

Mr. GROTHMAN. Mr. Speaker, I encourage my colleagues to support this bill naming a post office for Paul Ignatius, a dedicated soldier and public servant, and I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Wisconsin (Mr. GROTHMAN) that the House suspend the rules and pass the bill, H.R. 4662.

The question was taken; and (two-thirds being in the affirmative) the rules were suspended and the bill was passed.

A motion to reconsider was laid on the table.

URSULA ELLEN KENNEDY POST OFFICE BUILDING

Mr. GROTHMAN. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 3350) to designate the facility of the United States Postal Service located at 340 East 1st Street in Tustin, California, as the "Ursula Ellen Kennedy Post Office Building".

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 3350

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. URSULA ELLEN KENNEDY POST OFFICE BUILDING.

(a) DESIGNATION.—The facility of the United States Postal Service located at 340 East 1st Street in Tustin, California, shall be known and designated as the "Ursula Ellen Kennedy Post Office Building".

(b) REFERENCES.—Any reference in a law, map, regulation, document, paper, or other record of the United States to the facility referred to in subsection (a) shall be deemed to be a reference to the "Ursula Ellen Kennedy Post Office Building".

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Wisconsin (Mr. GROTHMAN) and the gentleman from Virginia (Mr. SUBRAMANYAM) each will control 20 minutes.

The Chair recognizes the gentleman from Wisconsin.

GENERAL LEAVE

Mr. GROTHMAN. Mr. Speaker, I ask unanimous consent that all Members have 5 legislative days in which to revise and extend their remarks and include extraneous material on this measure.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Wisconsin?

There was no objection.

Mr. GROTHMAN. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I rise in support of this bill to rename a post office in Tustin, California, for Ursula Ellen Kennedy.

Ursula and her husband raised three children in Tustin, California. She was an accomplished author, publishing more than 500 articles and a book on essays.

In 1978, Ursula became the first woman ever elected to the Tustin City

Council. Twelve years later, Ursula became the first woman elected to mayor where she served for two terms.

Through her dedicated leadership to the city of Tustin, Ursula contributed to the creation of senior services, community planning, and environmental protections, leaving a lasting civic legacy.

She will be remembered for her humor, persistence, and relentless work ethic.

Mr. Speaker, I call on my House colleagues to support this bill, and I reserve the balance of my time.

Mr. SUBRAMANYAM. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I join my colleagues in supporting this bill. I encourage my colleagues to join me in supporting the life of Mayor Kennedy and her public service for the city of Tustin, California, by naming this post office after her.

Mr. Speaker, I reserve the balance of my time.

Mr. GROTHMAN. Mr. Speaker, I yield 4 minutes to the gentlewoman from California (Mrs. KIM).

Mrs. KIM. Mr. Speaker, I thank the gentleman for yielding.

Mr. Speaker, I rise today in strong support of H.R. 3350, to designate a post office in the city of Tustin, California, as the Ursula Ellen Kennedy Post Office Building.

Ursula Ellen Kennedy made history as the first woman elected to the Tustin City Council and the first woman to serve as mayor of Tustin.

At a time when few women held public office, Ursula stepped forward to serve the city she loved. In 1978, she was elected to the Tustin City Council, and 6 years later, her colleagues chose her to serve as Tustin's mayor.

However, her story did not begin in city hall. While raising her family, she became a writer, publishing more than 500 articles and a book of essays. In her forties, she enrolled in law school, earned her degree, passed the bar, and built her career as an attorney while raising her family.

Ursula came to city hall to build a stronger Tustin. When the city's planning commission was disbanded, she fought to restore it because she believed residents deserved a voice in their community's future.

She helped guide the development of east Tustin into the neighborhood we know today as Tustin Ranch. She also championed the senior center that still serves residents today, helping bring it from vision to reality. More than three decades later, it remains a lasting testament to her leadership.

Ursula Kennedy passed away in 2024 at the age of 87. She is remembered as a woman of vision, humor, fairness, and heart. She leaves behind a loving family who continues her legacy.

While we can never fully repay leaders like Ursula Kennedy, dedicating this post office ensures her legacy lives on in the community she helped build.

Mr. Speaker, I thank the Kennedy family for working with me on this bill, and I urge my colleagues to support H.R. 3350. May Ursula Kennedy's life continue to inspire us all.

□ 1530

Mr. SUBRAMANYAM. Mr. Speaker, I urge my colleagues to support me in passing H.R. 3350, and I yield back the balance of my time.

Mr. GROTHMAN. Mr. Speaker, I encourage my colleagues to support this bill naming a post office for Ursula Ellen Kennedy, an author, mother, and dedicated leader in public service.

Mr. Speaker, I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Wisconsin (Mr. GROTHMAN) that the House suspend the rules and pass the bill, H.R. 3350.

The question was taken; and (two-thirds being in the affirmative) the rules were suspended and the bill was passed.

A motion to reconsider was laid on the table.

KIDS INTERNET AND DIGITAL SAFETY ACT

Mr. GUTHRIE. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 7757) to protect children and teens online, empower parents and strengthen families, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 7757

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Kids Internet and Digital Safety Act" or the "KIDS Act".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

Sec. 1. Short title; table of contents.
Sec. 2. Definitions.

TITLE I—SHIELDING MINORS FROM OBSCENITY

Sec. 101. Short title.
Sec. 102. Definitions.
Sec. 103. Technology verification measures.
Sec. 104. Consultation requirements.
Sec. 105. GAO report.

TITLE II—ONLINE PLATFORMS

Sec. 201. Definitions.
Subtitle A—Kids Online Safety
Sec. 211. Short title.
Sec. 212. Definitions.
Sec. 213. Addressing harms to minors.
Sec. 214. Safeguards for minors, parental tools, and teen messaging controls.
Sec. 215. Reporting mechanism.
Sec. 216. Disclosure.
Sec. 217. Advertising and marketing information and labels.
Sec. 218. Advertising of illegal products to minors.
Sec. 219. Audit; report.
Sec. 220. Rule of construction on age verification.
Sec. 221. Rule of construction on encryption.
Subtitle B—Stop Profiling Youth and Kids
Sec. 231. Short title.

Sec. 232. Know; knows defined.

Sec. 233. Market research.

Sec. 234. Effective date.

TITLE III—SOCIAL GAMING PLATFORMS

Sec. 301. Short title.

Sec. 302. Definitions.

Sec. 303. Safeguards requirements for online video game providers.

TITLE IV—ARTIFICIAL INTELLIGENCE CHATBOTS

Sec. 401. Short title.

Sec. 402. Definitions.

Sec. 403. Certain statements prohibited.

Sec. 404. Disclosure required.

Sec. 405. Policies required.

Sec. 406. Rule of construction.

TITLE V—RESEARCH, EDUCATION, AND BEST PRACTICES FOR PROTECTING MINORS ONLINE

Subtitle A—Research

Sec. 501. Definitions.

Sec. 502. Exemption.

PART 1—SAFE SOCIAL MEDIA ACT

Sec. 511. Short title.

Sec. 512. Report by Commission on social media use by minors.

PART 2—NO FENTANYL ON SOCIAL MEDIA ACT

Sec. 513. Short title.

Sec. 514. Report on the ability of minors to access fentanyl through social media platforms.

PART 3—ASSESSING SAFETY TOOLS FOR PARENTS AND MINORS ACT

Sec. 515. Short title.

Sec. 516. Industry review and report.

PART 4—STUDY ON CHATBOTS AND MENTAL HEALTH OF MINORS

Sec. 517. Study required.

Sec. 518. Consultation.

Sec. 519. Report.

Subtitle B—Education

PART 1—PROMOTING A SAFE INTERNET FOR MINORS ACT

Sec. 521. Short title.

Sec. 522. Online safety education for minors.

