December 1, 2025

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

Re: Office of the New York Attorney General's Notice of Proposed Rulemaking pursuant to New York General Business Law section 1500 *et seq.*, the SAFE for Kids Act

Dear Attorney General James:

On behalf of the Computer & Communication Industry Association ("CCIA"),[1] I write in response to the Office of the New York State Attorney General's ("the OAG's") Notice of Proposed Rulemaking ("NPRM") pursuant to New York General Business Law section 1500 *et seq.*, the Stop Addictive Feeds Exploitation ("SAFE") for Kids Act.[2] CCIA previously submitted comments in response to the Advanced Notice of Proposed Rulemaking ("ANPRM").[3]

CCIA firmly believes that children are entitled to greater security and privacy online. Our members have designed and developed settings and parental tools to individually tailor younger users' online use to their developmental needs. For example, various services allow parents to set time limits, provide enhanced privacy protections by default for known child users, and other tools allow parents to block specific sites entirely.[4] This is also why CCIA supports implementing digital citizenship curricula in schools, to not only educate children on proper social media use but also help teach parents how they can use existing mechanisms and tools to protect their children as they see fit.

These comments provide some key considerations to ensure effective and balanced approaches to protecting online safety and privacy as the OAG refines the "Proposed Rules."[5] The OAG must avoid restrictive regulations that would effectively force online services to institute age verification to ensure compliance. Instead, policymakers should promote voluntary measures that do not jeopardize New Yorkers' sensitive personal information or inevitably cut many of them off from accessing protected speech.

Counter to peer-reviewed research and long-standing precedent, the Proposed Rules frame what is unconstitutional speech regulation as "addiction," as if that takes it outside the limits of state control. Deeming websites' protected editorial discretion to customize user preferences as "addictive" does not exempt government action from First Amendment scrutiny.

---

[1] CCIA is an international, not-for-profit trade association representing a broad cross section of communications and technology firms. For 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. A list of CCIA members is available at https://www.ccianet.org/members.

[2] *Available at* https://ag.ny.gov/press-release/2025/attorney-general-james-releases-proposed-rules-safe-kids-act-restrict-addictive.

[3] CCIA Comments to Office of the New York State Attorney General on Advanced Notice of Proposed Rulemaking on SAFE For Kids Act (Sept. 26, 2024), https://ccianet.org/library/ccia-comments-on-ny-anpr-safe-for-kids-act/.

[4] Competitive Enterprise Institute, *Children Online Safety Tools*, https://cei.org/children-online-safety-tools/ (last updated June 10, 2025).

[5] *Available at* https://ag.ny.gov/sites/default/files/regulatory-documents/safe-for-kids-act-nprm.pdf.

Limiting children's access to online services curtails their First Amendment right to information accessibility.

A lack of narrowly tailored definitions could incentivize businesses to simply prohibit minors from using digital services rather than face potential legal action and hefty fines for non-compliance. The First Amendment, including the right to access information, applies to teens.[6] Moreover, requiring businesses to deny access to social networking sites or other online resources may also unintentionally restrict children's ability to access and connect with like-minded individuals and communities. For example, children of certain minority groups may not live in an area where they can easily connect with others that represent and relate to their own unique experiences, so an online central meeting place where kids can share their experiences and find support can have positive impacts.[7]

Due to the nuanced ways in which people under the age of 18 use the internet, it is also imperative to appropriately tailor such treatments to respective age groups. For example, if a 16-year-old is conducting research for a school project, it is expected that they would come across, learn from, and discern from a wider array of materials than a 7-year-old on the internet playing video games. Any definition of "child" or "minor" should be a user under the age of 13 to align with the federal Children's Online Privacy Protection Act (COPPA) standard. Aligning the definition with COPPA ensures consistency with longstanding federal policy and avoids overlapping or conflicting obligations for covered services. This would also allow for those over 13, who use the internet much differently than their younger peers, to continue to benefit from its resources.

For similar reasons, the OAG should adhere to COPPA's definition of "verifiable parental consent"[8] rather than crafting a narrower one. A definition that denies New York businesses the ability to adopt federally accepted methods of showing parental consent disincentivizes businesses from serving both adults and minors in the state without any compensating benefit to online safety.

Terms such as "addiction" or "addictive" in an online context lack an adequate scientific foundation.

