

H.R. 7757, THE KIDS INTERNET AND DIGITAL SAFETY (KIDS) ACT

SECTION-BY-SECTION

Section 1. Short Title; Table of Contents.

This section provides the short title, the “Kids Internet and Digital Safety Act” or the “KIDS Act,” and the table of contents for the Act.

Section 2. Definitions.

This section provides definitions for terms used throughout the Act.

TITLE I. SHIELDING MINORS FROM OBSCENITY

This title includes sections 101-106, incorporating the Shielding Children’s Retinas from Egregious Exposure on the Net [SCREEN] Act (*H.R. 1623, Rep. Miller-IL*).

Section 102. Definitions

This section defines key terms used throughout the title, including:

Covered Platform: Publicly accessible websites that contain more than one-third of content consisting of sexual material harmful to minors.

Sexual Material Harmful to Minors: Utilizes the U.S. Supreme Court’s Miller Test to determine what is obscene for minors.

Section 103. Technology Verification Measures

This section requires covered platforms, such as pornography websites, to adopt technological commercially available age verification measures to identify minors and prevent minors from accessing the obscene content on the covered platform. This section also prevents self-attestation from being used as a method to verify age, provide notice to users of a covered platform’s policies and procedures on age verification, and includes provisions to prevent anti-circumvention, and ensure data security and privacy protection. Finally, this section includes a rule of construction clarifying that this title cannot be construed to require a government-issued identification.

Section 104. Consultation Requirements

This section requires the Federal Trade Commission to consult with certain stakeholders regarding appropriate age verification standards and metrics, including data privacy and security experts, vendors of age verification technology, and child online safety advocates.

Section 105. GAO Report

This section requires that the Comptroller General of the United States submit a report to Congress three years after enactment on the implementation of this title and the impacts of this title with respect to compliance, data privacy and security, and other societal and economic effects.



TITLE II. ADDRESSING HARMS TO MINORS ON ONLINE PLATFORMS

Section 201. Definitions.

This section provides definitions for this Title, including:

Covered Platform: A website, software, application or electronic service that is publicly available to consumers, enables the creation of a searchable and accessible user name or identifier, whose primary purpose is to facilitate the sharing and access of user-generated content, uses design features to promote user engagement, and uses personal information to advertise, market, and make content recommendations.

Subtitle A. Kids Online Safety

This subtitle includes sections 211-221, incorporating the Kids Online Safety Act (KOSA) *(H.R. 6484, Rep. Bilirakis)* and Safe Messaging for Kids Act *(H.R. 6257, Rep. Dunn)*.

Section 212. Definitions.

This section provides definitions for this subtitle, including compulsive usage, direct messaging feature, ephemeral messaging feature, geolocation information, messaging controls, teen, and unapproved contact. It also defines the terms “know” and “knows” to include both actual knowledge or should have known standards.

Section 213. Addressing Harms to Minors.

This section requires covered platforms to establish, maintain, implement, and enforce policies, practices, and procedures to address certain harms to minors including severe and pervasive threats of physical violence, sexual exploitation and abuse, narcotic drugs, tobacco and cannabis products, gambling, alcohol, and financial harms.

Section 214. Safeguards for Minors, Parental Tools, and Teen Messaging Controls.

Subsection (a) provides several optional safeguards for minors that are turned on at the most protective level by default. These safeguards include the following:

- Limiting the ability of other users to communicate with a minor.
- Preventing a minor’s profile from being promoted to non-minors.
- Preventing users from viewing a minor’s online status.
- Limiting design features that encourage compulsive usage by minors.
- Restricting the sharing of a minor’s geolocation information.
- Allowing for an opt-out from personalized recommendation systems.
- Limiting the types of recommendations from a personalized recommendation system.
- Limiting time spent by a minor on the covered platform.

Subsection (b) provides parents of minors parental tools. Covered platforms must provide notice to minors and parents about these tools, and for a child these tools are set by default at the most protective level. These tools include:

- Viewing privacy and account settings, including teen messaging settings.
- Changing and controlling privacy and account settings for a child.
- Restricting purchases and financial transactions.
- Viewing metrics of total time spent and for restrictions on time spent on the platform.
- Receiving a notification when another user seeks to request to initiate direct or ephemeral messaging.
- Disabling direct and ephemeral messaging features for a child.