PART 2—AI WARNINGS AND RESOURCES FOR EDUCATION (AWARE) ACT

Sec. 523. Short title.

Sec. 524. Safe chatbot use for minors.

Subtitle C—Partnerships and Best Practices

Sec. 525. Short title.

Sec. 526. Kids Internet Safety Partnership.

TITLE VI—KIDS PRIVACY PROTECTIONS

Subtitle A—COPPA 2.0

Sec. 601. Short title.

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

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

Sec. 604. GAO study.

Sec. 605. Severability.

Subtitle B—Data Broker Disclosures

Sec. 611. Definitions.

Sec. 612. Registration requirement.

Sec. 613. Rule of construction.

TITLE VII—GENERAL PROVISIONS

Sec. 701. Enforcement.

Sec. 702. Judicial review.

Sec. 703. Rules of construction.

Sec. 704. Relationship to State laws.

Sec. 705. Severability.

Sec. 706. Effective date.

SEC. 2. DEFINITIONS.

In this Act:

(1) **AGENCY.**—The term “agency” has the meaning given that term in section 551 of title 5, United States Code.

(2) **ALGORITHM.**—The term “algorithm” means any computational process, model, or

other automated means of processing to rank, order, promote, recommend, amplify, or similarly alter the delivery or display of information (including any text, image, audio, or video post and any page, group, account, channel, or affiliation).

(3) **ARTIFICIAL INTELLIGENCE.**—The term “artificial intelligence” has the meaning given that term in section 5002 of the National Artificial Intelligence Initiative Act of 2020 (15 U.S.C. 9401).

(4) **CHATBOT.**—The term “chatbot” means an artificial intelligence system, marketed to and available for use by consumers, that engages in interactive, natural-language communication with a user and generates or selects content in response to user inputs (including text, voice, or other inputs) using a conversational context.

(5) **COMMISSION.**—The term “Commission” means the Federal Trade Commission.

(6) **DESIGN FEATURE.**—The term “design feature”—

(A) means any feature or component of a covered platform that encourages an increase in or increases the frequency of use or time spent by a user who is a minor with respect to such covered platform; and

(B) includes—

(i) infinite scrolling or auto play;

(ii) rewards or incentives based on frequency of use or time spent;

(iii) notifications and push alerts;

(iv) badges or other visual award symbols based on frequency of use or time spent;

(v) appearance altering filters; and

(vi) personalized recommendation systems.

(7) **FULLY AUTOMATED SYSTEM.**—The term “fully automated system” means an algorithm the final outputs of which are, once computed, displayed directly to a covered user without review or alteration by a covered online platform.

(8) **MINOR.**—Except as otherwise provided, the term “minor” means an individual under the age of 17 years.

(9) **NARCOTIC DRUG.**—The term “narcotic drug” has the meaning given that term in section 102 of the Controlled Substances Act (21 U.S.C. 802).

(10) **PARENT.**—The term “parent”, with respect to a minor, means an adult with the legal right to make decisions on behalf of the minor, including any of the following:

(A) A natural parent.

(B) An adoptive parent.

(C) A legal guardian.

(D) An individual with legal custody over the minor.

(11) **PERSONAL INFORMATION.**—The term “personal information” has the meaning given that term in section 1302 of the Children’s Online Privacy Protection Act of 1998 (15 U.S.C. 6501) (as amended by section 602(a)(4) of this Act).

(12) **PERSONALIZED RECOMMENDATION SYSTEM.**—The term “personalized recommendation system”—

(A) means a fully automated system used to suggest, promote, or rank content, including other users, hashtags, and posts, based on the personal information of a user; and

(B) does not include a fully automated system that suggests, promotes, or ranks content based solely on the language, city or town, or age of a user.

(13) **SEXUAL EXPLOITATION AND ABUSE.**—The term “sexual exploitation and abuse” means any of the following:

(A) Any offense, including coercion and enticement, described in section 2422 of title 18, United States Code.

(B) Child pornography (as defined in section 2256 of title 18, United States Code).

(C) Trafficking for the production of images (as described in section 2251 of title 18, United States Code).

(D) Any offense described in section 1591 of title 18, United States Code.

(14) **STATE.**—The term “State” means each State of the United States, the District of Columbia, each commonwealth, territory, or possession of the United States, and each federally recognized Indian Tribe.

(15) **VERIFIABLE CONSENT.**—The term “verifiable consent” has the meaning given that term in section 1302 of the Children’s Online Privacy Protection Act of 1998 (15 U.S.C. 6501) (as amended by section 602(a)(5) of this Act).

TITLE I—SHIELDING MINORS FROM OBSCENITY

SEC. 101. SHORT TITLE.

This title may be cited as the “Shielding Children’s Retinas from Eggregious Exposure on the Net Act” or the “SCREEN Act”.

SEC. 102. DEFINITIONS.

In this title:

(1) **COVERED PLATFORM.**—The term “covered platform” means a website or other online platform—

(A) that is accessible by the public;

(B) with respect to which more than one-third of the material made available thereon is sexual material harmful to minors; and

(C) with respect to which the provider of such platform knowingly makes available the sexual material harmful to minors described in subparagraph (B).

(2) **MINOR.**—The terms “minor” has the meaning given that term in section 2256 of title 18, United States Code.

(3) **SEXUAL ACT; SEXUAL CONTACT.**—The terms “sexual act” and “sexual contact” have the meanings given those terms in section 2246 of title 18, United States Code.

(4) **SEXUAL MATERIAL HARMFUL TO MINORS.**—The term “sexual material harmful to minors” means a picture, image, graphic image file, film, videotape, or other visual depiction that—

(A)(i) taken as a whole and with respect to minors, appeals to the prurient interest in nudity, sex, or excretion;

(ii) depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or lewd exhibition of the genitals; and

(iii) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors; or

(B) is child pornography.

(5) **TECHNOLOGY VERIFICATION MEASURE.**—The term “technology verification measure” means technology that employs a system or process to determine whether it is more likely than not that a user of a covered platform is a minor.

(6) **TECHNOLOGY VERIFICATION MEASURE DATA.**—The term “technology verification measure data” means data that—

(A) is collected or processed for the purpose of fulfilling a request by an individual to access a covered platform or material on a covered platform; and

(B) is collected or processed for the purpose of utilizing or providing a technology verification measure pursuant to this title.

SEC. 103. TECHNOLOGY VERIFICATION MEASURES.

(a) **COVERED PLATFORM REQUIREMENTS.**—Beginning on the date that is 1 year after the date of the enactment of this Act, a provider of a covered platform shall—

(1) adopt and utilize commercially available technology verification measures with respect to the covered platform of such provider to identify minors; and

(2) prevent such minors from accessing any sexual material harmful to minors on the covered platform.

(b) **ADDITIONAL REQUIREMENTS FOR COMPLIANCE.**—In order to comply with subsection

(a), a provider of a covered platform (or a third party contracted by a provider of a covered platform with respect to such covered platform) shall, with respect to a covered platform of the provider, carry out the following:

(1) Use a technology verification measure in order to verify the age of a user.

(2) Provide that a user confirming that the user is not a minor is not sufficient to verify age.

(3) Provide clear and conspicuous notice containing information on the technology verification measures and other policies and procedures related to the technology verification measure data used to comply with this title.

(4) Take reasonable measures to address circumvention of technology verification measures.

(5) Not transfer, disclose, or retain any technology verification measure data beyond what is strictly necessary to use a technology verification measure pursuant to this title.

(6) Not collect or use technology verification measure data for any purpose beyond what is strictly necessary to utilize a technology verification measure pursuant to this title.

(c) USE OF THIRD PARTIES.—

(1) IN GENERAL.—A provider of a covered platform may contract with a third party to use technology verification measures for purposes of complying with subsection (a).

