

February 4, 2025

Chairman Ted Cruz
554 Dirksen Senate Office Building
Washington, DC 20510

Ranking Member Maria Cantwell
254 Russell Senate Office Building
Washington, DC 20510

Re: Concerns with S. 278's Threats to Minors' Privacy and Safety Online

Dear Chairman Cruz, Ranking Member Cantwell, and Members of the Committee,

We, the undersigned civil rights, digital rights, and civil liberties organizations, write to express our significant concerns with the [Kids Off Social Media Act \(S. 278\)](#) (KOSMA), introduced by Senators Schatz and Cruz. While protecting children online is imperative, this bill—if enacted—would actively undermine child safety, harm marginalized youth, erode privacy, and impose unconstitutional restrictions on young people's ability to engage online.

1. The bill has a significant, potentially unconstitutional, restriction on young people's access to online services

All U.S. residents, including minors, have First Amendment rights to access information and express themselves. The Supreme Court has long recognized that young people are “entitled to a significant measure of First Amendment protection [...] and only in relatively narrow and well-defined circumstances may the government bar public dissemination of protected materials to them.”¹ Today, the internet is our nation's primary marketplace of ideas, and social media platforms serve as essential spaces for young people to communicate, learn, and participate in civic life. Banning kids from creating an account, including ones with appropriate safeguards, would cut them off from online expression, political engagement, news and even essential educational resources on platforms like YouTube, Pinterest, and GroupMe. At a time when books are being banned in schools and curricula are being restricted, ensuring young people can access a broad range of perspectives online – and be able to [engage](#) with a broad community– is more critical than ever. KOSMA, however, would completely shut kids under 13 off from this world, in violation of the First Amendment.

This legislation would also bar schools from receiving E-Rate funding if they do not enforce “a policy of preventing students of the school from accessing social media platforms on any supported service, device, or network.” Not only would this prevent students of all ages from accessing social media during after-school activities or when relying on parking lot wi-fi, but this prohibition will also extend into students' homes. Today, [schools](#) often provide students with computers, [hotspots](#), and other networking equipment. However, these devices are [disproportionately](#) used outside of school by low-income households, who [struggle to afford](#) a

¹ ERZNOZNIK v. CITY OF JACKSONVILLE 422 U.S. 205 (1975)

device or broadband connection on their own. In fact, for many low-income households, a child's school-provided device is the only device in the home and is consequently shared by the entire household. Because the social media ban applies to any supported devices and networks from E-Rate schools, regardless of where the device is physically located, all members of families using school-provided devices would be blocked from accessing social media—even at home. Because higher income households are more likely to have their own devices, this legislation would create a world that enables wealthier households to access social media, while lower income households cannot.

2. KOSMA would threaten speech and privacy due to age verification

Although KOSMA states that it will not require platforms to conduct age verification, implement age gating, or collect additional data to determine a user's age, platforms are nevertheless [likely to](#) take significant steps to assess users' ages because they are liable if they have "knowledge fairly implied on the basis of objective circumstances that a user is a child or teen... including whether a reasonable and prudent person under the circumstances would have known that the user is a child or teen." Because this standard falls short of *actually knowing* that a user is a teen, most platforms would seek to avoid potentially massive liability by verifying the ages of its users. As many of our groups have noted previously, age verification creates new privacy risks, and could prevent adult users from accessing First Amendment protected content if they don't have identification or are unable to verify their age due to technological malfunction.

3. The bill will incentivize invasive surveillance of children

KOSMA would expand the Children's Internet Protection Act ([CIPA](#)) in ways that would accelerate the adoption of invasive and unproven student monitoring technologies. Although CIPA's monitoring requirement never [intended](#) for children and families to be surveilled, [research](#) has shown that schools have interpreted CIPA's past requirements to require AI-driven, persistent monitoring of students, despite the bill being enacted long before this technology even existed. This misinterpretation has given tech companies the opportunity to sell [dangerous](#) and [discriminatory](#) online activity monitoring technologies to be used against kids in schools, logging families' online browsing, search history, chats, and keystrokes.