Subsection (c) provides messaging controls that can be used by teens. These controls include:

- Receiving notifications on new requests from other users to initiate direct and ephemeral messaging and allow for the teen to approve or deny the request.
- Viewing and manage direct and ephemeral messaging contact lists.
- Disabling direct and ephemeral messaging features.
- Preventing the continuation of ongoing direct and ephemeral messaging.
- Enabling a teen to hide their profile.

This section also ensures that the safeguards, tools, and controls provided in this section can effectively be used by a user or a parent, such as being readily accessible and easy to use and not impaired or obscured by the covered platform. Further, this section also includes rules of construction ensuring covered platforms can still take measures to block, detect, or prevent unlawful, obscene, or harmful material to minors and allow third parties to continue to provide software safety tools.

Section 215. Reporting Mechanism.

This section requires covered platforms to allow users and visitors of a platform to submit a report on any harm to a minor on the platform. A covered platform is required to provide a point of contact, confirm the receipt of the report, and substantively respond to the report in a timely manner.

Section 216. Disclosure.

This section requires a covered platform to disclose information on safeguards, parental tools, and teen messaging controls to users prior to registration or purchase. The covered platform is also required to obtain verifiable parental consent with respect to parental tools and safeguards required by this Subtitle.

Section 217. Advertising and Marketing Information and Labels.

This section requires a covered platform to provide clear, conspicuous, and easy to understand labels and information to a user that is a minor of the covered platform on advertisements regarding the disclosure of endorsements of products or services.

Section 218. Advertising of Illegal Products to Minors.

This section prohibits a covered platform from facilitating the advertising of narcotic drugs, cannabis products, tobacco products, gambling, or alcohol to a known minor.

Section 219. Audit; Report.

This section states that not later than 18 months after the date of enactment of this subtitle, and annually thereafter, a covered platform shall ensure that an independent third-party auditor conducts an independent, third-party audit of the covered platform. The section also requires the content that should be included in the audit, and it also requires the audit to be submitted to the FTC and to be made public.

Section 220. Rule of construction on age verification.

This section states that nothing in this subtitle may be construed to require the provider of a covered platform to implement an age gating or age verification functionality on the covered platform.

Section 221. Rule of construction on encryption.

This section clarifies that nothing in this subtitle requiring a covered platform to restrict a feature for a user or to provide messaging controls for a direct messaging feature or ephemeral messaging feature may be construed to override encryption protections.



Subtitle B. Stop Profiling Youth and Kids.

This subtitle includes sections 231-234, incorporating the Stop Profiling Youth and Kids Act (SPY KIDS Act) (H.R.6273, Rep. Miller-Meeks).

Section 232. Know; Knows Defined.

This section defines know or knows as having actual knowledge or having acted in willful disregard.

Section 233. Market Research.

This section prohibits covered platforms from knowingly conducting product-focused or market research on individuals under 17 unless such research is used to improve the privacy, security, safety, and transparency of the covered platform. This section also includes a rule of construction stating that nothing in this subtitle may be construed to limit the processing of personal information solely for measuring or reporting advertising or content performance, reach, or frequency, including through an independent measurement.

Section 234. Effective Date.

This section provides that the effective date is 90 days after the date of enactment.

TITLE III. SAFEGUARDING MINORS ON SOCIAL GAMING PLATFORMS

This title includes sections 301-304, incorporating the Safer Guarding of Adolescents from Malicious Interactions on Network Games (GAMING) Act (H.R. 6265, Rep. Kean).

Sec. 302. Definitions.

This section defines key terms used throughout the title, including:

Covered Communication Tool: A capability available to a user of an interactive online video game that allows for the exchange of verbal, written, or visual messages between such user and any other user of such interactive online video game.

Interactive Online Video Game: A video game that connects to the internet and allows a user of such video game to communicate with other users of such video game.