(2) OBLIGATIONS; LIABILITY.—A provider of a covered platform who contracts with a third party as described in paragraph (1) is not relieved from any obligation or liability under this title.

(d) CHOICE OF VERIFICATION MEASURES.—A provider of a covered platform may choose the specific technology verification measures to utilize for purposes of complying with subsection (a), if such measures satisfy subsection (b).

(e) TECHNOLOGY VERIFICATION MEASURE DATA SECURITY.—A provider of a covered platform (or a third party contracted by a provider of a covered platform with respect to such covered platform) shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and availability of technology verification measure data collected with respect to the covered platform of such provider (including by a third party contracted by such covered provider with respect to such covered platform) and protect such technology verification measure data against unauthorized access.

(f) RULE OF CONSTRUCTION.—Nothing in this section may be construed to require the submission of government-issued identification of any individual to a covered platform or a third party contracted by a provider of a covered platform to use a technology verification measure.

SEC. 104. CONSULTATION REQUIREMENTS.

In carrying out this title, the Commission shall consult with the following individuals, including with respect to the applicable standards and metrics for making a determination on whether a user of a covered platform is or is not a minor:

(1) Individuals with experience in computer science and software engineering.

(2) Individuals with experience in—

(A) advocating for online child safety; or

(B) providing services to minors who have been victimized by online child exploitation.

(3) Individuals with experience in consumer protection and online privacy.

(4) Individuals who supply technology verification measure products or have expertise in technology verification measures.

(5) Individuals with experience in data security and cryptography.

SEC. 105. GAO REPORT.

Not later than 3 years after the date of the enactment of this Act, the Comptroller General of the United States shall submit to Congress a report that includes the following:

(1) An analysis of the effectiveness of the technology verification measures required by section 103.

(2) An analysis of the rate of compliance with such section by providers of covered platforms and third parties contracted by such providers with respect to such covered platforms.

(3) An analysis of the data privacy and security measures used by covered platforms with respect to age verification processes.

(4) An analysis of the expression, speech, behavioral, economic, psychological, and societal effects of the technology verification measures required by section 103.

(5) Recommendations, if any, to the Commission on improving the enforcement of this title.

TITLE II—ONLINE PLATFORMS

SEC. 201. DEFINITIONS.

In this title:

(1) COVERED PLATFORM.—The term “covered platform” means a platform that is a website, software, application, or electronic service connected to the internet that meets the following requirements:

(A) Is publicly available for use by consumers.

(B) Enables the creation of a username or user identifier—

(i) that is searchable on the platform by other users through a function made available by the platform; and

(ii) that can be followed by or is similarly accessible to other users of the platform.

(C) As the primary purpose of the platform, facilitates the sharing and access to user-generated content through text, images, video, audio, or any other interactive medium.

(D) Uses a design feature to promote user engagement on the platform.

(E) Uses the personal information of the user to advertise, market, or make content recommendations.

(2) USER.—The term “user”, with respect to a covered platform, means an individual who registers an account or creates a profile on the covered platform.

Subtitle A—Kids Online Safety

SEC. 211. SHORT TITLE.

This subtitle may be cited as the “Kids Online Safety Act”.

SEC. 212. DEFINITIONS.

In this subtitle:

(1) CHILD.—The term “child” means an individual who is under the age of 13.

(2) COMPULSIVE USAGE.—The term “compulsive usage” means a persistent and repetitive use of a covered platform that substantially limits 1 or more major life activities of an individual (as described in section 3 of the Americans with Disabilities Act of 1990 (42 U.S.C. 12102)).

(3) DIRECT MESSAGING FEATURE.—

(A) IN GENERAL.—The term “direct messaging feature” means a function of a covered platform that enables a user to send a message, image, video, audio, or other communication directly to another user or a specific group of users of the covered platform.

(B) EXCLUSION.—The term “direct messaging feature” does not include a function of a covered platform that enables a user to post content on the covered platform to—

(i) a public or semi-public profile; or

(ii) a feed accessible to a broader group of users.

(4) EPHEMERAL MESSAGING FEATURE.—

(A) IN GENERAL.—The term “ephemeral messaging feature” means a function of a covered platform that permanently deletes or renders inaccessible a message, image, video, audio, or other communication sent between users of the covered platform (such that neither the sender nor any recipient of such communication, nor the covered platform, may readily retrieve or review the communication in the original form through the covered platform)—

(i) after a predetermined period;

(ii) once viewed by such a recipient; or

(iii) upon exiting the specific chat or messaging interface.

(B) EXCEPTIONS.—The term “ephemeral messaging feature” does not include—

(i) a function of a covered platform that allows a user of the covered platform to manually delete a message, image, video, audio, or other communication sent by such user after the transmission of the communication;

(ii) standard data volatility in transit or temporary caching for necessary functional and performance reasons;

(iii) the implementation of a time limited data retention schedule based on industry best practices as part of the explicit security policies of a covered platform or as needed to comply with applicable law or regulation; or

(iv) a standard process by which a user may request deletion of an account on a covered platform to include user content.

(5) GEOLOCATION INFORMATION.—The term “geolocation information” means information sufficient to identify a street name and name of a city or town.

(6) KNOW; KNOWS.—The term “know” or “knows” means to know or should have known.

(7) MESSAGING CONTROLS.—The term “messaging controls” means a set of tools or settings that a provider of a covered platform provides to a user of the covered platform that allows the user to manage the use of a direct messaging feature or an ephemeral messaging feature by such user.

(8) TEEN.—The term “teen” means an individual who has attained the age of 13 years and is under the age of 17 years.

(9) UNAPPROVED CONTACT.—The term “unapproved contact” means a user of a covered platform with respect to whom another user of the covered platform has not initiated a direct message conversation.

SEC. 213. ADDRESSING HARMS TO MINORS.

(a) IN GENERAL.—A provider of a covered platform shall establish, implement, maintain, and enforce reasonable policies, practices, and procedures that address the following harms to minors:

(1) Threats of physical violence so severe, pervasive, or objectively offensive that such threats impact a major life activity of a minor.

(2) Sexual exploitation and abuse.

(3) Distribution, sale, or use of narcotic drugs, tobacco products, cannabis products, gambling, or alcohol.

(4) Any financial harm caused by deceptive practices.

(b) CONSIDERATIONS.—The policies, practices, and procedures required by subsection (a) shall be appropriate to the size and complexity of the covered platform.

(c) RULES OF CONSTRUCTION.—Nothing in subsection (a) may be construed to—

(1) require a provider of a covered platform to prevent or preclude any minor from—

(A) deliberately and independently searching for, or specifically requesting, content; or

(B) accessing resources and information regarding the prevention or mitigation of the harms described in subsection (a); or

(2) impose a duty of care on a provider of a covered platform.

SEC. 214. SAFEGUARDS FOR MINORS, PARENTAL TOOLS, AND TEEN MESSAGING CONTROLS.**(a) SAFEGUARDS FOR MINORS.—**

(1) **SAFEGUARDS.**—A provider of a covered platform shall provide a user of or visitor to the covered platform who the provider knows is a minor with readily accessible and easy-to-use safeguards to do each of the following, as applicable:

(A) Limit the ability of other users to communicate with such user or visitor, including through direct messages or ephemeral messages.

(B) Prevent the profile or personal information of such user or visitor from being recommended or suggested to another user or visitor who the provider knows is not a minor.

(C) Prevent other users or visitors from seeing the current online or offline status of such user.

(D) Limit design features that encourage compulsive usage of the covered platform by such user or visitor.

(E) Restrict the sharing of geolocation information of such user or visitor to a third party that is not a processor and provide notice to such user or visitor and the parent of such user or visitor that geolocation information is collected.

(F) Control any personalized recommendation system on such covered platform, including with respect to the ability for such user or visitor to have—

(i) a prominently displayed option to opt out of any such personalized recommendation system, and

(ii) a prominently displayed option to limit types or categories of recommendations from any such personalized recommendation system.

