

The House Passes the KIDS Act

August 3, 2026

On June 29, 2026, the U.S. House of Representatives passed the Kids Internet and Digital Safety (KIDS) Act ([H.R. 7757](#)). The KIDS Act consolidates a variety of legislative proposals aimed at protecting children and teens online. These proposals include the Kids Online Safety Act (KOSA), which would require online platforms to adopt default safeguards for minors, and the Children and Teens’ Online Privacy Protection Act (referred to as “COPPA 2.0”), which would expand federal privacy protections for minors.

This Legal Sidebar provides a summary of the KIDS Act. The Sidebar describes the various legislative proposals that make up the bill and considers certain legal questions related to the bill, such as the bill’s knowledge standards, enforcement mechanisms, and interaction with state law. The Sidebar also discusses potential First Amendment challenges to the bill. It closes with some considerations for Congress. A [different CRS product](#) discusses specifically the KOSA provisions of the KIDS Act from the policy perspective.

Summary of the Bill

The KIDS Act combines various kids-safety-related bills introduced in the 119th Congress. These bills are described below and are listed in the order in which they appear in the KIDS Act. The descriptions are based on the versions of the bills incorporated into the KIDS Act, rather than the versions introduced separately.

- The [Shielding Children’s Retinas from Egregious Exposure on the Net \(SCREEN\) Act](#) would [require](#) certain online platforms to use age-verification technology that meets certain requirements to identify minors and prevent them from accessing “[sexual material harmful to minors](#).” Platforms would [be required](#) to comply with this age-verification requirement if (1) they are accessible to the public, (2) more than one-third of the material on the website or platform is sexual material harmful to minors, and (3) they make such material available “knowingly.” Platforms would also be required to comply with certain data [privacy](#) and [security](#) requirements for the age-verification information that they collect.
- The [Kids Online Safety Act \(KOSA\)](#) would require certain online platforms to implement measures designed to promote the safety of [minors](#). KOSA would apply to

Congressional Research Service

<https://crsreports.congress.gov>

LSB11465

publicly available online platforms meeting certain criteria, including having the primary purpose of facilitating the sharing of and access to user-generated content. Among other provisions, KOSA would require platforms to establish and enforce reasonable policies, practices, and procedures to address certain harms, such as threats of physical violence and sexual exploitation. KOSA would further require platforms to implement three types of measures when they “know or should have known” that a user or a visitor is a minor: (1) safeguards, (2) parental tools, and (3) messaging controls for teens. First, platforms must offer minors easy-to-use controls, such as the ability to limit others from communicating with them, limit compulsive design features, and control any personalized recommendation system. Second, platforms must offer minors’ parents tools that, among other things, allow them to view the minor’s privacy and account settings, restrict their purchases, control account settings, turn off messaging for children (minors under the age of 13), and be notified when the minor receives a first-time messaging request from another user. Finally, platforms must allow teens (minors who have “attained the age” of 13 but are younger than 17) to control the messages they receive on the platform, such as by allowing them to disable direct messages, receive an alert before receiving a message from an unapproved contact, and prevent specific users or groups of users from messaging them.

- The **Stop Profiling Youth and Kids (SPY Kids) Act** applies to the same platforms subject to KOSA. It prohibits them from conducting market or product-focused research on users or visitors that a platform knows are minors, subject to limited exceptions.
- The **Safer Guarding of Adolescents from Malicious Interactions on Network Games (Safer GAMING) Act** would apply to providers of video games that connect to the internet and allow users to communicate with each other. When such providers “know or should have known” that a user is a minor, they would be required to give parents tools to limit the minor’s communication with others. Providers would also be required to offer other safety settings, such as those that limit the minor’s financial transactions or limit the time they spend on the platform.
- The **Safeguarding Adolescents from Exploitative (SAFE) BOTs Act** would require providers of chatbots to disclose to users that they “know or should have known” are minors that the chatbots are an AI system and not a natural person, and in response to prompts about suicide, to offer resources for contacting a suicide and crisis intervention hotline. Chatbot providers would also have to establish “reasonable policies” related to minors, including addressing sexual exploitation and abuse, the promotion of gambling, and the promotion and distribution of drugs, tobacco, and alcohol. A different provision of the KIDS Act would further require the Secretary of Health and Human Services (HHS), in consultation with the Director of the National Institutes of Health, to conduct a “4-year longitudinal study” to evaluate the impact of chatbots on minors’ mental health and, within four years, submit a report to Congress.
- The **Safe Social Media Act** would require the Federal Trade Commission (FTC), in coordination with HHS, to study minors’ social media use and, within three years, submit a report to Congress.
- The **No Fentanyl on Social Media Act** would require the FTC, in coordination with HHS, to study minors’ access to fentanyl through social media platforms and, within one year, submit a report to Congress.
- The **Assessing Safety Tools for Parents and Minors Act** would require the FTC, in consultation with various stakeholders, to review the effectiveness of industry efforts to promote online safety for minors and, within three years, submit a report to Congress.

