



**Comments in response to the New York State
Office of the Attorney General's (OAG)
Advanced Notice of Proposed Rulemaking (ANPRM)
for the Stop Addictive Feeds Exploitation (SAFE) for Kids Act (S7694A)**

Respectfully submitted,

Holly Grosshans, Senior Counsel for Tech Policy
Common Sense Media

on behalf of

Common Sense Media
Fairplay
NY State American Academy of Pediatrics

September 30, 2024

Comments in response to the New York State Office of the Attorney General's (OAG) Advanced Notice of Proposed Rulemaking (ANPRM) for the SAFE for Kids Act.

Introduction.

On behalf of Common Sense Media, Fairplay, and the NY State American Academy of Pediatrics, we are pleased to submit these comments in response to the New York State Office of the Attorney General's (OAG) Advanced Notice of Proposed Rulemaking (ANPRM) for the SAFE for Kids Act. We support New York State's OAG's efforts to protect children's safety while ensuring their privacy, and we offer constructive suggestions to achieve this balance below.

Common Sense Media is the leading nonprofit organization dedicated to improving the lives of all children and families by providing the trustworthy information, education, and independent voice they need to thrive in the 21st century. Fairplay is a nonprofit organization committed to helping children thrive in an increasingly commercialized, screen-obsessed culture, and the only organization dedicated to ending marketing to children. The NY State American Academy of Pediatrics (NYS AAP), District II, comprised of Chapters 1, 2, & 3, is dedicated to the physical, mental, and social health and wellbeing of all infants, toddlers, children, and adolescents. NYS AAP is committed to advocating for a state that supports all children to ensure they can thrive.

According to the U.S. Surgeon General's advisory, Social Media and Youth Mental Health: The U.S. Surgeon General's Advisory, up to 95% of youth ages 13-17 report using social media, with more than a third saying they use social media "almost constantly."¹ The advisory noted that children and adolescents who spend more than 3 hours a day on social media face double the risk of mental health problems including experiencing symptoms of depression and anxiety. This is concerning as a recent survey showed that teenagers spend an average of 4.8 hours a day on social media.² And when asked about the impact of social media on their body image, 46% of adolescents aged 13-17 said social media makes them feel worse.³

Social media companies use personally tailored and targeted feeds (addictive feeds) to get kids and teens to engage and view the platforms for longer in order to make more money. Addictive

¹ U.S. Dept. of Health and Human Services, *Social Media and Youth Mental Health: The U.S. Surgeon General's Advisory* (2024), <https://www.hhs.gov/surgeongeneral/priorities/youth-mental-health/social-media/index.html#:~:text=The%20Surgeon%20General's%20Advisory%20on.%2C%20technology%20companies%2C%20researchers%2C%20and>.

² Jonathan Rothwell, *Teens Spend Average of 4.8 Hours on Social Media Per Day* (Oct. 13, 2023), <https://news.gallup.com/poll/512576/teens-spend-average-hours-social-media-per-day.aspx>.

³ The Digital Wellness Lab's Pulse Survey, *Adolescent Media Use: Attitudes, Effects, and Online Experiences* (August 2022), https://digitalwellnesslab.org/wp-content/uploads/Pulse-Survey_Adolescent-Attitudes-Effects-and-Experiences.pdf.

feeds have had an increasingly devastating effect on children and teenagers; spending more time on social media has been tied to significantly higher rates of youth depression, anxiety, suicidal ideation, and self-harm.

In response to the negative impact of social media use on children and teens, the New York Legislature passed, and Governor Kathy Hochul signed into law, the Stop Addictive Feeds Exploitation (SAFE) for Kids Act. The SAFE for Kids Act has two main features to protect young users online. It bans the use of algorithmic, or addictive, feeds to minors, and it bans overnight notifications from addictive feeds to minors. Both features can be overridden with parental consent. This landmark law offers the best of both worlds when it comes to protecting kids online - eliminating two features that are known to cause harm to kids while allowing full access to the internet and community of friends, family and areas of interests for those same users."