(2) **OPTION.**—A covered platform shall provide a user that the covered platform knows is a minor with a readily accessible and easy-to-use option to limit the amount of time spent by such user on the covered platform.

(3) **DEFAULT SAFEGUARD SETTINGS FOR MINORS.**—A provider of a covered platform shall ensure that, in the case of a user of or visitor to the covered platform who the provider knows is a minor, the default setting of any safeguard described in paragraph (1) is the option available on the covered platform that provides the most protective level of control with respect to privacy and safety for such user or visitor.

(b) PARENTAL TOOLS.—

(1) **TOOLS.**—A provider of a covered platform shall provide readily accessible and easy-to-use parental tools that meet the requirements described in paragraph (2) for a parent of a user of the covered platform who the provider knows is a minor.

(2) **REQUIREMENTS.**—The parental tools described in paragraph (1) shall allow a parent of a user of the covered platform who the provider knows is a minor to do any of the following:

(A) View the privacy and account settings of such user, including the teen messaging controls described in subsection (c)(2).

(B) In the case of a user that the covered platform knows is a child, manage, change, and control the privacy and account settings of such user.

(C) The ability to restrict purchases and financial transactions by such user, if applicable.

(D) The ability to view metrics of total time spent on the covered platform and restrict time spent on the covered platform by such user, if such time restrictions do not amount to full exclusion of access of such user to the covered platform.

(E) Receive a notification when such user receives a request from another user who seeks to initiate direct messaging or ephemeral

messaging with such user for the first time.

(F) In the case of a user that the covered platform knows is a child, disable any ephemeral messaging features or direct messaging features.

(3) **NOTICE TO PARENTS OF MINORS.**—A provider of a covered platform shall provide clear and conspicuous notice to a parent of a user of the covered platform who the provider knows is a minor about the availability of the parental tools described in paragraph (1).

(4) **NOTICE TO MINORS.**—A provider of a covered platform shall provide clear and conspicuous notice to a user of the covered platform who the provider knows is a minor when any parental tool described in paragraph (1) is in effect and any setting or control that has been applied.

(5) **DEFAULT TOOLS FOR CHILDREN.**—A provider of a covered platform shall ensure that, in the case of a user of or visitor to the covered platform who the provider knows is a child, the default setting for any parental tool described in paragraph (1) is the option available on the covered platform that provides the most protective level of control with respect to privacy and safety for such user or visitor.

(6) **APPLICATION TO EXISTING ACCOUNTS.**—If, before the effective date of this subtitle, a provider of a covered platform provides a parent of a user of the covered platform who the provider knows is a child with notice and the ability to enable a parental tool described in paragraph (1) in a manner that would otherwise comply with this subsection and the parent opts out of enabling any such parental tool, the covered platform is not required to enable any such parental tool with respect to such user by default on or after such effective date.

(c) ADDITIONAL MESSAGING CONTROLS FOR TEENS.—

(1) **IN GENERAL.**—A provider of a covered platform that offers, provides, or enables any direct messaging feature or ephemeral messaging feature of such covered platform to any user of the covered platform who the provider knows is a teen shall provide easily accessible and usable messaging controls described in paragraph (2) to such user that the user may activate and manage.

(2) **TEEN MESSAGING CONTROLS.**—The teen messaging controls described in this paragraph shall allow a user of the covered platform to do any of the following:

(A) Receive a timely notification that—

(i) alerts the user about a request from an unapproved contact who seeks to use a direct messaging feature or an ephemeral messaging feature of the covered platform with respect to the user; and

(ii) allows the user to approve or deny the request before the unapproved contact and the user engage in any direct messaging or ephemeral messaging through any such direct messaging feature or ephemeral messaging feature.

(B) View and manage a list of any contacts approved for engaging in direct messaging or ephemeral messaging with the user through any direct messaging feature or any ephemeral messaging feature of the covered platform.

(C) Disable any direct messaging feature or ephemeral messaging feature.

(D) Prevent any specific user, any specific group of users, or other user in general from initiating or continuing to engage in direct messaging or ephemeral messaging with the user through any direct messaging feature or any ephemeral messaging feature of the covered platform.

(E) Enable the user to set a profile of the user on the covered platform as hidden.

(d) **RULES OF APPLICATION.**—

(1) **ACCESSIBILITY.**—With respect to any safeguard described in subsection (a)(1), any parental tool described in subsection (b)(1), and any teen messaging control described in subsection (c)(2), a provider of a covered platform shall provide each of the following:

(A) Information and control options in a clear and conspicuous manner that takes into consideration the differing ages, capacities, and developmental needs of a user of the covered platform who the provider knows is a minor most likely to access the covered platform and does not encourage such a user or a parent of such a user to weaken or disable any such safeguard, parental tool, or teen messaging control.

(B) Readily accessible and easy-to-use controls to enable or disable any such safeguard, parental tool, or teen messaging control, as appropriate.

(C) Information and control options in the same language, form, and manner as the provider provides the product or service used by such a user or a parent of such a user.

(2) **TIMING CONSIDERATIONS; APPLICATION OF CHANGES TO OFFLINE DEVICES OR ACCOUNTS.**—If the device of a user or user account does not have access to the internet at the time of a change to a parental tool described in subsection (b)(1), the provider of the relevant covered platform shall apply changes the next time the device or user is connected to the internet.

(3) **PROHIBITION.**—A provider of a covered platform may not knowingly use a user interface with the purpose or substantial effect of obscuring, subverting, or impairing the use by a user of the covered platform who the provider knows is a minor or a parent of such a user of any safeguard described in subsection (a)(1), any parental tool described in subsection (b)(1), or any teen messaging control described in subsection (c)(2).

(e) **RULES OF CONSTRUCTION.**—Nothing in this section may be construed to do any of the following:

(1) Prevent a provider of a covered platform from taking reasonable measures to block, detect, or prevent the distribution of unlawful, obscene, or other harmful material to minors or any other harms to minors described in section 213(a).

(2) Prevent a provider of a covered platform from entering into an agreement with a third party with a primary or exclusive function of—

(A) providing—

(i) any safeguard described in subsection (a)(1);

(ii) any parental tool described in subsection (b)(1); or

(iii) any teen messaging control described in subsection (c)(2); or

(B) otherwise assisting with meeting the requirements described in subsections (a), (b), and (c).

(3) Prevent a parent or user from authorizing a third party described in paragraph (2) to implement—

(A) any safeguard described in subsection (a)(1);

(B) any parental tool described in subsection (b)(1); or

(C) any teen messaging control described in subsection (c)(2).

SEC. 215. REPORTING MECHANISM.

(a) **REPORTING TOOLS.**—A provider of a covered platform shall provide each of the following:

(1) A readily accessible and easy-to-use means for a user of or visitor to the covered platform to submit a report to the covered platform of any harm to a minor related to the use of the covered platform.

(2) An electronic point of contact specific to matters involving harms to a minor.

(3) Confirmation of the receipt of any such report and, within the applicable time period

described in subsection (b), a substantive response to the user or visitor who submitted the report.

(b) **TIMING.**—A covered platform shall establish an internal process to receive and substantively respond to a report submitted under subsection (a)(1) in a reasonable and timely manner, but in no case later than—

(1) 10 days after the date on which the report is received; or

(2) if the report involves an imminent threat to the safety of a minor, the date that is as prompt as needed to address the reported threat to safety.

SEC. 216. DISCLOSURE.

(a) **NOTICE.**—

(1) **REGISTRATION OR PURCHASE.**—Before any registration or purchase on a covered platform by a user of or visitor to the covered platform who the provider knows is a minor, the provider shall provide clear, conspicuous, and easy-to-understand notice with respect to each of the following:

(A) The policies and practices of the covered platform with respect to safeguards for minors.