Online Video Game Provider: A person engaged in the business of providing directly to a consumer over the internet or other online means a digital storefront, console network, mobile or cloud gaming platform, or similar means of digital distribution that offers access to an interactive online video game for use by the consumer.

Sec. 303. Safeguards Requirements for Online Video Game Providers.

This section requires a provider of an interactive online video game to provide parents with certain safeguards which must be accessible and easy to use, enabled by default to the most protective level, and provide notice to users about whether these safeguards are in effect. The safeguards include the following:

- Prevent the recommendation of a minor's profile to other users;
- Allow the parent to restrict financial transactions by the minor; and
- Allow the parent to limit the amount of time spent by the minor playing an online video game.



TITLE IV. ARTIFICIAL INTELLIGENCE CHATBOTS

This title includes sections 401-407, incorporating the Safeguarding Adolescents From Exploitative (SAFE) Bots Act (*H.R. 6489, Rep. Houchin*).

Sec. 402. Definitions.

This section defines key terms used throughout the title, including:

Chatbot Provider: A person engaged in the business of providing a chatbot directly to a consumer for the use of the consumer, including through a website, mobile application, or other online means. It excludes chat functions incidental to the primary purpose of the website, application, or service.

Know; Knows: Defines know or knows as having actual knowledge or should have known.

Sec. 403. Certain Statements Prohibited.

This section prohibits chatbots from stating that the chatbot is a licensed professional.

Sec. 404. Disclosure required.

This section requires chatbot providers to disclose, in age-appropriate language, that the chatbot is an AI system at certain points of use and provide suicide and crisis intervention hotline information if the user prompts the chatbot about suicide or suicidal ideation.

Sec. 405. Policies required.

The section directs chatbot platforms to establish and implement policies, practices, and procedures that include:

- Advising the covered user to take a break after 3 hours of continuous, uninterrupted use.
- Addressing sexual exploitation and abuse, the promotion of gambling, narcotic drugs, tobacco products, or alcohol.

Sec. 406. Rule of construction.

This section clarifies that nothing in this title may be construed to require a chatbot provider to prevent or preclude any covered user from accessing resources and information regarding the prevention or mitigation of the harms described in section 405.

TITLE V. RESEARCH, EDUCATION, AND BEST PRACTICES FOR PROTECTING CHILDREN ONLINE

Subtitle A. Research

Section 501. Definitions.

This section defines key terms used throughout the title, including:

Social Media Platform: A public-facing website, internet application, or mobile internet application, including a social network for video sharing service that serves the public and primarily provides a forum for user-generated content, including messages, videos, images, games, and audio files.

Sec. 502. Paperwork Reduction Act Exemption.

This section exempts this subtitle from the requirements contained in Paperwork Reduction Act.

Part 1. Safe Social Media Act

This part includes sections 511-512, incorporating the Safe Social Media Act (*H.R. 6290, Reps. Bentz and Schrier*), which directs the FTC and the Department of Health and Human Services to study and report on the collection and use of minors' personal information, minors' use of social media including differences by age, and mental health effects of social platforms on minors, both positive and negative.



Part 2. No Fentanyl on Social Media Act

This part includes sections 513-514, incorporating the No Fentanyl on Social Media Act (*H.R. 6259, Reps. Evans and Dingell*). Section 514 directs the FTC, in collaboration with relevant stakeholders and agencies, to produce a report on the ability for minors to access fentanyl on social media, the impact of that access, how drug sellers use social media, the impact of social media design features on access to fentanyl, the effectiveness of solutions by social media platforms to address fentanyl access, and recommendations to Congress to prevent minors from accessing fentanyl on social media.

Part 3. Assessing Safety Tools for Parents and Minors Act

This part includes sections 515-516, incorporating the Assessing Safety Tools for Parents Act (*H.R. 6499, Reps. Fulcher and Landsman*). Section 516 directs the FTC, in consultation with relevant stakeholders, to review industry efforts to promote online safety for minors through education, parental controls, age-appropriate content labels, privacy and safety settings and the effectiveness of such efforts. The FTC is required to submit a report to Congress on the review and include recommendations.