The Proposed Rules use definitions for "addictive social media platform," "addictive feed," and "addictive features." However, humans engage in various compulsive and repetitive behaviors — some of which may negatively impact physical and/or mental health. These could range from binge eating unhealthy foods to exercising excessively to watching favorite shows for hours on end. However, these behaviors do not necessarily amount to clinical "addictions." There is no single clinical definition or universally accepted diagnostic criteria for "social media addiction," nor is it recognized as a formal disorder in the American Psychiatric Association's (APA) Diagnostic and Statistical Manual of Mental Disorders (DSM-5-TR) or by the WHO's International Statistical Classification of Disease (ICD-11). In fact, the most recent edition of the Diagnostic and Statistical Manual of Mental Disorders: Fifth Edition Text Revision (DSM-5-TR) declined to include definitions for "Internet gaming disorder," "Internet addiction,"

[6] *See, e.g.*, *Brown v. Ent. Merchs. Ass'n*, 564 U.S. 786, 795 (2011).
[7] *The Importance of Belonging: Developmental Context of Adolescence*, Boston Children's Hospital Digital Wellness Lab (Oct. 2024), https://digitalwellnesslab.org/research-briefs/young-peoples-sense-of-belonging-online/.
[8] *See* 15 U.S.C. § 6501(9) (1998).

"excessive use of the Internet," or "excessive use of social media," noting that "[g]ambling disorder is currently the only non-substance-related disorder included in the DSM-5-TR chapter 'Substance-Related and Addictive Disorders.'"[9]

The connected nature of social media has led some to allege that online services may be negatively impacting teenagers' mental health. However, the full body of scientific research does not support a causal relationship between social media and mental health harms in teens. As such, researchers explain that this theory is not well supported by existing evidence and repeats a 'moral panic' argument frequently associated with new technologies and modes of communication since the advent of the printing press, from dime novels, comic books, and fashion magazines, to rap CDs, video games, and Blackberry phones.[10] Instead, social media effects are nuanced,[11] individualized, reciprocal over time, and gender-specific — with many studies citing benefits of social media to teens, as well.

Much research on social media and adolescent health (including the National Academies of Sciences, the University of Oxford, the American Psychological Association, and the Journal of Pediatrics) has found that social media does not cause changes in adolescent health at the population level.[12] Even the Surgeon General's Social Media and Youth Mental Health advisory acknowledges the benefits of social media, including social connection, information sharing, and civic engagement.[13] Indeed, as a federal court recently noted, "nearly all of the research showing any harmful effects" for minors on social media "is based on correlation, not evidence of causation."[14]

Because of age verification's constitutional problems, the OAG should hold covered operators to an actual knowledge standard.

Several federal courts have held that laws requiring age verification and parental consent for social media sites violate the First Amendment's guarantee of free speech. Federal courts in Ohio and Georgia have held that states cannot "prevent children from hearing or saying anything without their parents' prior consent."[15] An Arkansas court further held that "such laws do not enforce parental authority over children's speech . . . ; they impose *governmental* authority, subject only to a parental veto."[16] New York proposes a similar state-mandated system within the Proposed Rules, and does not allow parents to make decisions about their

[9] Am. Psychiatric Ass'n, *Diagnostic and Statistical Manual of Mental Disorders: Fifth Edition Text Revision* (2022).
[10] Alvaro Marañon & Dalia Wrocherinsky, *Public Panics and Youth Online Safety — A Deep Dive*, Disruptive Competition Project (July 7, 2023), https://project-disco.org/featured/public-panics-and-youth-online-safety-a-deep-dive/.
[11] Amy Orben et al., *Social Media's Enduring Effect on Adolescent Life Satisfaction*, PNAS (May 6, 2019), https://www.pnas.org/doi/10.1073/pnas.1902058116.
[12] Regina Park, *The Internet Isn't Harmful to Your Mental Health, Oxford Study Finds*, Disruptive Competition Project (Jan. 29, 2024), https://project-disco.org/innovation/the-internet-isnt-harmful-to-your-mental-health-oxford-study-finds/.
[13] Mike Masnick, *Warning: Believing The Surgeon General's Social Media Warning May Be Hazardous To Teens' Health*, Techdirt (June 18, 2024), https://www.techdirt.com/2024/06/18/warning-believing-the-surgeon-generals-social-media-warning-may-be-hazardous-to-teens-health/.
[14] *NetChoice v. Yost*, 778 F. Supp. 3d 923, 955 (S.D. Ohio 2025).
[15] *Id.* at 954; *NetChoice v. Carr*, 789 F. Supp. 3d 1200, 1224 (N.D. Ga. 2025) (each quoting *Brown v. Ent. Merchs. Ass'n*, 564 U.S. at 795 n. 3 (2011)).
[16] *NetChoice v. Griffin*, No. 23-cv-05105, 2025 WL 978607 at *31 (W.D. Ark. Mar. 31, 2025) (quoting *Brown*, 564 U.S. at 795 n. 3).

child's internet use. Numerous other federal judges have placed similar laws wholly or partially on hold until challenges can be fully reviewed.[17]

An age verification mandate would curtail individuals' ability to tailor their content preferences and violate their privacy.

