Response by the Centre for Information Policy Leadership to the Notice of Proposed Rulemaking regarding the Stop Addictive Feeds Exploitation (SAFE) for Kids Act

Submitted December 1, 2025

The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to provide feedback to the Notice of Proposed Rulemaking (NPRM)[2] regarding the Stop Addictive Feeds Exploitation (SAFE) for Kids Act,[3] which enters into effect on the 180th day after the Office of the Attorney General (OAG) promulgates rules and regulations necessary to effectuate the provisions of the Act.[4]

CIPL recognizes the importance of designing and delivering appropriate online environments for children[5] and has continuously worked to identify effective and practical solutions that can ensure the protection of children online so they can participate and thrive in the digital space. In April 2021, CIPL launched a special global project on children's privacy and, in October 2022, published a detailed Policy Paper on international issues and compliance challenges.[6] Among the issues identified for further exploration was the use of age assurance and its impact on children's privacy and safety.

In recognition of the importance of appropriate age assurance, CIPL, together with WeProtect Global Alliance, created a Multistakeholder Dialogue on Age Assurance[7] to further drive the discussion and

---

[1] **The Centre for Information Policy Leadership (CIPL)** is a global privacy and data policy think tank within the Hunton law firm that is financially supported by the firm, 85+ member companies that are leaders in key sectors of the global economy, and other private and public sector stakeholders through consulting and advisory projects. CIPL's mission is to engage in thought leadership and develop best practices for the responsible and beneficial use of data in the modern information age. CIPL's work facilitates constructive engagement between business leaders, data governance and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at www.informationpolicycentre.com. Nothing in this document should be construed as representing the views of any individual CIPL member company or Hunton. This document is not designed to be and should not be taken as legal advice.

[2] See https://ag.ny.gov/resources/individuals/consumer-issues/technology/protecting-children-online.

[3] N.Y. Gen. Bus. Law § 1500 *et seq.*

[4] See 2024 N.Y. Laws ch. 120, Sec. 3.

[5] For the purpose of this consultation and unless otherwise noted, CIPL will use the terms *child*, *children*, and *minor* to refer to persons under the age of 18. CIPL recognizes that the Colorado Privacy Act defines a "child" as individual under the age of 13, Colo. Rev. Stat. § 6-1-1303(4), and that the Children's Privacy Amendment defines a "minor" as any consumer under the age of 18, Colo. Rev. Stat. § 6-1-1303(16.5) (effective Oct. 1, 2025).

[6] CIPL Policy Paper (2022) *International Issues and Compliance Challenges*, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_childrens_privacy_policy_paper_i_-_international_issues___compliance_challenges__21_oct_2022_.pdf.

[7] The takeaways from these discussions are available on CIPL's website:

- Roundtable 1 (March 2024), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/key_takeaways_from_a_multi-stakeholder_dialogue_on_age_assurance.pdf.

Copyright © 2025 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

explore best practices. This dialogue has involved a diverse range of stakeholders, including child rights organizations, privacy and safety regulators, academia, lawmakers, government representatives, civil society, age assurance providers, and industry representatives. These Multistakeholder Dialogues are ongoing, and we welcome the OAG's participation at future meetings.

In September 2024, CIPL issued a discussion paper focusing on U.S. state legislation requiring the use of age verification measures, with the goal of identifying technical, practical, and legal challenges affecting stakeholders and society more broadly.[8] We followed up with a Roundtable held in San Francisco that addressed these challenges, and we published our takeaways from that discussion.[9]

In light of our research and our work in this space, CIPL supports strong protections for the privacy, safety, and security of minors online. We support robust privacy-by-design requirements and the use of a balanced, risk-based approach that recognizes the positive role of system design features when responsibly implemented. CIPL seeks to foster the development of context-specific risk taxonomies to assist companies in employing measures that are proportionate and appropriate to potential harms and do not restrict minors' access to beneficial, age-appropriate content and services.

In addition, CIPL notes that delivering effective privacy and safety protections for children and teens online requires more than mere compliance with the letter of the law. For more than a decade, CIPL has pioneered organizational accountability as a key building block of effective data privacy regulation and its corresponding implementation within companies. Indeed, **CIPL's Accountability Framework**[10] (see Figure 1 below) is a recognized standard for the development of best-in-class data privacy protections and responsible business practices. It identifies seven essential elements of organizational

---

- Roundtable 2 (July 2024), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_weprotectglobalalliance_key_takeaways_age_assurance_law_and_regulation.pdf.
- Roundtable 3 (September 2024), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_weprotectglobalalliance_keytakeaways_multistakeholderdialogue_sep24.pdf.
- Roundtable 4 (October 2024), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/oct_22_key_takeaways_final.pdf.
- Roundtables 5 & 6 (October–November 2024), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_weprotect_a_multistakeholder_dialogue_on_age_assurance_law_and_regulation_apr25.pdf.
- Roundtable 7 (June 2025), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-weprotect_global_alliance_-_considerations_towards_an_interoperable_assurance_framework_nov25.pdf.

[8] CIPL Discussion Paper: *Age Assurance & Age Verification Laws in the United States*, September 24, 2024, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_age_assurance_in_the_us_sept24.pdf.