Our comments focus on several areas of this new law for which the OAG is seeking responses, including regarding commercially reasonable and technically feasible methods of age determination, parental consent, addictive feeds, and other questions. As the SAFE for Kids Act requires the OAG to promulgate regulation regarding age assurance, in addition to our comments below we also offer [here](#) our newly released whitepaper on age assurance, *U.S. Age Assurance is Beginning to Come of Age: The long path toward protecting children online and safeguarding access to the internet*, which considers in more detail the current state of age assurance and potential paths forward to ensure that all children can thrive in the digital world while preserving access to the internet for all users.

Commercially reasonable and technically feasible age determination methods.

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

Age assurance should be privacy protective, proportionate, fair, and equitable. OAG regulations should ensure that any age assurance technology used to comply with the SAFE for Kids Act meets express standards for accuracy and fairness, and the OAG should consider requiring such systems to be independently verified. Technology is increasingly available to make it so, and efforts in other countries will demonstrate this. It is also possible for age assurance and protections for children online to exist within the bounds of the First Amendment – especially in contexts like the SAFE for Kids Act which does not limit access to content. This is consistent with how we operate in an everyday world, and it should not be impossible to draw nuanced lines just because technology is involved.

When assessing the proportionality of “commercially reasonable and technically feasible” methods, the SAFE for Kids Act should weigh the risk of harm to kids associated with the platform

as well as the risk of harm associated with the age assurance method (often claimed to be a violation of the user's First Amendment rights in the form of limiting access to information content or free speech). In the case of the SAFE for Kids Act, the Act does not put at risk any user's access to information, content or speech. The Act focuses on regulating the addictive design features of the addictive feed and notifications. Because of this lack of risk in loss of access to information, content, or ability to speak online, there is little risk of harm to a user for using age assurance methods. In other words, if the age assurance gets it wrong and assesses an adult as a minor under the Act, the adult wouldn't lose access to any content; they only wouldn't have access to the addictive design features of the addictive feed and notifications from the addictive feed.

The greatest challenge in the U.S. for any age determination method is the allegation that use of age assurance is a violation of the First Amendment rights of the users – sometimes of children, and sometimes of adults who may be deterred from visiting sites if there are age assurance mechanisms in place.⁴ And sometimes – including when privacy and data are involved – concerns have involved companies' free speech rights.

While challenges to age assurance laws regarding design, access, and privacy (with the California Age Appropriate Design Code (CA AADC)⁵ being a major example of design and privacy), most of the cases have generally involved access to content involving pornography or social media in general.

In situations that involve age assurance to make sure product design is appropriate, or when age assurance is used to ensure that privacy protections are provided, the First Amendment could be considered less of a factor. As indicated by the Ninth Circuit considering the California AADC in *Netchoice v. Bonta*, age assurance targeted at product features or privacy protections may not always impact protected speech. Specifically, the Ninth Circuit found that certain provisions of the CA AADC are likely to fail under the strict scrutiny standard of the First Amendment – primarily a data protection impact assessment (DPIA). However, the court was precise in finding that “whether NetChoice is likely to succeed on its facial challenge as to the remaining challenges is less certain. For instance, most of those provisions, by their plain language, do not necessarily impact protected speech in all or even most of their applications.”⁶ The age assurance provision of the AADC was one of these provisions, which did not necessarily impact protected speech in all or most applications. This finding by the Ninth Circuit seemingly suggests that age assurance that does not restrict access to content but rather design features such as dark patterns is not a violation of the First Amendment.

⁴ See focus on challenges and first amendment concerns in OTI's “Age Verification: The Complicated Effort to Protect Youth Online”, <https://www.newamerica.org/oti/reports/age-verification-the-complicated-effort-to-protect-youth-online/challenges-with-age-verification>.

⁵ A.B. 2273 (Cal. 2021), https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=20210220AB2273.

⁶ *NetChoice v. Bonta*, No. 23-2969 (9th Cir. Aug. 16, 2024).

