entities. The comment did not identify any specific existing laws that conflict with the rule, but suggested that without an express provision permitting such laws to address the same subject matter as the rule, municipalities and other local authorities will be reluctant to consider passing them. Section 700.7(e) of the rule expressly contemplates that covered operators may need to comply with multiple laws (including federal laws as well as municipal laws) regarding data protection. This section provides clear guidance in case of a conflict between laws, stating that a covered operator must comply with the law that is "more

[66] *Reed v. Town of Gilbert*, 576 U.S. 155, 163 (2015).

[67] For example, one comment suggested that any law requiring online identity verification should be "stopped." Another comment similarly suggested that the Kids Online Safety Act, a proposed federal bill, should not be passed. Addressing the enactment of any law besides the Act is beyond the scope of the rule.

protective of a covered minor's privacy and safety." It is not necessary for the rule to further address potential legislative activities by municipal and local entities.

Some comments proposed that the rule address aspects of online platforms that may harm minors but that are not governed by the Act, providing examples such as artificial intelligence functionality, auto-loading or playing of content (including "infinite scroll" and similar features), other types of feeds and notifications, and certain types of content. A few comments suggested that the rule go further than the Act in addressing a covered minor's access to the entirety of an online platform. While OAG takes seriously any allegation of harm to minors and will review them for potential violations of New York law, such topics are also beyond the scope of the Act and the rule.

A few comments suggested including references in the rule to specific technologies that they believed would be helpful in complying with the Act, such as digital wallets and identification technology and platform-use monitoring technology. The OAG has considered these comments and, as explained in more detail in the appropriate sections, OAG has balanced specificity with flexibility in the rule to support a range of compliance methods. If a given technology meets the rule's requirements, then it can be used to comply with the Act, so it is not necessary for the rule to explicitly mention that technology.

Accordingly, OAG makes no changes in response to these comments.