Part 4. Study on Chatbots and Mental Health of Minors

This part includes sections 517-519, which direct the Secretary of Health and Human Services, in consultation with relevant experts, to conduct a longitudinal study and subsequent report to Congress on the effects of chatbots on the mental health of minors, including on loneliness, anxiety, social skill building, social isolation, depression, self-harm, and suicidal ideation.

Subtitle B. Education.

Part 1. Promoting a Safe Internet for Minors Act

This part includes sections 521-522, incorporating the Promoting a Safe Internet for Minors Act (*H.R. 6289, Reps. Lee-FL and Soto*). Section 522 amends the Protecting Children in the 21st Century Act (15 U.S.C. 6551 et seq.) requiring the FTC, in consultation with relevant entities, to carry out a program which promotes best practices to protect minors online, establishes an outreach and education campaign to strengthen online safety for minors, and facilitates access to publicly accessible online safety education and public awareness efforts by government and non-governmental entities. This section also requires the FTC to submit an annual report to Congress.

Part 2. AI Warnings and Resources for Education (AWARE) Act

This part includes sections 523-524, incorporating the AI Warnings And Resources for Education (AWARE) Act (*H.R. 5360, Reps. Houchin and Auchincloss*). Section 524 directs the FTC, in consultation with relevant agencies, to develop and make publicly available educational resources, modeled on the FTC's "Youville" program for parents, educators, and minors, on the risks and benefits of chatbot use, privacy and data collection practices of AI chatbots, and best practices for parental supervision of minors' use of AI chatbots.

Subtitle C. Partnerships and Best Practices

This subtitle includes sections 525-526, incorporating The Kids Internet Safety Partnership Act (*H.R. 6437, Reps. Fry and Landsman*). Section 526 directs the Secretary of Commerce, in coordination with relevant agencies and stakeholders, to establish the Kids Internet Safety Partnership Act, whose duties include:

- Identifying risks and benefits for minors online and how to address such risks or preserve such benefits.
- Publishing a report on the risks and benefits of minors online, assessing efficacy of safeguards for minors and parental tools used by online services and mobile applications.
- Publishing a "playbook" of widely accepted or evidence-based best practices related to age verification, assurance, and estimation techniques, design features, parental tools, default privacy and account settings, third-party safety software services, and limitations and opt-outs related to personalized recommendation systems and chatbots.



TITLE VI. KIDS PRIVACY PROTECTIONS

This title establishes new protections for the personal data of children and teens.

Subtitle A. COPPA 2.0.

This subtitle includes sections 601-605, incorporating the Children and Teens' Online Privacy Protection Act (COPPA 2.0) *(H.R. 6291, Reps. Walberg and Lee)*.

Sec. 601. Short title.

This section may be cited as the “Children and Teens’ Online Privacy Protection Act.”

Sec. 602. Online collection, use, disclosure, and deletion of personal information of children and teens.

Sec. 602. Online collection, use, disclosure, and deletion of personal information of children and teens.

- Child. The term “child” means an individual under the age of 14.
- Operator. The term “operator” means any person who for commercial purposes operates a website, online service, online application, or mobile application, and collects the personal information from or about users, either directly or through a service provider. A nonprofit entity that would otherwise be exempt from section 5 of the Federal Trade Commission Act [15 U.S.C. 45] is not an operator.
- Personal Information. The term “personal information” means individually identifiable information about an individual collected online, including a first and last name, address, email address, telephone number, Social Security number, a persistent identifier, a photograph or video or audio file that contains the image or voice of a specific child or teen, geolocation information, biometric information, and information linked or reasonably linkable to a child or teen.
- Verifiable Consent. The term “verifiable consent” means any reasonable effort by an operator to ensure that: (1) a parent of a child (in the case of a child) or a teen (in the case of a teen) received direct notice about the operator’s collection, maintenance, and disclosure practices before the personal information is collected; and the (2) verifiable consent freely and unambiguously authorizes the collection, use, maintenance, and disclosure of such information.
- Teen. The term “teen” means an individual who has attained the age of 14 and is under the age of 18.
- Individual-Specific Advertising to Children or Teens. The term “individual-specific advertising to children or teens” means advertising or any other effort to market a product or service that is directed to a specific child or teen or a connected device that is linked or reasonably linkable to a child or teen based on the personal information of a child or teen, a group of children or teens, profiling of such child or teen or group of children or teens, or a unique identifier.
- Knowledge. The term “knowledge” means the operator has actual knowledge or should have known that a user is a child or teen.

