December 2, 2025

The Honorable Brett Guthrie
Chair
House Energy and Commerce Committee
U.S. House of Representatives
Washington, DC 20515

The Honorable Frank Pallone, Jr.
Ranking Member
House Energy and Commerce Committee
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Guthrie and Ranking Member Pallone:

On behalf of National Taxpayers Union (NTU), the nation's oldest taxpayer advocacy organization, I write to express our views on the latest draft of the Kids Online Safety Act (KOSA). While NTU appreciates the continued efforts to improve online safety and acknowledges that recent changes represent meaningful progress, we urge Congress to exercise caution. Several of the core concerns that NTU outlined in earlier letters have been only partially resolved, and the current draft still risks introducing significant unintended consequences for online privacy, regulatory accountability, and user rights.

I. The Narrower Definition of "Harm" Is a Meaningful Improvement, but Important Structural Issues Remain

One of the most significant changes in the latest draft is the narrower definition of "harm." An earlier version included issues such as anxiety, depression, and eating disorders, which made the scope of the bill considerably broader. The latest draft no longer includes these categories, resulting in a more limited set of harms.

The revised KOSA more specifically targets "physical violence," "sexual exploitation and abuse," the distribution and sale of narcotics, alcohol, and cannabis products to minors, and financial harms arising from deceptive practices. This revision represents a more targeted approach and provides greater clarity about what the legislation is intended to cover.

However, the incentives that would lead platforms to install age verification and monitor online activities for potential liability—as was the case with earlier drafts—remain largely unchanged. The bill continues to tie liability to whether a company has "actual knowledge" or has acted in "willful

disregard" of a user's age. In practice, this structure could still encourage companies to monitor user behavior to manage compliance risk, with significant implications for privacy. These implications are more pronounced in the United States, where—unlike in the European Union, Japan, or the United Kingdom—there is no comprehensive federal privacy framework governing how such information should be collected, stored, or used. As a result, the narrower definition of harm is a meaningful improvement, but it does not resolve the broader questions concerning privacy and the extent of user monitoring under the bill.

II. The Consolidated Knowledge Standard Simplifies the Statute but Overlooks Key Differences Among Platforms

The latest draft eliminates the tiered knowledge standards that previously applied different thresholds depending on a platform's size and user base. The new version adopts a single standard—"actual knowledge" or "willful disregard"—for all covered services. This revision streamlines the statute but removes distinctions that were intended to reflect the operational differences between large, general-purpose platforms and smaller or more specialized services.

The unified standard does not account for the varied ways in which different platforms interact with users or the extent to which age information is relevant to their core functions. As a result, platforms with very different architectures may face similar liability exposure, even though their ability to assess or document age-related signals differs substantially. This raises practical questions about how smaller or more specialized services can satisfy the standard without introducing monitoring or documentation practices that are disproportionate to their size, technical capacity, or risk profile.

In this respect, the revised draft improves the structure of the statute but leaves open how the same knowledge standard should apply across services with markedly different risk profiles, user interactions, and technical capabilities.

III. Lack of Statutory Standards Creates Uncertainty About Compliance Obligations

The revised KOSA includes several obligations requiring platforms to establish, implement, and maintain a range of safeguards and internal processes. However, the statute does not specify what constitutes an adequate response to these requirements or how companies should demonstrate compliance. The draft also leaves open whether future rulemakings or enforcement actions will provide this detail, which makes it difficult for companies to anticipate how these obligations will be interpreted in practice.

The legislation includes several obligations requiring platforms to establish, implement, and maintain a range of safeguards and internal processes. However, it does not specify what constitutes an adequate response to these requirements or how companies should demonstrate compliance. The draft also leaves open whether future rulemakings or enforcement actions will supply this detail, which makes it difficult for companies to anticipate how these obligations will be interpreted in practice.

This uncertainty is particularly relevant for platforms that do not operate as traditional social media services or that function at a smaller scale. Without more detailed statutory guidance, there is a risk that compliance expectations may be interpreted differently across jurisdictions or enforcement contexts. These questions are also closely tied to the bill's new audit requirements, since unclear compliance standards may lead to differing expectations about what auditors must review or evaluate. Additional clarity would help ensure that companies understand what is required of them and that the framework is applied consistently across services with different operating models and risk profiles.

IV. Unclear Audit and Reporting Requirements Create Privacy and Implementation Challenges

The latest KOSA draft adds annual independent audits and expanded reporting obligations for covered services. These provisions require companies to disclose detailed information about their internal policies, technical safeguards, and data practices involving minors. While intended to strengthen oversight, several elements of the audit framework remain insufficiently defined.

First, the statute does not specify the limits on what information auditors may access or how sensitive operational materials should be handled. Given the nature of the documents involved—including internal system architecture, data-flow descriptions, and content-moderation processes—clearer parameters would help reduce the risk that audit activities expose confidential information or introduce additional privacy and security concerns.

Second, the latest draft does not indicate what standards auditors should apply or how services should demonstrate that they satisfy the bill's requirements. Without clear statutory criteria, companies may face uncertainty about the level of detail expected in their documentation, and auditors may reach different conclusions about what constitutes compliance. These uncertainties may affect services differently, particularly those with fewer resources or more specialized operating models.

Greater specificity regarding the scope, methodology, and protections associated with the audit process would help ensure that the framework can be implemented predictably and in a manner that protects both user privacy and sensitive operational information.

V. Enforcement Consistency and Regulatory Interpretation Remain Uncertain

The revised KOSA grants enforcement authority to both the Federal Trade Commission and state attorneys general. While this dual structure mirrors other federal statutes, the bill does not clarify how enforcement priorities should be coordinated or how differing interpretations should be reconciled. Where compliance standards are articulated in general terms or left undefined, this lack of coordination may lead to variation in how the statute is applied across jurisdictions.

Several of the bill's obligations also rely on terms that are not defined with precision—including what constitutes adequate safeguards, appropriate internal processes, or sufficient documentation. Because these concepts are not further specified, companies may face uncertainty about how they will be

evaluated by different enforcement bodies. Divergent interpretations could result in uneven expectations for services operating nationwide.

Greater clarity on the respective roles of federal and state enforcement, as well as more defined criteria for assessing compliance, would help ensure that the framework is implemented in a consistent and predictable manner.

Conclusion

While the latest draft of KOSA includes meaningful improvements, significant questions remain about how the statute would operate in practice. The uncertainties outlined above—particularly with respect to compliance expectations, age-related liability incentives, audit requirements, and enforcement—suggest that the bill may introduce new privacy and operational risks without providing sufficient clarity for platforms or user

For these reasons, we remain concerned about the current framework and do not believe the draft is ready to be advanced in its present form. The National Taxpayers Union appreciates Congress's consideration of these issues and stands ready to assist as lawmakers evaluate the most effective and proportionate ways to support youth online safety while safeguarding user privacy.

Sincerely,

Ryan Nabil
Director of Technology Policy and Senior Fellow
National Taxpayers Union
122 C St NW, Suite 700
Washington, DC 20001