[9] *Takeaways from CIPL Roundtable: The State of Play in Age Assurance in the US*, October 2024, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/the_state_of_play_in_age_assurance_in_the_us_-_key_takeaways_oct24.pdf.

[10] See CIPL resources and papers on organizational accountability: https://www.informationpolicycentre.com/organizational-accountability.html.

Copyright © 2025 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

accountability and can serve as a starting point for setting up a meaningful accountability program within an organization.

Figure 1

CIPL strongly believes that accountability is a modern and future-proof concept that can be applied to all digital regulation and corporate compliance. Meaningful and demonstrable accountability will ensure effective governance within an organization, placing the responsibility and discretion of how to operationalize legal obligations into risk-based controls, policies, procedures, and tools, commensurate with their business models and internal set-up.[11]

Specifically regarding age assurance, CIPL recommends that:

- The deployment of effective age assurance methods should follow a risk-based and proportionate approach. This means that age assurance measures should be appropriate and proportionate to the context and level of risk. Therefore, they should not apply to services that present minimal risk. Nor should they apply indiscriminately to adult users.
- Age assurance measures should also be based on the specific issue being addressed, the context, and the type of services and products offered to children.

To make sure that the age assurance measures correspond to the risks children face when they navigate online content, risk assessments should incorporate the following considerations:

- Risk assessments should be holistic, addressing both safety and privacy risks.
- Companies must be able to demonstrate the effectiveness of age assurance solutions in the context of their service and provide evidence of how these solutions mitigate the assessed risk and their efficacy.
- As services develop and the online environment evolves, risks will change. This means that risk assessments should not be a one-time exercise, but a flexible and continuous process.

[11] CIPL Accountability Discussion Paper 1 - The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society, July 23, 2018 https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf

Copyright © 2025 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

- Clear, nuanced and commonly understood risk taxonomy is needed to provide a structured way to understand, categorize, and assess various types of risks (e.g., high, medium, low), so that appropriate and effective age assurance measures can be implemented.

Age assurance should not only be seen as a measure to exclude children from inappropriate content but also as a tool to enable access to age-appropriate, tailored experiences. Knowing a child's age or age bracket can help ensure that children receive suitable content, thereby supporting both children's online engagement and safer online experiences, avoiding unnecessary restrictions or overprotection that could limit minors' access to beneficial, age-appropriate content and services. For example, recommender systems can serve as a risk-minimizing measure by tailoring content appropriately, helping to strike a balance between offering personalized experiences and maintaining safety.

It is important that age assurance measures are user-friendly and easy for both children and parents to understand and use. They should maximize accessibility and offer alternative paths for users who cannot successfully pass initial age assurance (e.g., adapt approaches for those who have different needs based on socio-economic status, disabilities, etc.) to avoid impacting user rights. This means that they should also be equitable and work appropriately for all users, including those from marginalized communities or those who may lack government-issued IDs.

At the same time it is important to understand that age assurance is not a silver bullet or a standalone solution, but rather a part of broader compliance and accountability measures for online safety and privacy. Accountability means that parents', guardians' and children's perspectives have an important role to play in the context of effective age assurance and should not be overlooked in the design and implementation of age assurance measures. In particular, young people can offer unique perspectives and valuable feedback on the ease, effectiveness, and utility of a given methodology.

Additionally, CIPL believes that working towards further standardization, including the development of interoperable age assurance solutions to aid a streamlined processes and reduce repeated checks across multiple services, is crucial for the protection and safety of children online. Any age assurance framework must balance privacy, security, competition, cost, and liability. It is also important to incentivize the application of Privacy-Enhancing Technologies (PETs) in age assurance to verify age without requiring access to excessive personal data, thereby upholding privacy and data minimization. CIPL supports the practical use of PETs, such as Zero Knowledge Proof (ZKP) technologies, for implementing effective age assurance mechanisms. Age assurance solutions should consistent with principles of privacy and safety by design, meaning that data minimization, storage limitation, and data security must be considered along with the necessity of processing data in a manner consistent with the perceived risk.

In addition to our above commentary on age assurance, CIPL offers recommendations on the following specific provisions.

700.1(c) – Addictive Feed

- CIPL recommends to clarify that a *Feed* does not include a home screen, menu, or search page that provides links, thumbnails, or exemplary images of content to connect to specific content.

700.1(d) – Addictive Online Platform

- CIPL notes that the definition of an addictive online platform under the NPRM is ambiguous and submits that the subject remains highly contested. Regardless, CIPL recommends

Copyright © 2025 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

increasing the threshold from 20% to 50% to better align with text's underlying assumption that the feed comprises "a **significant** part of the services."

700.1(y) – Monthly Active User.

- CIPL recommends providing a threshold to clarify that a feed on which a user spends less than 30 minutes cumulatively each day would be out-of-scope.
- CIPL recommends amending the definition of *Monthly Active User* to require an element of intentionality and/or interaction with the platform, so as not include, for example, passive users who merely keep an app open in the background.

700.2(e) & 700.3(e) – Verifiable parental consent requirements

- CIPL recommends clarifying the process of obtaining consent from the minor. For example, is the request of the minor to obtain parental consent commensurate with the minor's consent, or does this involve two different steps?

Copyright © 2025 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.