This view has led to courts distinguishing between conduct (including design features) and speech.⁷ Particularly in the case of the SAFE for Kids Act, speech is not being regulated. The law is content-neutral; in fact, the SAFE for Kids Act does not limit a user's ability to search for any material (even material that many would consider "harmful") that they are interested in. Section 1500.1(c) has an exception for content when "the user expressly and unambiguously requested the specific media or media by the author, creator, or poster of the media." This law actually elevates the content the user is seeking, by eliminating the content that the user is not seeking - through the limiting of the algorithmic, or addictive, feed. Additionally, companies could choose to offer this feature of eliminating the algorithmic feed and nighttime notifications from such a feed - or any privacy or safety feature by default - to all users. In this scenario, only the adult users that would prefer to opt out of these default privacy and safety features would potentially be subjected to an age assurance method, if it is not clear from their transactional data that the user is not a minor.

5. What methods do social media platforms currently use to determine (or attempt to determine) age? Do these methods vary based on the specific industry or focus of the social media platform, or are they based on other factors?

Social media platforms operate under a diverse set of user age requirements and what methods they choose to use for age assurance also varies depending on the operating location(s), size and resources of the company. Companies based in or operating in the U.S. and the European Union, for example, must determine which users are under 13 years old. Despite these mandates, we see that when companies that are not explicitly required to employ age assurance systems they do not - at least in terms of assessing age to provide protections. Instead, most major social media platforms rely primarily on users to self-identify their age without any kind of verification.

There are a variety of age assurance systems used by the largest social media companies with significant user bases in the United States, both in their structure and effectiveness.

Facebook, owned by Meta, is the largest social media company by far, with just over 3 billion monthly active users.⁸ It is also one of the few social media platforms that purports to implement some version of age assurance other than just relying on attestation. Facebook's policy requires users to be at least 13 years old to sign up for an account.⁹ Prospective users must provide their age to the platform when they sign up, and they will be locked out of making an account if they do not attest to being at least 13.¹⁰ Once a user is on the platform, Facebook uses artificial intelligence systems drawing on "multiple signals," including things like birthday messages from

⁷ Social Media Cases, Case No JCCP 5255, Lead Case 22STCV21355, Superior Court of CA, County of LA, Carolyn Kuhl, OCT 13, 2023 (negligence claims based on social media design features not barred by First Amendment).

⁸ Stacey Jo Dixon, *Number of Monthly Active Facebook Users Worldwide as of 4th quarter 2023*, STATISTA (Feb. 2024).

⁹ Pavni Diwanji, *How Do We Know Someone Is Old Enough to Use Our Apps?*, META (July 27, 2021), <https://about.fb.com/news/2021/07/age-verification/>.

¹⁰ *Id.*

friends and the kinds of content the user searches for on the platform, to verify that the user is actually as old as they identified themselves to be.¹¹ (Facebook claims to use this for keeping people on or off its apps; as noted above, however, per court documents it has historically seemed to rely on only the self-provided age for “legal purposes” and used the signals from user activity for marketing and other purposes.¹²) Finally, Facebook also uses human content moderation — if an account is flagged as a terms of service violation (normally, these flags are unrelated to the account’s age, e.g. an account is flagged for hate speech or doxing), then the human content moderator assigned to investigate the activity also reviews the account to ensure it is properly of age.¹³ The assessment of the effectiveness of this system is mixed. On the one hand, Facebook has been applauded for taking a voluntary and “first step” in age assurance.¹⁴ On the other hand, serious questions have been raised about the efficacy of these systems; in fact, the European Commission recently launched a probe that includes an investigation into the efficacy and proportionality of Facebook’s age assurance methods.¹⁵