Both digital and physical products can have effective child safety features installed on them, even if they are primarily designed for adults. For example, bicycles are designed for general use by adults, with standard frames and safety features like reflectors and brakes. However, parents can choose to add training wheels, smaller seats, or handlebar attachments to make the bicycle safer and more suitable for a child. Likewise, many devices and services have content filtering technologies that allow parents to individually tailor settings and preferences to select age-appropriate content for themselves and their children. These types of filters and settings, however, are not activated by default.

Regulations that force covered businesses to activate settings for minors by default should therefore be avoided. Such mandates violate the First Amendment, with the Supreme Court holding that governments may not "suppress[] a large amount of speech that adults have a constitutional right to receive and to address to one another" merely to "deny minors access to potentially harmful speech."[18]

In addition to ensuring age-appropriate experiences, the ability to curate and personalize feeds lets all users explore their interests and form communities. Restrictive regulations of personalized feeds and algorithmic rankings impede digital services' ability to provide their users with the relevant content they expect to receive. Forcing businesses to activate default settings for minors therefore creates significant problems for adults who wish to use the covered services. Many will be unwilling to forgo their constitutional right to access such speech anonymously,[19] and may not even possess the requisite forms of ID.

Even well-meaning proposals requiring individuals to share sensitive personal information with third parties, including IDs or biometrics, can make recipients a prime target for cyberattacks or data breaches.[20] The collection of detailed personal information about children—and adults—creates massive amounts of data that criminals will attempt to target for purposes of identity theft. Moreover, the NPRM requires individuals to share personal information with many different services with data protection measures of varying strengths, compounding the security risks. Furthermore, government officials could access this sensitive data through enforcement inquiries and processes. The ID requirements also incentivize criminals to pose as covered services and obtain user IDs through phishing scams. Such policies run contrary to the data minimization principles underlying federal and international best practices for privacy protection, for precisely these reasons.[21]

---

[17] *See, e.g.*, *NetChoice v. Bonta*, 770 F. Supp. 3d 1164 (N.D. Cal. 2025); *NetChoice v. Bonta*, No. 25-146 (9th Cir. Sept. 9, 2025); *CCIA v. Paxton*, 747 F. Supp. 3d 1011 (W.D. Tex. 2024); *NetChoice v. Reyes*, 748 F. Supp. 3d 1105 (D. Utah 2024).
[18] *Reno v. ACLU*, 521 U.S. 844, 874 (1997).
[19] *See, e.g.*, *Am. Booksellers Found, v. Dean*, 342 F.3d 96, 99 (2d Cir. 2003); *ACLU v. Mukasey*, 534 F.3d 181, 197 (3d Cir. 2008); *NetChoice v. Griffin*, No. 23-cv-05105, 2025 WL 978607 at *20-21 (W.D. Ark. Mar. 31, 2025).
[20] *Age-Verification Legislation Discourages Data Minimization, Even When Legislators Don't Intend That,* R St. Inst. (May 24, 2023), https://www.rstreet.org/commentary/age-verification-legislation-discourages-data-minimization-even-when-legislators-dont-intend-that/.
[21] *See, e.g.*, *Fair Information Practice Principles (FIPPs)*, Fed. Privacy Council, https://www.fpc.gov/resources/fipps/; *Principle (c): Data Minimisation,* U.K. Info. Comm'r Off.,

The proposed rulemaking's decade-long data retention requirement compounds all of these risks — an excessive length of time inconsistent with standard data minimization practices. This component of the proposed rulemaking dangerously assumes that all covered online services, including new and emerging ones, have the infrastructure to securely store millions of users' private information for an unreasonable and arbitrary duration of time. Many such services will not have these capabilities, exposing users to the privacy risks noted above.

For these reasons, CCIA believes that targeted protections, including parental controls, filtering tools, and media literacy education, offer greater safety than age verification mandates. By working with businesses to continue their ongoing private efforts to implement safety and security mechanisms, the state can provide greater flexibility for families and service providers alike, and better safeguard free speech and privacy. The Proposed Rules would establish a state-mandated system for determining users' age. This approach limits parents' ability to make personalized decisions about their child's internet use. Rather, it would substitute a one-size-fits-all state requirement for parents' personal judgment.

Current age determination tools estimate users' ages imperfectly.