(B) Information about how to access any safeguard described in section 214(a)(1), any parental tool described in section 214(b)(1), and any teen messaging control described in section 214(c)(2).

(2) **NOTIFICATION.**—

(A) **NOTICE AND ACKNOWLEDGMENT.**—In the case of a user of or visitor to a covered platform who the provider of the covered platform knows is a minor, the provider shall provide information about any safeguard described in section 214(a)(1) and any parental tool described in section 214(b)(1) to a parent of such user or visitor.

(B) **REASONABLE EFFORT.**—A covered platform shall be deemed to have satisfied the requirement described in subparagraph (A) if the provider of the covered platform is in compliance with the requirements of the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501 et seq.) to use reasonable efforts (taking into consideration commercially available technology) to provide a parent with the information required by paragraph (1)(B).

(b) **CONSOLIDATED NOTICES.**—For purposes of this section, a provider of a covered platform may consolidate the process for providing information required by this section with the obligations of the provider to provide relevant notice and obtain verifiable consent under the Children's Online Privacy Protection Act of 1998.

SEC. 217. ADVERTISING AND MARKETING INFORMATION AND LABELS.

A provider of a covered platform shall provide clear, conspicuous, and easy-to-understand labels and information, which may be provided through a link to another web page or disclosure, to a user of or visitor to the covered platform who the provider knows is a minor on advertisements regarding the disclosure of endorsements of products, services, or brands made for commercial consideration by other users of the covered platform.

SEC. 218. ADVERTISING OF ILLEGAL PRODUCTS TO MINORS.

A provider of a covered platform may not facilitate the advertising of narcotic drugs, cannabis products, tobacco products, gambling, or alcohol to a user of or visitor to the covered platform who the provider knows is a minor.

SEC. 219. AUDIT; REPORT.

(a) **AUDIT REQUIRED.**—Not later than 18 months after the date of the enactment of this subtitle, and annually thereafter, a provider of a covered platform shall ensure that an independent, third-party auditor conducts an independent, third-party audit of the covered platform.

(b) **AUDIT SPECIFICATIONS.**—

(1) **CRITERIA.**—In conducting an audit required by subsection (a), an independent, third-party auditor shall do the following:

(A) Consider widely accepted or evidence-based approaches, best practices, frameworks, and methods related to any safeguard described in section 214(a)(1), any parental tool described in section 214(b)(1), and any teen messaging control described in section 214(c)(2).

(B) Consider widely accepted or evidence-based approaches, best practices, frameworks, and methods related to identifying, preventing, and mitigating the harms to minors described in section 213(a).

(C) Consult with parents (including parents with relevant experience), public health and mental health nonprofit organizations, health and development organizations, and experts in freedom of expression about methods to identify, prevent, and mitigate such harms.

(2) **CONTENTS.**—An audit required by subsection (a) shall include the following:

(A) An assessment of the extent to which the relevant covered platform is likely to be accessed by minors, including with respect to any difference between children and teens.

(B) An accounting of the following:

(i) The number of users using such covered platform who the provider of such covered platform knows to be minors located in the United States.

(ii) The median and mean amounts of time spent on such covered platform by such users during the year in which such audit is conducted.

(iii) A description of the policies, practices, and procedures implemented to address the harms to minors described in section 213(a).

(iv) The number of times that any safeguard described in section 214(a)(1) has been exercised during the year in which such audit is conducted.

(v) The number of times that any parental tool described in section 214(b)(1) has been exercised during the year in which such audit is conducted.

(vi) The number of times that any teen messaging control described in section 214(c)(2) has been exercised during the year in which such audit is conducted.

(vii) The number of reports, categorized by types of harms to a minor, received by such covered platform through the reporting mechanism described in section 215(a)(1) during the year in which such audit is conducted.

(C) A description of such safeguards for minors and parental tools that are available to minors and parents on such covered platform.

(D) A description of how such covered platform handles reports received through such reporting mechanism, including the rate of response to such a report and the timeliness and substantiveness of any such response.

(E) A description of whether, how, and for what purpose such covered platform collects or processes categories of personal information of minors.

(F) If the covered platform has a process used to create, implement, or evaluate the impact of a design feature of the covered platform used by minors, a description of such process.

(3) **COOPERATION BY COVERED PLATFORM.**—A provider of a covered platform shall facilitate an audit of the covered platform required by subsection (a) by doing the following:

(A) Providing or otherwise making available to the independent, third-party auditor that conducts such audit any information or material in the possession, custody, or control of such covered platform relevant to such audit.

(B) Providing or otherwise making available to such auditor access to any network, system, or asset relevant to such audit.

(C) Disclosing any material fact to such auditor and not misrepresenting any material fact.

(c) **REPORT TO COMMISSION.**—Not later than 30 days after the date on which an audit required by subsection (a) is completed, the provider of the relevant covered platform shall submit to the Commission the results of the audit.

(d) **PUBLIC REPORT.**—Not later than 45 days after the date on which an audit required by subsection (a) is completed, the provider of the relevant covered platform shall issue a public report that—

(1) includes the information required by clauses (i), (ii), (iv), (v), and (vi) of subsection (b)(2)(B); and

(2) notwithstanding paragraph (1), may include any other information required by this section.

SEC. 220. RULE OF CONSTRUCTION ON AGE VERIFICATION.

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.

SEC. 221. RULE OF CONSTRUCTION ON ENCRYPTION.

No requirement under this subtitle to restrict any feature for a user of a covered platform or to provide messaging controls for a direct messaging feature or ephemeral messaging feature of a covered platform may be construed to override any protection for an encrypted communication described in this subtitle and a provider of a covered platform shall adhere to any such requirement, to the maximum extent technically feasible, through means that do not compromise the integrity of strong encryption offered to any user of the covered platform.

Subtitle B—Stop Profiling Youth and Kids

SEC. 231. SHORT TITLE.

This subtitle may be cited as the “Stop Profiling Youth and Kids Act” or the “SPY Kids Act”.

SEC. 232. KNOW; KNOWS DEFINED.

The term “know” or “knows” means to have actual knowledge or to have acted in willful disregard.

SEC. 233. MARKET RESEARCH.

(a) **PROHIBITION OF RESEARCH ON MINORS.**—A provider of a covered platform may not, in the case of a user or visitor of the covered platform who the provider knows is a minor, conduct market or product-focused research on such user or visitor unless any such research is—

(1) used solely to improve the privacy, security, transparency, or safety of the covered platform, including with respect to a design feature or any safeguard, setting, or tool offered to such user or visitor or a parent of such user or visitor; or

(2) necessary for compliance with a Federal or State law.

(b) **RULE OF CONSTRUCTION.**—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.

SEC. 234. EFFECTIVE DATE.

This subtitle shall take effect on the date that is 90 days after the date of the enactment of this Act.

TITLE III—SOCIAL GAMING PLATFORMS

SEC. 301. SHORT TITLE.

This title may be cited as the “Safer Guarding of Adolescents from Malicious

Interactions on Network Games Act” or the “Safer GAMING Act”.

SEC. 302. DEFINITIONS.

(a) **DEFINITIONS.**—In this title:

(1) **COVERED COMMUNICATION TOOL.**—The term “covered communication tool” means 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.

(2) **COVERED USER.**—The term “covered user” means a user of an interactive online video game if the online video game provider of such interactive online video game knows that such user is a minor.

(3) **INTERACTIVE ONLINE VIDEO GAME.**—The term “interactive online video game” means a video game that—

(A) connects to the internet; and

(B) allows a user of such video game to communicate with other users of such video game.

(4) **KNOW; KNOWS.**—The term “know” or “knows” means know or should have known.

(5) **MINOR.**—The term “minor” means an individual under the age of 17 years.

