



July 25, 2024

The Honorable Charles E. Schumer
Majority Leader
United States Senate
Washington, DC 20510

The Honorable Mitch McConnell
Minority Leader
United States Senate
Washington, DC 20510

Re: National Taxpayers Union's View on KOSA and COPPA 2.0

Dear Majority Leader Schumer, Minority Leader McConnell, and Members of the U.S. Senate:

On behalf of the National Taxpayers Union (NTU), the nation's oldest taxpayer advocacy organization, I write to express our views on the Kids Online Safety Act ([KOSA](#)) and the amended Children and Teens' Online Privacy Protection Act ([COPPA 2.0](#)). NTU applauds the Senate for its continued efforts to advance legislation to promote online safety and privacy. However, given several concerns associated with this legislation, NTU stands in opposition to the two bills and urges you to vote against the legislation, as explained below.

I. Summary

a) The Kids Online Safety Act (KOSA)

While Congressional efforts to protect online safety and privacy for young people are laudable, KOSA would significantly increase surveillance and privacy risks for all internet users.

We believe that KOSA rightly identifies a growing range of social and mental health challenges that American youth face today, including anxiety, depression, and substance use. A growing body of evidence suggests that these issues increasingly affect the youth in the [United States](#) and across the developed world, including many [European countries](#). Some of these issues, like [depression](#) and [substance use](#), are also on the rise in adult populations—suggesting a multifaceted, broader systemic challenge for the United States and beyond.

However, KOSA's main problem is that it seeks to solve complex societal and mental health issues through technical solutions for online platforms and websites. We believe that no single technical solution can adequately address the complex challenges that increasingly affect youth in the United States and beyond. On the contrary, by holding online platforms and websites responsible for all sorts of societal ills, KOSA would provide an incentive to increase surveillance of users of all ages. While the legislation does not prescribe a specific age verification method, its language potentially provides a backdoor for regulators to mandate such a requirement later, which could exacerbate data privacy and security risks for all users.

b) The Amended Children and Teens' Online Privacy Protection Act (COPPA 2.0)

Whereas KOSA proposes to create a new legal framework for online harm, COPPA 2.0 seeks to update [COPPA](#), initially passed in 1998. While COPPA 2.0 might be less expansive than KOSA in scope, several of its proposals risk creating unintended consequences for online privacy and regulatory accountability while restricting access to many

online platforms and services for American users aged 13 to 15. Finally, like KOSA, COPPA 2.0 grants the Federal Trade Commission significant enforcement authority without establishing mechanisms to ensure regulatory neutrality and accountability.

II. KOSA's Mandatory Age Verification Would Increase Surveillance and Privacy Risks for All Users

Unlike earlier drafts, the latest KOSA draft does not directly mandate age verification. Instead, it proposes a study to evaluate “the most technologically feasible methods and options for developing systems to verify age at the device or operating system level” ([KOSA](#) §9(a)). However, at a time when age verification systems are increasingly [gaining](#) popularity at the state level, the language of Section 9 potentially creates a backdoor through which regulators could implement an invasive age verification requirement. That is especially concerning considering that 18 states have already [established](#) age verification requirements for certain websites, several of which are currently subject to legal challenges in the respective state courts.

The bill's sponsors, such as Senator Richard Blumenthal (D-CT), [emphasize](#) that it “does not impose age verification requirements or require platforms to collect more data about users (government IDs or otherwise).” Others might highlight the growing [availability](#) of alternative forms of identity verification, including credit cards, cellphone registration, or facial age estimation techniques. Yet, these identification systems often carry privacy and security risks of their own, especially depending on how they are implemented. These age-verification methods would also [apply](#) to *all* users—not only those below the statutory minimum age.

Furthermore, even with less intrusive (and potentially less accurate) [forms](#) of identity verification, businesses have an incentive to minimize potential risks and costs by asking all users for government-issued identification. At a time when Congress has not established a federal privacy law and the misuse of sensitive private data and cyberattacks are increasingly common, the proposed legislation could add new vulnerabilities for the sensitive personal data of U.S. adults and youth—from biometric data to financial information and social security numbers.

In this context, a comparison with minimum-age drinking might provide a helpful, albeit imperfect, frame of reference. The 1984 Federal Uniform Drinking Age Act [established](#) 21 as the minimum national drinking age in the U.S. As for KOSA, this law's provisions are intended to apply to underage consumers since it only forbids serving alcohol to those under 21. However, drinking establishments must establish whether a customer is 21 or older by asking for an ID to avoid liability. Wanting to avoid penalties, bars often err on the side of caution, with the result that customers might be asked for identification even if they are well above the drinking age. As a result, although the law is intended to apply to those under 21, it also affects older adults, who must now carry identification to establish their age.