Even with the Proposed Rules using requirements such as "commercially reasonable" and "privacy-preserving," various privacy and security concerns remain. There is no perfect method of age determination, and the more data a method collects, the greater risk it poses to consumer privacy[22] and small business sustainability.[23] A recent Digital Trust & Safety Partnership (DTSP) report, *Age Assurance: Guiding Principles and Best Practices*, contains more information regarding guiding principles for age assurance and how digital services have used such principles to develop best practices.[24] The report found that "smaller companies may not be able to sustain their business" if forced to implement costly age verification or assurance methods, and that "[h]ighly accurate age assurance methods may depend on collection of new personal data such as facial imagery or government-issued ID."[25]

Furthermore, the Proposed Rules include confusing and conflicting "accuracy minimum" and "total accuracy minimum" provisions containing several infeasible mandates. These include requiring a 98% rate of detecting method circumvention and various false positive rates, and an unclear ongoing obligation to monitor and "address the detection of new or previously undetected forms of method circumvention in real time." This proposal creates an unrealistic standard for age verification accuracy and circumvention. Given the technical infeasibility of maintaining such accuracy rates, covered operators may opt for recognition methods that overclassify users as minors out of caution. Many adults would thus be inadvertently denied access to services with personalized feeds. The Proposed Rules should allow covered operators to adopt age assurance methods that best protect their users rather than institute rigid accuracy targets that will block access to protected speech for minors and adults.

---

https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/data-minimisation/.

[22] Kate Ruane, *CDT Files Brief in* NetChoice v. Bonta *Highlighting Age Verification Technology Risks* (Feb. 10, 2025), https://cdt.org/insights/cdt-files-brief-in-netchoice-v-bonta-highlighting-age-verification-technology-risks/.

[23] Engine, *More Than Just a Number: How Determining User Age Impacts Startups* (Feb. 2024), https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/66ad1ff867b7114cc6f16b00/1722621944736/More+Than+Just+A+Number+-+Updated+August+2024.pdf.

[24] *Age Assurance: Guiding Principles and Best Practices*, Digital Trust & Safety Partnership (Sept. 2023), https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf.

[25] *Id.* at 10.

Additionally, age estimation software will sometimes classify adults as minors, or vice versa, and does not process all populations with equal accuracy. The National Institute of Standards and Technology (NIST) recently published a report evaluating six software-based age estimation and age verification tools that estimate a person's age based on the physical characteristics evident in a photo of their face.[26] The report notes that facial age estimation accuracy is strongly influenced by algorithm, sex, image quality, region-of-birth, age itself, and interactions between those factors, with false positive rates varying across demographics, generally being higher in women compared to men. CCIA encourages policymakers to consider the current technological limitations in providing reliably accurate age estimation tools across all demographic groups.

Even in proposals that do not explicitly mandate age verification, businesses often need to *determine the age of all users* to ensure that they can adhere to the regulations regarding minors. As explained above, this in turn requires using invasive age verification methods that force businesses to collect sensitive personal identifying information about their users.[27]

Time-based notification restrictions undermine user privacy.

In Section 700.3, the "OAG proposes a default prohibition of nighttime notifications from covered operators to covered users" who do not provide age assurance or parental consent. Such requirements inevitably require that covered operators track when it is nighttime in a given device's location. This requirement therefore effectively mandates location-based tracking of minors' devices, thus undermining the privacy of the very population the Proposed Rules are designed to protect. Requiring covered operators to track their users serves no benefit, particularly since covered operators regularly offer users the option to turn off notifications themselves.

* * * * *

For the above reasons, the OAG should avoid prescriptive regulations that compel age verification or restrict lawful design features. Instead, CCIA recommends the support of flexible, evidence-based approaches that respect privacy, parental choice, and constitutional rights. We appreciate your consideration of these comments. CCIA looks forward to continuing to participate in the ongoing regulatory process, including reviewing and providing feedback on any revised rules or regulations. We hope you will consider CCIA a resource as these discussions progress.

Respectfully submitted,

Kyle J. Sepe
Regional State Policy Manager, Northeast
Computer & Communications Industry Association

[26] Kayee Hanaoka et al., *Face Analysis Technology Evaluation: Age Estimation and Verification (NIST IR 8525),* Nat'l Inst. Standards & Tech. (May 30, 2024), https://doi.org/10.6028/NIST.IR.8525.
[27] Berin Szóka, *Comments of TechFreedom In the Matter of Children's Online Privacy Protection Rule Proposed Parental Consent Method; Application of the ESRB Group for Approval of Parental Consent Method*, TechFreedom (Aug. 21, 2023), https://techfreedom.org/wp-content/uploads/2023/08/Childrens-Online-Privacy-Protection-Rule-Proposed-Parental-Consent-Method.pdf.