(6) **ONLINE VIDEO GAME PROVIDER.**—The term “online video game provider” means 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.

(7) **VIDEO GAME.**—The term “video game” means a software program that—

(A) receives and stores data or instructions generated by the user of such software program; and

(B) processes such data or instructions to create an interactive game for such user to play on a computer, gaming system, console, mobile device, or other technological means.

SEC. 303. SAFEGUARDS REQUIREMENTS FOR ONLINE VIDEO GAME PROVIDERS.

(a) **COMMUNICATION SAFEGUARDS.**—An online video game provider shall provide safeguards to a parent of a covered user of an interactive online video game of such online video game provider that allow the parent to limit communication between such covered user and any other user of such interactive online video game.

(b) **FEATURES.**—

(1) **IN GENERAL.**—An online video game provider shall ensure that the safeguards required by subsection (a) meet the following requirements:

(A) Be accessible and easy to use.

(B) Be enabled by default on an account of a covered user of the interactive online video game of such online video game provider.

(C) Be set to the most protective level of control by default on any such account.

(2) **PROTECTIVE LEVEL OF CONTROL.**—For purposes of paragraph (1)(C), the term “most protective level of control” means the relevant safeguards—

(A) are set to the most restrictive setting by default; and

(B) may be set to a less restrictive setting only by a parent of a covered user.

(3) **OTHER SAFEGUARDS REQUIRED.**—An online video game provider shall provide to a covered user and a parent of a covered user of an interactive online video game of the online video game provider readily accessible and easy-to-use safeguards to do the following:

(A) Prevent a profile of such covered user or personal information connected to such covered user from being recommended or suggested to any other user of such interactive online video game who is not a minor.

(B) Restrict purchases and financial transactions by such covered user.

(C) Limit the amount of time spent by such covered user on such interactive online video game.

(c) **DEVICE CONTROLS.**—Nothing in this section may be construed to prohibit an online video game provider from making available to the parent of a covered user of an interactive online video game of the online video game provider a single user interface that permits such parent to do the following:

(1) Set the level or scope of any covered communication tool with respect to multiple other users or categories of users or set the level or scope of multiple covered communication tools.

(2) Control the safeguards required by this section.

(d) **NOTICE TO COVERED USERS.**—An online video game provider shall provide clear and conspicuous notice to a covered user of an interactive online video game of the online video game provider when the safeguards required by this section are in effect that describes the settings or safeguards that have been applied.

TITLE IV—ARTIFICIAL INTELLIGENCE CHATBOTS

SEC. 401. SHORT TITLE.

This title may be cited as the “Safe-guarding Adolescents From Exploitative BOTs Act” or the “SAFE BOTs Act”.

SEC. 402. DEFINITIONS.

In this title:

(1) **CHATBOT PROVIDER.**—

(A) **IN GENERAL.**—The term “chatbot provider” means 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.

(B) **LIMITATION.**—A person that provides a website, mobile application, or other online service that includes a chat function incidental to the primary purpose of such website, application, or service may not be treated as a chatbot provider solely on the basis of such incidental chat function.

(2) **COVERED USER.**—The term “covered user” means a user of a chatbot if the provider of such chatbot knows that such user is a minor.

(3) **KNOW; KNOWS.**—The term “know” or “knows” means know or should have known.

SEC. 403. CERTAIN STATEMENTS PROHIBITED.

A chatbot provider may not provide to a covered user a chatbot that states to the covered user that the chatbot is a licensed professional (unless such statement is true).

SEC. 404. DISCLOSURE REQUIRED.

(a) **IN GENERAL.**—A chatbot provider shall clearly and conspicuously disclose to each covered user of a chatbot of such chat provider a disclosure of the following:

(1) The chatbot is an artificial intelligence system and not a natural person.

(2) Resources for contacting a suicide and crisis intervention hotline.

(b) **TIMING.**—

(1) **AI SYSTEM DISCLOSURE.**—A disclosure required by subsection (a)(1) shall be made—

(A) at the initiation of the first interaction of a covered user with a chatbot; and

(B) at any point at which, during an interaction between a covered user and a chatbot, the covered user prompts the chatbot about whether the chatbot is an artificial intelligence system.

(2) **CRISIS RESOURCES DISCLOSURE.**—A disclosure required by subsection (a)(2) shall be made at any point at which, during an interaction between a covered user and a chatbot, the covered user prompts the chatbot about suicide or suicidal ideation.

(c) **USE OF PLAIN LANGUAGE.**—Any disclosure required by subsection (a) shall be made in a manner that is clear and age-appro-

priate using plain language such that the disclosure is reasonably understandable by a minor.

SEC. 405. POLICIES REQUIRED.

A chatbot provider shall establish, implement, and maintain reasonable policies, practices, and procedures—

(1) to ensure that a chatbot of the chatbot provider advises a covered user of the chatbot to take a break from the chatbot at the point at which a continuous and uninterrupted interaction of such covered user with such chatbot has lasted for 3 hours; and

(2) to address, with respect to covered users—

(A) sexual exploitation and abuse;

(B) the promotion of gambling that is restricted from or prohibited for minors by law; and

(C) the promotion of the distribution, sale, or use of narcotic drugs, tobacco products, or alcohol that are restricted from or prohibited for minors by law.

SEC. 406. RULE OF CONSTRUCTION.

Nothing in this title may be construed to require a chatbot provider to prevent or preclude any covered user of a chatbot of the chatbot provider from accessing resources and information regarding the prevention or mitigation of the harms described in section 405(2).

TITLE V—RESEARCH, EDUCATION, AND BEST PRACTICES FOR PROTECTING MINORS ONLINE

Subtitle A—Research

SEC. 501. DEFINITIONS.

In this subtitle:

(1) **FENTANYL.**—The term “fentanyl” includes any fentanyl analogue and fentanyl-related substance.

(2) **FENTANYL-RELATED SUBSTANCE.**—The term “fentanyl-related substance” has the meaning given that term in subsection (e) of schedule I of section 202(c) of the Controlled Substances Act (21 U.S.C. 812(c)).

(3) **RELEVANT CONGRESSIONAL COMMITTEES.**—The term “relevant congressional committees” means—

(A) the Committee on Energy and Commerce of the House of Representatives; and

(B) the Committee on Commerce, Science, and Transportation of the Senate.

(4) **SOCIAL MEDIA PLATFORM.**—The term “social media platform”—

(A) means a public-facing website, internet application, or mobile internet application, including a social network or video sharing service—

(i) that serves the public; and

(ii) that primarily provides a forum for user-generated content, including messages, videos, images, games, and audio files; and

(B) does not include—

(i) a provider of broadband internet access service (as described in section 8.1(b) of title 47, Code of Federal Regulations, or any successor regulation); or

(ii) electronic mail.

SEC. 502. EXEMPTION.

Subchapter I of chapter 35 of title 44, United States Code (commonly known as the “Paperwork Reduction Act”) does not apply to this subtitle.

PART 1—SAFE SOCIAL MEDIA ACT

SEC. 511. SHORT TITLE.

This part may be cited as the “Safe Social Media Act”.

SEC. 512. REPORT BY COMMISSION ON SOCIAL MEDIA USE BY MINORS.

The Commission, in coordination with the Secretary of Health and Human Services (acting through the Assistant Secretary for Mental Health and Substance Use), shall do the following:

(1) Conduct a study on social media platform use by minors, including with respect to the following:

(A) What personal information is collected by social media platforms with respect to minors.

(B) How such personal information is used by the algorithms of the social media platforms.

(C) How such personal information is used with respect to targeted advertising.

(D) How often minors use social media platforms daily.

(E) Differences in use of social media platforms related to the age ranges of minors.

(F) Mental health effects on minors linked to the use of social media platforms.

(G) Potential harmful effects and benefits for minors from extended social media platform use.

