



1420 New York Avenue NW, Suite 825
Washington, D.C. 20005
www.technet.org | @TechNetUpdate

July 26, 2023

The Honorable Maria Cantwell
Chair
Senate Committee on Commerce,
Science, and Transportation
511 Hart Senate Office Building
Washington, D.C. 20510

The Honorable Ted Cruz
Ranking Member
Senate Committee on Commerce,
Science, and Transportation
167 Russell Senate Office Building
Washington, D.C. 20510

Dear Chair Cantwell and Ranking Member Cruz:

Ahead of the Senate Commerce Committee's consideration of child safety legislation, I write on behalf of TechNet to urge the Committee to further refine these proposals to prevent restrictions on children and teens' access to educational and beneficial information online and mitigate the incentives towards overcollection of children and teens' personal data.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. Our [membership](#) includes dynamic American businesses ranging from startups to the most iconic companies on the planet and represents over 4.5 million employees and countless customers in the fields of information technology, e-commerce, the sharing and gig economies, advanced energy, cybersecurity, venture capital, and finance.

Protecting the mental health and security of children online is a top priority for the technology industry. The technology industry continues to innovate and launch new tools, features, and policies that are tailored to the developmental needs of young people, moderate and remove harmful and illegal content, limit unwanted interactions, set time limits, and protect child users, all while providing a safe, informative, and entertaining experience online. These settings and tools empower parents to manage and supervise their children's digital well-being in a manner that is age-appropriate and tailored to their child's individual needs.

We applaud Congress's efforts to examine ways to make the internet ecosystem healthier and safer for children. Last year, Congress enacted the *CAMRA Act*, which directs the National Institute of Health and the Department of Health and Human Services to lead a research program on technology and media's effects on infants, children, and adolescents in cognitive, physical, and socio-emotional development. We urge Congress to continue its efforts to fund this important research so that policymakers are better equipped to not only understand potential harms, but also the

value provided by internet and technology companies to enable teenagers' ability to access positive communities online and connect with peers with shared identities, abilities, and interests. In addition, further research is needed to ensure that proposals to limit access to information and spaces for self-expression do not harm young people, especially those from marginalized communities.

As the Senate Commerce Committee considers legislation directed at improving child safety online, we urge the Committee to further refine these bills to best achieve this broadly shared goal.

Kids Online Safety Act (KOSA)

As drafted, *KOSA* seeks to impose liability on covered platforms for failure to prevent a variety of harms to minors based on the speech and actions of third parties. However, in crafting this duty of care, *KOSA* creates a de facto age-verification requirement and runs counter to longstanding Supreme Court jurisprudence on the First Amendment which requires government regulations on speech to meet the strict scrutiny test. Ultimately, *KOSA*'s de facto age-verification requirement, while intended to protect children and teens from harmful content, will infringe on access to information for all users to the detriment of a healthy Internet ecosystem.

In *Reno v. ACLU* (1997), the Court held that the Internet is entitled to the full protection given to other forms of media and that portions of the *Communications Decency Act of 1996* that sought to criminalize certain types of Internet speech was unconstitutional because it was not narrowly tailored to serve a compelling governmental interest and because less restrictive alternatives were available. In *Ashcroft v. ACLU* (2004), the Court held that the *Child Online Protection Act (COPA)*, enacted in response to *Reno*, was also unconstitutional because the Government failed to demonstrate that existing technologies were less effective than the restrictions in *COPA*. In *Brown v. Entertainment Merchants Association* (2011), the Court struck down California's ban on the sale of violent video games to children without parental supervision because the law, however well-intentioned, violated the First Amendment since video games were protected speech.

Section 3(a) of *KOSA* would lead to children and teenagers being restricted from accessing protected speech. By failing to define with specificity the types of prohibited content or practices, covered platforms are faced with serious questions regarding ways to avoid liability under Section 11 of *KOSA*. Further compounding this uncertainty, Section 11 of *KOSA* provides for enforcement by both the Federal Trade Commission and State Attorneys General. Without clear definitions and guidance in Section 3, Attorneys General will no doubt enforce *KOSA* inconsistently, based on individual interpretations of which content is protected and could lead to mental health disorders or patterns of use that indicate addiction-like behaviors.