- The **Promoting a Safe Internet for Minors Act** would amend the **Protecting Children in the 21st Century Act** to, among other things, require the FTC to conduct a public awareness and educational campaign to promote the safe use of the internet by minors.
- The **AI Warnings and Resources for Education (AWARE) Act** would require the FTC to make publicly available educational resources on the safe and responsible use of chatbots by minors.
- The **Kids Internet Safety Partnership Act** would direct the Secretary of Commerce to establish a Kids Internet Safety Partnership that, in coordination with other agencies and stakeholders, would identify risks and benefits of minors operating online and would publish a “**playbook**” of best practices for mitigating the risks and enhancing the benefits. The playbook would **include** best practices with respect to age verification and parental tools, for instance.
- The **Children and Teens’ Online Privacy Protection Act (COPPA 2.0)** would amend the **Children’s Online Privacy Protection Act of 1998 (COPPA)**. COPPA, as it currently stands, provides privacy protections to children **under the age of 13**. COPPA’s requirements **apply** to online operators that direct their websites or online services to children or that have “actual knowledge” they are collecting children’s information. Under COPPA and the FTC’s **implementing regulations**, covered operators must, among other things, **obtain verifiable parental consent before collecting, using, or disclosing children’s personal information; provide parents with notice of the operator’s privacy policies; maintain reasonable data security procedures; and comply with data retention and deletion requirements**. COPPA 2.0 would update this regime by extending COPPA’s protections to teens **under the age of 18** and revising COPPA’s “actual knowledge” standard to **include** situations where a platform “should have known that a user is a child or teen.” COPPA 2.0 would also **ban** the collection, use, or disclosure of a child or teen’s data for “individual-specific advertising” to the child or teen; **prohibit** online operators from storing or transferring a child or teen’s data outside of the United States without providing direct notice; and **impose** data minimization requirements on online operators. COPPA 2.0 would also address how the parental consent requirement applies in the educational context by **allowing** online operators to access a child or teen’s information without consent if they are operating under an agreement with an educational institution. The Senate **passed** a similar, but not identical, **version** of COPPA 2.0 in March 2026.
- While it does not have its own short title, the KIDS Act includes a section governing “**Data Broker Disclosures**.” Data brokers who **knowingly** disclose for consideration (i.e., for money or something else of value) the personal data of minors would be **required** to register with the FTC and file information about their businesses. The FTC would **establish** a publicly available and searchable registry containing this information.

Knowledge Standard: “Should Have Known” Versus “Willful Disregard”

Many of the KIDS Act’s requirements apply only if the regulated platform knows that an individual is a minor. Different portions of the KIDS Act use different definitions of *knowledge*. **KOSA**, the **Safer GAMING Act**, the **SAFE BOTS Act**, and **COPPA 2.0** define knowledge to include situations where the regulated entity had actual knowledge or where it “should have known” the person was a minor. A court would likely interpret this “should have known” language as a **constructive knowledge** standard. A person has constructive knowledge when he or she “**fail[ed] to learn something that a reasonably diligent person would have learned**.” In contrast, the **SPY Kids Act** and the **data broker disclosure requirements** define

knowledge as “actual knowledge or willful disregard.” Under this “willful disregard” standard, it would not be enough to show that a reasonably diligent person would have learned that the user is a minor; rather, a court would [likely require evidence](#) that (1) the regulated entity subjectively believed that there was a high probability the person was a minor and (2) took deliberate actions to avoid learning of that fact. Thus, it would likely be more challenging to establish knowledge under the SPY Kids Act and data broker disclosure requirements than under the portions of the KIDS Act using a “should have known” standard.

Enforcement

The KIDS Act would be [enforced](#) by the FTC. Violations of the above requirements [would be treated](#) as violations of [rules defining unfair or deceptive acts or practices under the Federal Trade Commission Act](#), giving the FTC grounds to ask a court for [civil penalties, injunctions](#), and [other equitable relief](#) for violations. The KIDS Act would also [authorize](#) state attorneys general to bring civil actions on behalf of their states’ residents, [provided](#) they first notify the FTC and give the FTC an opportunity to intervene in the suit. In these actions, state attorneys general [could ask a federal court](#) to issue an injunction, award damages or restitution on behalf of their residents, or award other such relief the court may consider appropriate.

Interaction with State Law

The KIDS Act would set a “[federal floor](#)” on which states can build. The KIDS Act would preempt state laws only to the extent they “[conflict](#)” with the KIDS Act. Cases interpreting this kind of “[conflict preemption](#)” suggest a state law is preempted when compliance with both the federal and state law is a “physical impossibility” or when the state law “stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress.” For example, a state law prohibiting gaming platforms from limiting financial transactions for any user would likely be preempted, but a state law giving parents rights to impose further controls on minors’ activities on covered platforms, above and beyond what federal law requires, may be enforceable. The KIDS Act would also [expressly preserve](#) state contract, tort, and product liability laws and state laws providing “[greater protection to minors](#).”