Instagram, also owned by Meta, is not the next largest social media platform, but it is the next largest platform that relies on a unique age assurance method. Like Facebook, users must be at least 13 years old to create an account on Instagram.¹⁶ And also like Facebook, Instagram initially relies on users self-reporting their age at sign-up. However, if a user seeks to change the age on their account from under 18 to 18 or older, the user must go through an age assurance system.¹⁷ Instagram gives users three options to prove that they’re over 18: first, a user can submit a digital version of an ID; second, users can upload a video of themselves speaking into a camera, which is then submitted to Yoti — a company that uses AI to determine age from facial and voice recognition; and third, social vouching, where users can get three other users they follow, who are all at least 18 years old, to ‘vouch’ that the user who is seeking to change their account to 18+ is actually over 18.¹⁸ There is reason to believe that the first two verification methods — ID checking and facial recognition — are fairly effective. While ID checking is at risk of some circumvention the technology is becoming more reliable and more able to counter common circumvention tactics. For example, Yoti’s ID checking systems used by Instagram include face matching to ensure that the person submitting the ID is actually the person on the ID, authenticity checking to ensure that

¹¹ *Id.*

¹² Complaint for Injunctive and Other Relief, U.S. District Court for Northern District of California, 4:23-cv-05448-YGR Document 73-2, (“multi-state lawsuit”), page 28, line 6.

¹³ *Id.*

¹⁴ Peter Suci, *Meta Testing New Age Verification Tools – Experts Explain Why They Won’t Work*, FORBES (July 1, 2022), <https://www.forbes.com/sites/petersuci/2022/07/01/meta-testing-new-age-verification-tools--experts-explain-why-they-wont-work/>

¹⁵ Emma Woollacott, *European Commission Probes Meta Over Youth Social Media Addiction*, FORBES (May 16, 2024), <https://www.forbes.com/sites/emmawoollacott/2024/05/16/european-commission-investigates-facebook-and-instagram-rabbit-hole/>.

¹⁶ Diwanji, *supra* note 9.

¹⁷ Instagram, *How does video selfie age verification work on Instagram?*, Help Center, https://help.instagram.com/292521846402382/?helpref=uf_share.

¹⁸ Instagram, *Introducing New Ways to Verify Age on Instagram*, (June 23, 2022), <https://about.instagram.com/blog/announcements/new-ways-to-verify-age-on-instagram>.

the ID is legitimate, and technology that counters deepfakes that are designed to make the user look like the photo on the ID to circumvent the check.¹⁹ Yoti claims their facial recognition software currently accurately identifies 6-11 year olds as under 13 years old 98.35% of the time.²⁰ However, recent data published by the National Institute of Standards and Technology (NIST) raises questions about this claim of accuracy.²¹ Other organizations have challenged these claims as well.²² In addition to using age assurance when young people attempt to create adult-aged accounts, Instagram also announced in September 2024 that it was “building technology to proactively find accounts belonging to teens, even if the account lists an adult birthday” and that such technology would be tested in the US in early 2025.²³

The remaining major social media companies popular with young people in the U.S. — YouTube, TikTok, WhatsApp, Telegram, Snapchat, X, Reddit, Pinterest, Threads, and others — implement almost no age assurance. By virtue of operating in the U.S., they all have requirements within their terms of service that users must be at least 13 to create an account on their sites. However, all of these platforms, and other ones of equivalent size, rely entirely on self-reporting by users to determine age. That means that on the vast majority of social media platforms, users of any age can sign up simply by saying they’re older than 13, or can access adult-only content on the platform simply by saying they’re 18 or older. Some platforms implement remedial measures; companies like TikTok, YouTube, and Pinterest implement the same human content moderation system that Facebook and Instagram do, where accounts that are flagged for a community guideline violation are also evaluated for age. And some other sites — WhatsApp and imo.im — implement a system where a parent can request that their kid’s account be deleted if the child is under 13, but the process is a fairly onerous one.

6. Some social media platforms presently attempt to determine user ages for a variety of internal purposes based on information other than self-attestation. For what purposes do such platforms currently attempt to determine age? What processes do they use to attempt to determine age? What data do these methods use to infer age? How accurate, and how precise, are such determination attempts? What factors increase or decrease the accuracy of such determination attempts?