We are also concerned about *KOSA*'s restrictions on personalized recommendation systems. Personalization is essential for organizing the vast amount of information on

the Internet and the function of many online products and services. For children and teens, personalized recommendations can help connect younger users to high-quality, developmentally appropriate content that is best suited to their individual needs and interests.

While Section 4(a)(1)(D) says covered platforms must provide minors with safeguards to “opt out of such personalized recommendation systems,” the requirement in Section 4(a)(3) that the default setting for any safeguard be the “most protective level of control that is offered by the platform” suggests personalized recommendation systems may have to be off by default. While we appreciate the new rule of construction clarifying that nothing shall be construed to prevent a covered platform from using a personalized recommendation system to display content to a minor under certain circumstances, a covered platform still may not be able to deliver recommendations based on a user’s search query, device type, or time of day as these could all be considered personal information.

In addition, the requirement in Section 4(a)(1)(D)(i) that covered platforms still allow the display of content based on a chronological format for users that opt out will only help bad actors eager to take advantage of chronological ordering to reach more consumers with spam and other low-quality or harmful content. We urge the Committee to strike this language.

We appreciate the goals of the transparency requirements in Section 6. However, we are concerned that it does not strike the right balance between transparency, security, and user privacy. As currently drafted, *KOSA* would require covered platforms to provide third-party auditors with extremely detailed information. Until the government, academia, and the private sector can assure the public that allowing third party access to proprietary information and users’ personal information does not pose any additional risks from cyber threats and rogue actors, we recommend Congress first study how information will be adequately protected under such an auditing system. As an alternative, we believe such auditors can be internal to an organization so long as there are sufficient guardrails in place to ensure independence.

With respect to disclosure requirements in Section 5(c) regarding advertising and marketing information, such a requirement inappropriately places the burden on covered platforms to disclose an advertisement or marketing material despite the fact that the Federal Trade Commission has long held that advertisers and creators are responsible for disclosing this information.

Finally, we urge the Committee to add language to address the growing patchwork of state laws relating to kids’ online safety and establish one clear, national standard that provides clarity for kids and families across the country, as well as provides businesses with certainty about their responsibilities.

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

COPPA 2.0 seeks to expand the applicability of the *Children's Online Privacy Protection Act of 1998* to all minors under the age of 17, from the current threshold of 13. We appreciate the number of improvements included in the substitute amendment to address stakeholder concerns.

While we are supportive of efforts to prohibit personalized advertising (or "individual-specific advertising") to children and teens, we urge the Committee to ensure that the definition of individual-specific advertising does not sweep in contextual advertising that is essential to ensuring the availability of free, high-quality, educational content for children and teens, regardless of ability to pay. We appreciate the added clarity regarding contextual advertising in the substitute amendment, but urge the Committee to further clarify that a user's general geographic location, search query, device type, language settings, and time of day does not constitute "personal information."

We also urge the Committee to amend "information linked or reasonably linkable to a child or teen" to "information directly attributed to a child or teen" in the definition of "personal information," as this could otherwise sweep in aggregated or pseudonymous information, or other pieces of personal information not directly related to the child or teen held in a secondary user's account.

Conclusion

While each of these bills are well-intentioned in seeking to protect children online, we urge the Committee to refine these bills to strike the appropriate balance between protecting children from specified types of harmful content while ensuring that the prohibitions do not unduly burden lawful speech protected by the First Amendment or infringe on access to information for all users.

In addition, we applaud the Committee for its recognition of the need for enhanced privacy protections for Americans. Our members support consumers' right to access, correct, and delete their data, as well as the creation of comprehensive federal privacy legislation that creates a uniform national standard, preempts state law, and ends the growing privacy patchwork that is confusing consumers, hurting small businesses, and threatening America's leadership in innovation.

We appreciate your consideration of our perspective on this important issue and look forward to serving as a resource as the Committee continues its efforts to protect children and teens' privacy online.

Sincerely,



Carl Holshouser
Senior Vice President