Potential First Amendment Challenges

Some [commenters](#) have [argued](#) that certain provisions in the KIDS Act would infringe the First Amendment rights of online platforms and services or their users. The Supreme Court has recognized that both [platforms](#) and [users](#) have relevant First Amendment rights. The Court has, for example, said that “adults have a [constitutional right](#) to receive” and share certain speech on the internet. Minors also have [constitutional speech rights](#), and online platforms may engage in [protected expression](#) when they decide what content to display and how a content display “will be ordered and organized.”

These First Amendment rights, however, are [not absolute](#). When a law restricts protected speech, courts apply a [variety of tests](#) to determine whether the restriction violates the First Amendment. The appropriate test can depend on both the [type of speech](#) being restricted and the [way the regulation affects speech](#). Because different provisions in the KIDS Act regulate different types of speech in different ways, the constitutional test a court applies in any First Amendment challenge may depend on the specific provisions of the KIDS Act being challenged.

For example, the KIDS Act would [create](#) age-verification requirements. The SCREEN Act would [require](#) certain adult websites to use age-verification technology. KOSA provides that it [does not require](#) age verification, but some commenters have [argued](#) that platforms would need to adopt age-verification measures to ensure compliance with provisions that apply when a platform “[should have known](#)” a user is

a minor. Courts have held that age-verification requirements [can](#) prevent minors from accessing platforms to share and receive protected speech and can also burden adults' ability to use the platforms. The Supreme Court has, however, [upheld](#) a Texas law that—like the SCREEN Act—[requires](#) adult websites to verify users' ages if they publish a certain amount of “harmful” material, [defined](#) using the legal test for [obscenity](#) as applied to minors. In the case evaluating the Texas law, the Court applied a First Amendment test known as [intermediate scrutiny](#), which provides that a regulation does not violate the First Amendment if it “advances important governmental interests unrelated to the suppression of free speech and does not burden substantially more speech than necessary to further those interests.” Outside of the obscenity context, though, some courts have [held](#) that certain [restrictions](#) on minors' access to online platforms are subject to [strict scrutiny](#)—a constitutional standard that is more [difficult to satisfy](#)—and [violate](#) the First Amendment.

Other KIDS Act provisions prohibit certain [types](#) of [speech](#) or the [use](#) of certain information. These types of provisions can trigger [strict scrutiny](#) when they make content-based distinctions. They can, however, be subject to a version of [intermediate scrutiny](#)—making them more likely to be upheld—if they affect only [commercial speech](#).

Some provisions in the KIDS Act target [platform design](#) features. Again, such restrictions can be subject to strict scrutiny when they restrict speech with [particular content](#). They may also be subject to intermediate scrutiny if they are [content neutral](#). Some design regulations may not be subject to any level of heightened scrutiny: Courts have found that certain limitations on online platforms' design features [do not restrict](#) the platforms' or their users' speech. Laws that do not restrict [protected speech](#) or another [fundamental constitutional right](#) are often subject to rational basis review. Under that standard, a reviewing court [asks](#) whether there is a “reasonably conceivable state of facts that could provide a rational basis” for a law's enactment.

Finally, the KIDS Act includes [disclosure requirements](#). Disclosure requirements [compel specific content](#). They may therefore be subject [strict scrutiny](#) or, if they compel only commercial speech, [intermediate scrutiny](#). In addition, if the disclosure requirement compels “purely [factual and uncontroversial information](#)” about a commercial speaker's goods or services, a court may [apply](#) a more lenient [test](#) that asks if the challenged disclosure requirement is reasonably related to a sufficient government interest and neither unjustified nor unduly burdensome.

Considerations for Congress

The KIDS Act [passed](#) the House and now moves to the Senate. Some Senators have introduced their own versions of certain portions of the KIDS Act, including [KOSA](#) and the [SCREEN Act](#), and the Senate has [passed](#) a version of [COPPA 2.0](#). The bills introduced in or passed by the Senate [differ](#) from the versions incorporated into the KIDS Act in certain respects, and any consideration of the KIDS Act in the Senate may focus on areas where the proposals diverge. The Senate sponsors of KOSA, for example, issued a [statement](#) disagreeing with the “House's decision to strip out the Duty of Care” from KOSA. The version of KOSA introduced in the Senate would [require](#) covered platforms to “exercise reasonable care in the creation and implementation of any design feature to prevent and mitigate [certain] harms to minors.” The version of KOSA in the KIDS Act would [require](#) platforms to “establish, implement, maintain, and enforce reasonable policies, practices, and procedures that address” specified harms.

Other areas of the KIDS Act that may engender debate include [preemption](#) (i.e., whether to create [nationally uniform standards](#) or [permit states](#) to pass different or stronger laws) and the [knowledge standard](#) that would apply to provisions in [KOSA](#) and [COPPA 2.0](#). Because the KIDS Act combines several separately introduced bills, Members may also debate whether to consider the included bills as part of the KIDS Act, as stand-alone measures, or as part of a different [package of regulations](#).

Author Information

Peter J. Benson
Legislative Attorney

Chris D. Linebaugh
Legislative Attorney

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.