Currently, companies in the U.S. are more likely to use age assurance to determine age for marketing purposes - rather than for legal compliance issues. Facebook claims to use age

¹⁹ Amba Karsondas, *Effective Age Verification: Going Beyond Reading a Date of Birth on an ID*, Yoti (July 11, 2023), <https://www.yoti.com/blog/effective-age-verification-going-beyond-reading-date-of-birth-on-id/>.

²⁰ Yoti, *Facial Age Estimation Fact Sheet* (Oct. 2023), <https://www.yoti.com/wp-content/uploads/2023/10/Facial-age-estimation-fact-sheet.pdf>.

²¹ Kayee Hanaoka, et al., National Institute of Standards and Technology (NIST), *Face Analysis Technology Evaluation: Age Estimation and Verification*, (May 2024), https://pages.nist.gov/frvt/reports/aev/fate_aev_report.pdf.

²² EPIC, et al., *EPIC, CDD, Fairplay Comments to the FTC on Proposed Parental Consent Method Submitted by Yoti Inc. under COPPA Rule*, (August 221, 2023), <https://epic.org/documents/epic-cdd-fairplay-comments-to-the-ftc-on-proposed-parental-consent-method-s-ubmitted-by-yoti-inc-under-coppa-rule/>.

²³ Instagram, *Introducing Instagram Teen Accounts: Built-In Protections for Teens, Peace of Mind for Parents* (Sep. 17, 2024), <https://about.instagram.com/blog/announcements/instagram-teen-accounts>.

assurance for keeping people on or off its apps, however, per court documents, it has historically seemed to rely on only the self-provided age for “legal purposes” and used the signals from user activity for marketing and other purposes.²⁴

(See response to comment 5 for analysis of what Facebook and other companies utilize as far as age assurance methods).

7. Many existing users of social media platforms have already self-attested to being 18 years of age or older. What data exist on the accuracy of such self-attestations? How does this compare to the accuracy of users currently self-attesting to being 13 years old?

There is an obvious concern that self-attestation, while easy, is insufficient age assurance in terms of accuracy. Any user can circumvent the system at the click of a button. However, there is reason to believe that certain design features can enhance the effectiveness of self-attestation. For starters, if web services framed self-attestation as a benefit rather than a barrier, response accuracy would increase.²⁵ If users knew that the younger their self-reported age, the more privacy protections they would have in relation to the web service, they would be more likely to report accurately. Similarly, if users did not think that self-attestation age assurance was a method of blocking user access to certain content on the platform, they would be less likely to falsely report their age.

Another design feature that can increase the effectiveness of self-attestation is “friction.”²⁶ The Electronic Privacy Information Center (EPIC) uses the term friction to describe design elements that have the effect of slowing a process, which usually results in less reporting inaccuracies. For example, a web service may require a user to wait a certain amount of time before changing their birthdate, rather than immediately allowing the user to do so after their account is created.

As to data that exists about the accuracy of users currently self-attesting to being 13 years old (or older), according to a survey of 1,000 US-based kids aged 8 to 17 conducted by Ofcom, 32% of children between the ages of 8 and 17 have a social media account with an adult user age (18+) after signing up with a false date of birth.²⁷ Additionally, in a survey conducted by Express VPN of over 2,000 U.S.- and UK-based kids aged 4 to 13, 24% admitted to lying about their age on social media in order to gain access to social media platforms.²⁸

²⁴ *State of Arizona et al. v. Meta Platforms, Inc. et al.* (N.D. Cal Oct. 24, 2023), *Complaint for Injunctive and Other Relief*, 4:23-cv-05448-YGR Document 73-2.

²⁵ 5Rights Foundation, *But how do they know it is a child? Age Assurance in the Digital World*, October 2021. https://5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf.

²⁶ EPIC, *Amicus Brief for NetChoice, LLC v. Rob Bonta, Attorney General of the State of California, in his official capacity*, December 2023. <https://cdn.sanity.io/files/3tzzh18d/production/c567c26dc66cd9839ab87ec6db9b95975d80b1c4.pdf>.