KOSMA would expand CIPA's scope from pornographic and related content to the entirety of social media. The language in the Eyes on the Board section of the bill may reinforce the misperception that schools' access to E-Rate funding is tied to the installation and use of AI-powered spyware to surveil what students are doing online during and outside of school hours—scanning messages and documents, tracking websites visited, and even enabling real-time access to devices. A "rule of construction" included in recent versions of the bill does not do enough to dispel this misconception: that provision states that schools do not have "to track an individual website, online application, or mobile application that a student is attempting to access," but it does not disavow monitoring of students' activity on those applications. This only furthers misconceptions of CIPA's requirements. Moreover, blocking social media inherently requires monitoring traffic – a fact that the "rule of construction" concedes.

Under the threat of lost E-Rate funding, schools may also turn to these tech companies for content filtering technologies known to be overly restrictive of students' ability to access critical information, even for things like schoolwork. Recent polling by the Center for Democracy and Technology [shows](#) that strict content filters block students from accessing critical educational resources, with almost three-quarters of students and teachers reporting it interferes with schoolwork.

Further, this provision of the bill would disproportionately [impact students](#) who have been historically marginalized, including those [relying on](#) school-provided internet and devices to access online services. Because schools often misinterpret laws as requiring invasive surveillance, they may monitor student activity. This monitoring [chills](#) expression and results in discipline, law enforcement involvement, and outings of LGBTQ+ students. Polling [shows](#) that almost one in four teachers whose school uses this technology report that their school automatically shares this information with law enforcement outside of school hours and reported that a student was contacted by law enforcement as a result of this technology. Additionally, 18% of LGBTQ+ students say it has led to them or someone they know being outed as a result.

4. The bill may undermine existing child safety efforts

KOSMA prohibits social media services from using automated recommendation systems for users under 17 years of age under the flawed assumption that all algorithmic recommendations are harmful. The updated language of the bill provides limited exceptions, including the use of a minor's age, likely intended by the bill's sponsors to allow platforms to offer age-appropriate experiences. But, in reality, recommendation systems are crucial for *reducing* children's exposure to harmful content by better enabling youth to control their online experience. Worse, by making mainstream platforms less functional for minors, KOSMA may drive teens toward *riskier, unmoderated platforms* that do not enforce safety measures at all. When kids feel social media is unusable, they don't stop using the internet—they just find alternative spaces where harmful content, predatory behavior, and extremism are even harder to detect and prevent.

Protecting young people online is an important and urgent goal for all, but KOSMA takes the wrong approach. Instead of banning accounts, forcing surveillance, and removing key safety features, policymakers should focus on protecting all users' privacy, enforcing existing laws against child exploitation, and ensuring young people can safely navigate digital spaces. It is crucial to ensure that young people are prepared to navigate a digital world in responsible and healthy ways as they become adults. Tracking their every move online, cutting off their ability to learn and communicate, and forcing them into riskier online spaces will not make them safer and may impede the critical development that ensures their safety in the long run. Notwithstanding its intentions, KOSMA does not protect kids—it puts them at greater risk.

February 4, 2025

We stand ready to work with the sponsors of the Kids Off Social Media Act as well as all other members of Congress to enact policies that ultimately empower minors online and protect privacy for everyone. Please feel free to reach out to Jenna Leventoff (jleventoff@aclu.org) or Sydney Saubestre (saubestre@newamerica.org) with more questions.

Sincerely,

American Civil Liberties Union
Center for Democracy & Technology
Electronic Frontier Foundation
Fight for the Future
Free Press Action
Freedom of the Press Foundation
New America's Open Technology Institute
Public Knowledge
Restore The Fourth
Surveillance Technology Oversight Project
TechFreedom
Woodhull Freedom Foundation