(2) Not later than 3 years after the date of the enactment of this Act, submit to the relevant congressional committees a report on the findings of the study conducted under paragraph (1), including any recommended policy changes based on such findings.

PART 2—NO FENTANYL ON SOCIAL MEDIA ACT

SEC. 513. SHORT TITLE.

This part may be cited as the “No Fentanyl on Social Media Act”.

SEC. 514. REPORT ON THE ABILITY OF MINORS TO ACCESS FENTANYL THROUGH SOCIAL MEDIA PLATFORMS.

(a) REPORT REQUIRED.—Not later than 1 year after the date of the enactment of this Act, the Commission, in coordination with the Secretary of Health and Human Services (acting through the Commissioner of Food and Drugs), shall submit to the relevant congressional committees and publish on a website of the Commission a report on the ability of minors to access fentanyl, including through pressed pills, through social media platforms and that includes the following:

(1) The prevalence and ability for minors to access fentanyl from drug sellers on social media platforms.

(2) The impact of such prevalence and access on minors, including with respect to health risks and risks to physical safety.

(3) How drug sellers use social media platforms to market, sell, deliver, distribute, dispense, and engage in other transactions related to the provision of fentanyl to minors.

(4) How design features and other characteristics of social media platforms affect the ability of minors to access fentanyl.

(5) Other measures taken by law enforcement, the medical community, and others to address the issues described in paragraphs (1) through (4).

(6) Practices, policies, and other measures taken by social media platforms to address the ability of drug sellers to use social media platforms and the effectiveness of such practices, policies, and measures.

(7) Recommendations for Congress to eliminate the prevalence and ability for minors to access fentanyl through social media platforms.

(b) CONSULTATION REQUIRED.—In developing the report required by subsection (a), the Commission shall consult with any relevant agencies and stakeholders, including parents, social media platforms, law enforcement, medical professionals, and other relevant experts.

(c) REDACTION PERMITTED.—In publishing the report required by subsection (a), the Commission, in consultation with the Attorney General, may redact any information relating to paragraph (3) or (5) of such subsection that may compromise any law enforcement tactic, strategy, or technique.

PART 3—ASSESSING SAFETY TOOLS FOR PARENTS AND MINORS ACT

SEC. 515. SHORT TITLE.

This part may be cited as the “Assessing Safety Tools for Parents and Minors Act”.

SEC. 516. INDUSTRY REVIEW AND REPORT.

(a) REVIEW.—Not later than 6 months after the date of the enactment of this Act, the Commission, in consultation with industry, parents, individuals with expertise in communications technologies, parental controls, privacy, and mental health, and any other appropriate entities as determined by the Commission, shall—

(1) initiate a review of industry efforts to promote online safety for minors through education, parental and child safety tools, age-appropriate labels for content, privacy and other safety settings, and any other relevant technologies or initiatives; and

(2) examine the effectiveness of industry efforts identified under paragraph (1) to mitigate online harms for minors and provide recommendations for industry, Congress, and agencies to improve online safety for minors.

(b) SUBMISSION OF REPORT.—Not later than 3 years after the date of the enactment of this Act, the Commission shall submit to the relevant congressional committees a report with any findings and recommendations resulting from the review and examination required by subsection (a).

PART 4—STUDY ON CHATBOTS AND MENTAL HEALTH OF MINORS

SEC. 517. STUDY REQUIRED.

The Secretary of Health and Human Services, acting through the Director of the National Institutes of Health, shall conduct a 4-year longitudinal study to evaluate the risks and benefits of chatbots with respect to the mental health of minors, including with respect to loneliness, anxiety, social skill building, social isolation, depression, self-harm, and suicidal ideation.

SEC. 518. CONSULTATION.

In conducting the study required by section 517, the Secretary, acting through the Director, shall consult with the following:

(1) The Director of the National Institute of Mental Health.

(2) Pediatric mental health experts.

(3) Technologists.

(4) Ethicists.

(5) Educators.

SEC. 519. REPORT.

Not later than 4 years after the date of the enactment of this Act, the Secretary, acting through the Director, shall submit to the relevant congressional committees and the Committee on Health, Education, Labor, and Pensions of the Senate a report on the results of the study required by section 517 and any related recommendations.

Subtitle B—Education

PART 1—PROMOTING A SAFE INTERNET FOR MINORS ACT

SEC. 521. SHORT TITLE.

This part may be cited as the “Promoting a Safe Internet for Minors Act”.

SEC. 522. ONLINE SAFETY EDUCATION FOR MINORS.

(a) AMENDMENT.—Subtitle A of the Protecting Children in the 21st Century Act (15 U.S.C. 6551 et seq.) is amended—

(1) by striking sections 211 through 214 and 216 and inserting the following:

“SEC. 211. PUBLIC AWARENESS AND EDUCATIONAL CAMPAIGN.

“Not later than 180 days after the date of the enactment of this section, the Commission, in partnership with the heads of other relevant agencies, State and local governments, nonprofit organizations, schools, industry, law enforcement, medical profes-

sionals, and other appropriate entities, shall carry out a program throughout the United States to promote the safe use of the internet by minors that includes the following:

“(1) The identification, promotion, and encouragement of best practices for educators, online platforms, minors, and parents and guardians to protect minors online.

“(2) The establishment and implementation of an outreach and education campaign throughout the United States that promotes online safety for minors.

“(3) The facilitation of access to, and the exchange of, information regarding online safety for minors to promote up-to-date knowledge regarding harms and risks negatively impacting or benefits positively impacting minors online.

“(4) The facilitation of access to publicly accessible online safety education and public awareness efforts by other relevant agencies, State and local governments, nonprofit organizations, schools, industry, and other appropriate entities.

“SEC. 212. ANNUAL REPORT.

“Not later than 1 year after the date of the enactment of this section, and annually thereafter for 10 years, the Commission shall submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Energy and Commerce of the House of Representatives a report that describes the program carried out under section 211.

“SEC. 213. DEFINITIONS.

“In this subtitle:

“(1) AGENCY.—The term ‘agency’ has the meaning given that term in section 551 of title 5, United States Code.

“(2) COMMISSION.—The term ‘Commission’ means the Federal Trade Commission.

“(3) MINOR.—The term ‘minor’ means an individual under the age of 17.

“(4) NONPROFIT ORGANIZATION.—The term ‘nonprofit organization’ means an organization that is described in section 501(c)(3) of the Internal Revenue Code of 1986 and exempt from taxation under section 501(a) of such Code.

“(5) ONLINE SAFETY.—The term ‘online safety’ includes issues regarding the use of the internet in a manner that promotes safe online activity for minors through the following:

“(A) Protecting minors from cybercrimes, access to narcotics, tobacco products, gambling, alcohol, and other adult content.

“(B) Preventing compulsive behavior online and other adverse impacts on the physical and mental health of minors.

“(C) Facilitating the effective use of safeguards, parental controls, and other tools to empower parents, guardians, and minors to protect minors online.

“(6) STATE.—The term ‘State’ means each of the several States, the District of Columbia, each commonwealth, territory, or possession of the United States, and each federally recognized Indian Tribe.”; and

(2) by redesignating section 215 as section 214.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of contents of the Protecting Children in the 21st Century Act (15 U.S.C. 6551 et seq.) is amended by striking the items related to sections 211 through 216 and inserting the following:

“Sec. 211. Public awareness and educational campaign.

“Sec. 212. Annual report.

“Sec. 213. Definitions.

“Sec. 214. Promoting online safety in schools.”.

PART 2—AI WARNINGS AND RESOURCES FOR EDUCATION (AWARE) ACT

SEC. 523. SHORT TITLE.

This part may be cited as the “AI Warnings And Resources for Education Act” or the “AWARE Act”.