²⁷ Ofcom, *A third of children have false social media age of 18+*, October 2022 and updated January 2024. <https://www.ofcom.org.uk/online-safety/protecting-children/a-third-of-children-have-false-social-media-age-of-18/>.

²⁸ Express VPN, January 2024, *Dangers of social media for kids and how to protect them*,

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

The OAG regulations could call for trusted third-party verifiers that would be able to pass information to the platforms. Using this method is a way to limit the number of entities that hold age information and presumably could mean that data collected is in fewer – and possibly more trustworthy – hands. It should be noted that third-party verifiers may themselves seem to be ripe targets for hacking, which is an important concern to address. Therefore, it would be important to create strong data privacy regulations around what data is held by these third parties and the OAG could promulgate requirements or best practices for these third-party verifiers.²⁹ Already, under Section 1501(3) of the Act, any method chosen will delete information once age has been ascertained. Additionally, and more preferably, third-party verifiers could pass information on to the site or service requiring age assurance – and this information that is passed could be very limited, including through “zero knowledge proofs” that do not do anything other than indicate whether a user is or is not a certain age.³⁰

10. What obligations should OAG regulations specify concerning how social media platforms can request age determination? How can OAG ensure that users are effectively informed of the substance of the age determination process without creating an undue burden?

» **Should OAG regulations require notice about the harms of addictive feeds? If so, what form should the notice take? What content should it include?**

» **Should OAG regulations require notice about specified information concerning methods, such as how fast the method takes, what data it will require, its error rate, and any bias?**

Whichever age assurance method is chosen by the OAG, social media platforms should consider data minimization and, when data is collected, data security. Depending on the age assurance method chosen by the OAG, an explanation about what data is collected, and how that data is used and deleted immediately per Section 1501(3). Section 1501(3) states that “Information collected for the purpose of determining a covered user's age under paragraph (a) of subdivision one of this section shall not be used for any purpose other than age determination and shall be deleted immediately after an attempt to determine a covered user's age, except where necessary for compliance with any applicable provisions of New York state or federal law or regulation.” This information about their data not being retained should be shared with users.

<https://www.expressvpn.com/blog/survey-children-on-social-media/>.

²⁹ CNIL, *Online age verification: balancing privacy and the protection of minors*, (September 22, 2022), <https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors>.

³⁰ “A zero-knowledge proof (often abbreviated as “ZKP”) is a cryptographic protocol that can improve data privacy. It allows one party, known as the prover, to assure another party, the verifier, that a statement is true without revealing any extra information.” <https://aleo.org/post/what-is-a-zero-knowledge-proof/>

There are several considerations to be taken into account when thinking about requiring notice about the harms of addictive feeds. This summer, U.S. Surgeon General Dr. Vivek Murthy announced that social media platforms should carry a warning label to advise parents about the harms of usage on youth mental health.³¹ Casting the effects of social media on children and teenagers as a public health risk, on par with road fatalities or contaminated food, Murthy called for congressional action to remind parents and adolescents that social media has not been proven safe. Federal legislators, including Senators Fetterman and Britt, have introduced a social media warning label bill.³² Additionally, state officials, including NY Attorney General James and 41 other state attorneys general, have indicated support for a social media warning label.³³

A warning label is not the only method of alerting users to the potential harms from using social media. In Colorado, earlier this year, Governor Polis signed the Healthier Social Media Use Among Youth Act (HB24-1136)³⁴. This novel legislation requires pop-up notifications, with information about the impact of social media on users' mental and physical health, to be sent to kids and teens who are on a social media platform for more than one hour each day, and then every 30 minutes thereafter. It also requires these pop-up notifications every 30 minutes if using a social media platform between the hours of 10 pm and 6 am.