Section 602(b) amends Section 1303 of the Children’s Online Protection Privacy Protection Act of 1998 [15 U.S.C. 6502]. This section establishes new and revised requirements for the online collection, use, disclosure and deletion of the personal information of children and teens. The following practices are unlawful with respect to the personal information of a child or teen:

- The collection, use, or disclosure to third parties, or maintenance of personal information of a child or teen for purposes of individual-specific advertising to children or teens.
- The collection of the personal information of a child or teen unless the collection is consistent with the context of a particular transaction or service or the relationship of the child or teen with the operator, including collection necessary to fulfill a transaction or a product or service requested by the child or teen.
- The storage or transfer of the personal information of a child or teen outside of the United States, unless the operator provides direct notice to a parent of the child (in the case of a child) or to the teen (in the case of a teen) of such storage or transfer.
- Retention of the personal information of a child or teen for longer than is reasonably necessary to fulfill a transaction or provide a service requested by the child or teen.



This subsection amends or expands the consumer privacy rights available for the parents of children, including the following rights:

- To receive a description of the types of personal information collected, the method of collection, and the purposes of for which it is collected, used, disclosed, and retained.
- To delete personal information or content submitted by the child and refuse further use or collection.
- To correct inaccurate personal information.

This subsection establishes consumer privacy rights available for teens, including the following rights:

- To receive a description of the types of personal information collected, the method of collection, and the purposes of for which it is collected, used, disclosed, and retained.
- To delete personal information or content submitted by the child and refuse further use or collection.
- To correct inaccurate personal information.

This subsection requires operators to establish, implement, and maintain reasonable security practices to protect the confidentiality, integrity, and accessibility of personal information collected, and to protect such information from unauthorized use.

This subsection recognizes operators acting under a written agreement with an education agency or institution, provided the agreement requires the operator to, among other requirements, limit data collection, use, and disclosure to educational purposes only, provide a link to its online privacy notice, and provide the educational agency, upon request, a means to review, prevent further collection of, and delete personal information from children or teens.

This subsection requires the FTC to assess, with notice and public comment, the feasibility of common verifiable consent mechanisms through which a single operator could obtain consent on behalf of multiple listed operators providing a joint or related service. The FTC must submit a report to Congress within one year. If the FTC finds the mechanism feasible, it must permit its use.

Section 602(c) amends Section 1304 of the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6503) to extend the existing regulatory safe harbor program to cover teens in addition to children. The Commission is directed to publish on its website any reports or documentation submitted under safe harbor regulations, subject to standard FTC confidentiality restrictions.

Section 602(d) amends Section 1305 of the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6504). This subsection amends the state enforcement provision to authorize state attorneys general to bring civil actions for violations of the statutory provisions directly, not only for violations of FTC regulations.

Sec. 603. Study and reports of mobile and online application oversight and enforcement.

Section 603 directs the FTC to submit to the House Energy and Commerce Committee and the Senate Committee on Commerce, Science, and Transportation a report on the processes of websites, online service, online application, or mobile applications directed to children to operate in accordance with this subtitle and any regulation of the FTC with regard to marketing. The report must be submitted not later than three years after enactment of the subtitle.

This section also directs the FTC to submit to the House Energy and Commerce Committee and the Senate Committee on Commerce, Science, and Transportation a report on the enforcement of the subtitle. The report shall include, among several items, the number of actions brought by the Commission under such action and the outcome of such actions; the total number of investigations or inquiries into potential violations of the subtitle; and policy or legislative recommendations to strengthen online protections for children and teens. The report must be submitted not later than one year after enactment of the subtitle.