Unlike online platforms and websites, bars do not need sophisticated digital methods to verify someone's identity, reducing any associated privacy and surveillance risks. Furthermore, once customers are in, bars have little incentive to monitor their customers' activity. In contrast, online platforms and websites would not only need to introduce potentially intrusive methods of identity verification, but they would also have an incentive to monitor user activity continuously and, in some cases, remove content or censor speech to avoid liability. Therefore, compared to the analog world, the cybersecurity and surveillance risks associated with age verification for online platforms are much higher—and they could easily affect *all* users, not just those under the statutory minimum age.

III. KOSA Defines “Harm” Too Broadly and Fails to Create Meaningful Checks for the Federal Trade Commission

Another problematic aspect of KOSA is that it defines “harm” too broadly and gives the Federal Trade Commission and state attorneys general unchecked authority to decide how the law will be enforced. If harm were defined more narrowly (e.g., terrorism-related content or “grooming”), the increased surveillance and censoring activities would apply in a more limited set of circumstances. However, the overly broad definition of harm—which includes more commonplace issues like social anxiety—means that a significant part of online activity could be subject to surveillance. As a result, the surveillance risks associated with KOSA are much higher than they would have been if harms were more narrowly defined.

These risks are especially pronounced due to the absence of federal privacy legislation in the United States. As such, U.S. residents often do not enjoy consistent privacy protections across different sectors and state boundaries—unlike their counterparts in the European Union, the United Kingdom, and Canada. Against this backdrop, it is unsurprising that civil liberties groups, such as the Electronic Frontier Foundation ([EFF](#)) and American Civil Liberties Union ([ACLU](#)), have warned about the surveillance and censorship risks KOSA presents.

Likewise, KOSA would grant the FTC and state attorneys general significant authority in interpreting and enforcing the law without creating meaningful checks on their powers. Against the backdrop of an increasingly polarized political environment and politicized institutions, this raises the risk that KOSA could be used to sue websites and remove content that the government du jour deems “harmful” to minors—including social, political, or historical content from the other end of the political spectrum. In other words, it is possible that a less scrupulous future administration could use the legislation in an attempt to restrict information for teens on important but politically partisan topics such as abortion, climate change, and gun rights in certain contexts.¹ To prevent this problem, online harm legislation must include a more precisely defined, narrower set of harms and mechanisms to ensure regulatory neutrality and accountability.

IV. COPPA 2.0 Risks Significantly Restricting Access to Online Spaces and Services for American Teens

Some of the broader concerns with KOSA also apply to COPPA 2.0. For example, like KOSA, COPPA 2.0 would grant the FTC significant enforcement authority without establishing meaningful checks to ensure the Commission’s political neutrality and accountability. Unlike earlier KOSA drafts, COPPA 2.0 does not [propose](#) possible age-verification methods, nor does it propose a study to compare technologically feasible options to do so. However, the legislation proposes that the basis for establishing liability for online platforms be [changed](#) from the “actual” knowledge standard to the “fairly implied” knowledge standard. While it is unclear whether that will necessitate companies to establish age verification processes formally, it would require them to collect more personal data—increasing compliance costs for companies and potential privacy risks for users.

Finally, COPPA 2.0’s proposed [changes](#) could significantly curtail U.S. teens’ access to online spaces and services. The current [COPPA](#), passed in 1998, applies to individuals under 13. However, the obligations under the revised COPPA 2.0 would apply to users aged 13 to 16 in addition to those under 13. Several organizations, such as the Information Technology and Innovation Foundation ([ITIE](#)), point out that, in response to current COPPA rules,

¹ Note, however, that under §2(3)(B), KOSA’s proposed obligations and liability do not apply to educational institutions, non-profit organizations, and news organizations for certain types of content—limiting the FTC’s to take down content by those organizations that are deemed harmful.

many online platforms and websites currently do not allow users under 13. If these obligations also apply to users aged 13 to 16 under [COPPA 2.0](#), many platforms and websites might simply respond by [banning](#) American users under 17 from their platforms altogether. Likewise, certain companies might refuse to [provide](#) services to those users. Ultimately, for many companies, COPPA 2.0-related compliance costs could easily [outweigh](#) any additional revenue gained from serving a relatively limited demographic group.

Such a development could easily restrict American teens' access to many online platforms and services, while their European and Asian counterparts could enjoy such content without an issue. Furthermore, given that teens in lower-income households with parents who do not have university degrees might rely more heavily on online platforms for educational and extracurricular opportunities, restricted access to those sources might disproportionately affect teens from less affluent households without university-educated parents.

V. Conclusion

While the government must develop policies to improve youth online safety and address the broader social and mental health challenges the bills' sponsors correctly identify, KOSA and COPPA 2.0 are not the answer. Members of the U.S. Senate must recognize the unintended consequences that the two proposed laws would introduce for individuals of all ages. For the reasons outlined in this letter, our organization stands in opposition to KOSA and COPPA 2.0, and we urge you to oppose the bills in their current form.

The National Taxpayers Union appreciates the Senate's consideration of our views on this important issue, and we stand ready to work with you as you consider the best ways to improve online safety and privacy.

Sincerely,

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