These are two different circumstances that consider the requirement of notice. However, they could be instructive when considering how and what notice is issued. Regardless of the subject matter of the notice - social media harms or specifically algorithmic feed harms - considerations should include what information would be conveyed in a label, where the label is placed, how the label should be displayed, and when. There is research available on the efficacy of warning labels on other products, like cigarettes and videogames. For example, research has found that the labels on cigarettes have been effective in raising the awareness of the health risks associated with smoking. However, the direct impact of these warning labels is more limited on chain smoking behavior.³⁵

As Surgeon General Murthy indicated this summer, “to be clear, a warning label would not, on its own, make social media safe for young people.”³⁶ However, providing parents with notice of the

³¹ Vivek H. Murthy, U.S. Surgeon General, *Surgeon General: Why I’m Calling for a Warning Label on Social Media Platforms*, NY Times (June 17, 2024), <https://www.nytimes.com/2024/06/17/opinion/social-media-health-warning.html>.

³² U.S. Senate, Stop the Scroll Act, found at: <https://www.fetterman.senate.gov/wp-content/uploads/2024/09/RIL24816.pdf>.

³³ National Association of Attorneys General Letter to Congressman Johnson and Senators Schumer and McConnell, *Requiring a Surgeon General’s Warning Label on Social Media Platforms*, (September 9, 2024), <https://ag.ny.gov/sites/default/files/letters/social-warning-label-letter.pdf>.

³⁴ HB 24-11136 (Co. 2024) <https://leg.colorado.gov/bills/hb24-1136>.

³⁵ Lara Salahi, *Warning labels could help regulate social media. But will it make us healthier?* Association of Health Care Journalists, (August 30, 2024), <https://healthjournalism.org/blog/2024/08/warning-labels-could-help-regulate-social-media-but-will-it-make-us-healthier/>.

³⁶ Murthy, *supra*.

harms of addictive feeds could be effective when combined with the regulations in the SAFE for Kids Act.

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

The OAG could ensure that the age determinations based on attestation from such entities are interoperable in terms of standards and signals. One way this could be done is through the adoption of standards and signals like the Global Privacy Control (GPC). California, Colorado and Connecticut have all passed legislation that mandates compliance with these global privacy signals. GPC is just one way that users can universally operate and tell all sites their data or preferences. It is a "browser-level signal, maintained either by a browser or a browser extension, that a user of privacy-focused technology can set."³⁷ Allowing for interoperability between different jurisdictions will benefit both businesses, who do not have to technically address a multitude of signals, as well as U.S. consumers, who will face less confusion and can more easily adopt a signal that works in multiple states.

Parental consent.

Verifiable parental consent under the OAG regulations should require "informed consent"; this would mean that the information that the parents are presented with educates the parents about the risks of the algorithmic feed and/or notifications. Not only should this information be provided to parents, but the information provided needs to be understandable to all communities.

(See [Common Sense Media's NY Child Data Protection Act](#) comments for further analysis of parental consent).

Regarding the concerns of New Yorkers that information provided for parental consent will be immediately and securely deleted, in Section 1501(3) the SAFE for Kids Act requires that data collected for age determination must not be used for any other purpose and must be deleted immediately. These regulations as drafted by the OAG should include an enforcement mechanism (like the ability to report violations) and a penalty for these types of data misuse.

Addictive social media platform.

In determining whether a platform uses an addictive feed as a "significant part" of the platform, the OAG should look at § 2, the legislative intent of the SAFE for Kids Act. This section identified that social media platforms process enormous amounts of data about users and these data points

³⁷ Implementing GPC for publishers doc found at: <https://globalprivacycontrol.org/Implementing%20GPC%20for%20Publishers.pdf>.

are filtered through “sophisticated machine learning algorithms, to create media feeds personalized to each user³⁸.” This section further identifies that these feeds “make predictions about interests, mood, and other factors related to what is most likely to keep users engaged for as long as possible, creating a feed tailor-made to keep each user on the platform for longer periods.” We know through internal documents received from some of the largest social media platforms that these social media platforms use a business model that prioritizes maximizing user engagement for profit over the health and safety of kids. Furthermore, according to the definition of “significant” found in Merriam-Webster, something is a significant amount or effect when it is “having or likely to have influence or effect.”³⁹

Combining the definition of significance as well as the legislative intent of the act, it seems that the addictive feed is significant if it is likely to have an influence or effect on the user and their experience with the platform.