Sec. 604. GAO study.

Section 604 directs the Comptroller General to conduct a study on the privacy and mental health of teens who use financial technology products. The report will identify the type of financial technology product that teens use and the potential risks to the privacy and mental health of teens that may result from the use of such products. It will also determine whether existing laws are sufficient to address any such risks. The report must be submitted to Congress no later than one year after the date of enactment of this subtitle.

Sec. 605. Severability.

Section 605 establishes severability regarding the bill.

Subtitle B. Data Broker Disclosures.

Sec. 611. Definitions.

Section 611 outlines the key terms used in the subtitle, including:

- **Covered Data Broker.** The term “covered data broker” means an entity that, for valuable consideration, sells, licenses, rents, trades, transfers, releases, discloses, provides access to, or otherwise makes available to another entity personal data of an individual the data broker knows is a minor that the entity did not collect directly from such individual to another entity that is not acting as a service provider.
- **Knows.** The term “knows” in this subsection means to have actual knowledge or willful disregard.
- **Personal Data.** The term “personal data” has the same meaning as the definition of “personal data” in section 602(a)(4) of this Act.
- **Minor.** The term “minor” means an individual under the age of 18 years old.
- **Service Provider.** The term “service provider” means an entity that collects, processes, or transfers personal data on behalf of and at the direction of the minor to whom such information pertain; a parent of such a minor; a federal, state or local government entity; and entity acting as a covered data broker or another service provider.

Sec. 612. Registration requirement.

This section establishes a registration requirement for covered data brokers. No later than 12 months after the date of the enactment of this subtitle, a covered data broker shall register with the FTC by paying a registration fee and filing a registration statement. The Commission may charge a covered data broker an annual registration fee of at least \$22,500, adjusted for inflation.

The registration statement required by this section includes: (1) the legal name of the covered data broker; (2) a contact person and the primary physical address, email address, telephone number, and website address for the covered data broker; (3) a description of each category of personal data sold by the covered data broker; (4) a statement of whether the covered data broker implements a purchaser credentialing process; and (5) a description of any incident of unauthorized access to personal data that has been reported to a federal or state governmental entity pursuant to an applicable law, rule, or regulation during the year before the year in which the registration is filed.

The FTC shall establish and maintain on a publicly available website a searchable, central registry of covered data brokers registered pursuant to this section and includes the information provided in the registered statement.

Section 613. Rule of construction.

This section states that compliance with this subtitle shall not relieve a covered data broker of an obligation to register with any state covered data broker registry.



TITLE VII. GENERAL PROVISIONS

This title includes general provisions for the entire Act.

Section 701. Enforcement.

A violation of this Act shall be treated as a violation of a regulation of the FTC regarding unfair or deceptive acts or practices. A state Attorney General, or an official or agency of a state, may bring a civil action on behalf of the resident of the state to enjoin an act or practice, enforce compliance with this Act, obtain damages, restitution, or other compensation on behalf of their residents, or obtain other legal and equitable relief.

Section 702. Judicial review.

This section states that the U.S. District Court for the District of Columbia shall have exclusive jurisdiction over any challenge to the constitutionality of this Act or the constitutionality of any action, finding, or determination under this Act.

Section 703. Rules of construction.

This section establishes rules of construction, including regarding First Amendment protections, existing federal laws, cooperation with law enforcement, and encryption, among other issues.

Section 704. Relationship to State Laws

This section establishes the Act's relationship to state and local laws. The Act only preempts a law, rule, requirement, or regulation of a state or local entity, to the extent that such law, rule, requirement, or regulation conflicts with a provision of this Act. The preemption does not affect contract, tort, or product liability law. A state or law entity may also enact or enforce any law, rule, requirement, or regulation that provides greater protection to minors than the protection provided by this Act. This section also amends Section 1303 of the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6502) to align its relationship to state laws with the same preemption standard as the rest of this Act.

Section 705. Severability.

Section 705 establishes severability regarding the bill.

Section 706. Effective Date.

Section 706 states that the Act shall take effect 1 year after the date of enactment, unless otherwise provided for in the Act.