General questions.

What information concerning the harms of addictive feeds to minors should OAG consider when drafting its regulations?

Social media companies use addictive feeds to get kids and teens to view and engage with platforms longer to make larger profits. For social media companies, time online equals more money. Addictive feeds have had an increasingly devastating effect on children and teens, contributing to significantly higher rates of youth depression, anxiety, suicidal ideation, and self-harm. Common Sense Media’s own research has shown that kids and teens are struggling to set their own boundaries when it comes to fielding the barrage of notifications (teens reported receiving an average of 237 notifications per day) from apps on their smartphones.⁴⁰ It was revealed in the multi-state lawsuit against Meta that Facebook and Instagram both moved to algorithmic (addictive) feeds after they learned through their own internal research that this type of feed would engage users for longer periods of time.⁴¹

As early as June of 2018, in an internal Facebook presentation called “Facebook ‘Addiction,’” it was acknowledged the “mindless” consumption of a feed and the fact that “it is easy to keep scrolling and go on frequently” make it “difficult to limit one’s use.”⁴² Then, in November of 2019, there was another internal presentation at a Meta company, this time Instagram. This presentation was called “IG Notification Systems Roadshow.” In this presentation, it was revealed that Instagram

³⁸ S.B. S7694A (N.Y. 2023), <https://www.nysenate.gov/legislation/bills/2023/S7694/amendment/A>.

³⁹ <https://www.merriam-webster.com/dictionary/significant>.

⁴⁰ Jenny S. Radesky et al., *Constant Companion: A Week in the life of a Young Person’s Smartphone Use*, Common Sense Media and University of Michigan Medical School (2023), https://www.common Sense Media.org/sites/default/files/research/report/2023-cs-smartphone-research-report_final-for-web.pdf.

⁴¹ *State of Arizona et al. v. Meta Platforms, Inc. et al.* (N.D. Cal Oct. 24, 2023), *Complaint for Injunctive and Other Relief*, 4:23-cv-05448-YGR Document 73-2. page 28, line 6.

⁴² *Id.*, page 23, line 2

users are “overloaded because they are inherently more susceptible to notification dependency.” Despite acknowledging users’ concerns that Instagram’s push notifications had the potential to “constantly harm . . . mental health,” the presentation did not propose any product changes to protect young users’ mental health — instead Meta decided to further investigate the mental health issue.”⁴³

Now, years after Meta (both Facebook and Instagram) knew of the harms they were causing to kids and teens, there is a growing body of research that reveals that addictive feeds are contributing to the mental health crisis. We know from the discovery in these lawsuits that the platforms continue to use addictive feeds that push harmful material to kids despite knowing they are contributing to this crisis because they drive user engagement.

According to Fairplay, “Instagram hosts more than 90,000 pro-eating disorder accounts, which reach more than 20,000,000 users, generating more than \$230 million in profits for Meta.”⁴⁴ According to the American Association of Pediatrics, the amount of emergency room visits for girls with eating disorders doubled since 2019.⁴⁵

And yet, platforms continue to use these addictive feeds to drive engagement - making more money at the expense of the well-being of children and teens.

⁴³ Multi-state lawsuit, page 53, line 3.

⁴⁴ Fairplay for Kids, *Designing for Disorder: Instagram’s Pro-eating Disorder Bubble* (April 2022), https://fairplayforkids.org/wp-content/uploads/2022/04/designing_for_disorder.pdf.

⁴⁵ Carley E. Milliren, MPH, et al. *Emergency Department Visits and Hospitalizations for Eating Disorders During the COVID-19 Pandemic*, American Academy of Pediatrics, (December 21, 2022), <https://publications.aap.org/pediatrics/article/151/1/e2022058198/190339/Emergency-Department-Visits-and-Hospitalizations?autologincheck=redirected>.