SEC. 524. SAFE CHATBOT USE FOR MINORS.

(a) **EDUCATIONAL RESOURCES.**—Not later than 1 year after the date of the enactment of this Act, the Commission, in consultation with relevant agencies, shall develop and make available to the public educational resources for parents, educators, and minors with respect to the safe and responsible use of chatbots by minors.

(b) **CONTENTS.**—The educational resources developed and made available under subsection (a) shall include resources on the following:

(1) The risks and benefits of chatbot use.
(2) Privacy and data collection practices.
(3) Best practices for parents supporting the safe use of chatbots by minors.

(c) **YOUVILLE.**—The Commission, in a manner appropriate for minors, shall model the educational resources developed and made available under subsection (a) on the Youville program of the Commission.

Subtitle C—Partnerships and Best Practices

SEC. 525. SHORT TITLE.

This subtitle may be cited as the “Kids Internet Safety Partnership Act”.

SEC. 526. KIDS INTERNET SAFETY PARTNERSHIP.

(a) **ESTABLISHMENT.**—Not later than 1 year after the date of the enactment of this Act, the Secretary shall establish the Kids Internet Safety Partnership.

(b) **DIRECTOR.**—The Secretary shall appoint a Director to be the head of the Partnership.

(c) **DUTIES.**—The duties of the Partnership shall be the following:

(1) Coordinate with relevant agencies (including the Commission) and stakeholders to identify the following:

(A) The risks for minors with respect to the use of websites, online services, online applications, and mobile applications.

(B) The benefits for minors with respect to the use of websites, online services, online applications, and mobile applications.

(C) Widely accepted or evidence-based best practices, taking into account minors of different ages, to—

(i) address the risks identified under subparagraph (A); and

(ii) preserve and enhance the benefits identified under subparagraph (B).

(2) Not later than 1 year after the date on which the Partnership is established, and every 2 years thereafter, publish on a publicly available website a report that details—

(A) the identifications made under paragraph (1); and

(B) the efficacy and adoption by websites, online services, online applications, and mobile applications of—

(i) safeguards for minors; and

(ii) parental tools.

(3) Not later than 2 years after the date on which the Partnership is established, publish on a publicly available website a playbook for providers and developers of websites, online services, online applications, and mobile applications to facilitate the implementation of widely accepted or evidence-based best practices that account for minors of different ages and address the risks identified under paragraph (1)(A) and preserve and enhance the benefits identified under paragraph (1)(B), including best practices with respect to the following:

(A) Age verification, assurance, and estimation techniques.

(B) Design features.

(C) Parental tools.

(D) Default privacy and account settings.

(E) Reporting systems and tools.

(F) Third-party safety software services.

(G) Limitations and opt-outs related to personalized recommendation systems and chatbots.

(d) **STAKEHOLDERS.**—In coordinating with stakeholders as required by subsection (c)(1), the Partnership shall coordinate with the following:

(1) Academic experts with specific expertise with respect to the prevention of risks for minors online.

(2) Researchers with specific expertise with respect to social media.

(3) Parents and minors with demonstrated experience with respect to the safety of minors online.

(4) Educators with demonstrated experience with respect to the safety of minors online.

(5) Online platforms.

(6) Experts in academia and civil society with specific expertise with respect to constitutional law, privacy, free expression, access to information, and civil liberties.

(7) State attorneys general (or designees thereof who work in State or local government).

(e) **SUNSET.**—The Partnership shall terminate on the date that is 5 years after the date on which the Partnership is established.

(f) **DEFINITIONS.**—In this section:

(1) **PARENTAL TOOL.**—The term “parental tool”—

(A) means a tool that—

(i) the provider of a website, online service, online application, or mobile application provides to a parent of a user who such provider knows is a minor; and

(ii) the parent uses to support such user with respect to the use of the website, service, or application; and

(B) includes a tool that allows a parent of a user who the provider of such a website, service, or application knows is a minor to—

(i) view or change the privacy and account settings of such user;

(ii) grant or withdraw verifiable consent;

(iii) restrict the purchases and financial transactions of such user;

(iv) view metrics of the total time spent on such website, service, or application by such user;

(v) restrict time spent on such website, service, or application by such user;

(vi) report illegal or harmful conduct on such website, service, or application with respect to which such user may be a victim; and

(vii) limit or opt-out of personalized recommendation systems or chatbots.

(2) **PARTNERSHIP.**—The term “Partnership” means the Kids Internet Safety Partnership established under subsection (a).

(3) **SECRETARY.**—The term “Secretary” means the Secretary of Commerce.

TITLE VI—KIDS PRIVACY PROTECTIONS

Subtitle A—COPPA 2.0

SEC. 601. SHORT TITLE.

This subtitle 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.

(a) **DEFINITIONS.**—Section 1302 of the Children’s Online Privacy Protection Act of 1998 (15 U.S.C. 6501) is amended—

(1) by amending paragraph (1) to read as follows:

“(1) **CHILD.**—The term ‘child’ means an individual under the age of 14.”;

(2) by amending paragraph (2) to read as follows:

“(2) **OPERATOR.**—The term ‘operator’—

(A) means any person—

(i) who, for commercial purposes in interstate or foreign commerce, operates or pro-

vides a website on the internet, an online service, an online application, or a mobile application; and

“(ii) who—

“(I) collects or maintains, either directly or through a service provider, personal information from or about the users of that website, service, or application;

“(II) allows another person to collect personal information directly from users of that website, service, or application (in which case, the operator is deemed to have collected the information); or

“(III) allows users of that website, service, or application to publicly disclose personal information (in which case, the operator is deemed to have collected the information); and

“(B) does not include any nonprofit entity that would otherwise be exempt from coverage under section 5 of the Federal Trade Commission Act (15 U.S.C. 45).”;

(3) in paragraph (4)—

(A) by amending subparagraph (A) to read as follows:

“(A) the release of personal information collected from a child or teen by an operator for any purpose, except where the personal information is provided to a person other than an operator who—

“(i) provides support for the internal operations of the website, online service, online application, or mobile application of the operator, excluding any activity relating to individual-specific advertising to children or teens; and

“(ii) does not disclose or use that personal information for any other purpose; and”;

(B) in subparagraph (B)—

(i) by inserting “or teen” after “child” each place the term appears;

(ii) by striking “website or online service” and inserting “website, online service, online application, or mobile application”; and

(iii) by striking “actual knowledge” and inserting “knowledge”;

(4) by amending paragraph (8) to read as follows:

“(8) **PERSONAL INFORMATION.**—

“(A) **IN GENERAL.**—The term ‘personal information’ means individually identifiable information about an individual collected online, including—

“(i) a first and last name;

“(ii) a home or other physical address, including a street name and a name of a city or town;

“(iii) an e-mail address;

“(iv) a telephone number;

“(v) a Social Security number;

“(vi) any other identifier that the Commission determines permits the physical or online contacting of a specific individual;

“(vii) a persistent identifier that can be used to recognize a specific child or teen over time and across different websites, online services, online applications, or mobile applications, that—

“(I) includes—

“(aa) a customer number held in a cookie;

“(bb) an Internet Protocol (IP) address;

“(cc) a processor or device serial number; and

“(dd) a unique device identifier; and

“(II) excludes an identifier that is used by an operator solely for providing support for the internal operations of the website, online service, online application, or mobile application;

“(viii) a photograph, video, or audio file that contains the image or voice of a specific child or teen;

“(ix) geolocation information;

“(x) information generated from the measurement or technological processing of an the biological, physical, or physiological characteristics of an individual that is used to identify an individual, including—

“(I) fingerprints;
 “(II) voice prints;
 “(III) iris or retina imagery scans;
 “(IV) facial templates;
 “(V) deoxyribonucleic acid (DNA) information; and
 “(VI) gait; and

“(xi) information linked or reasonably linkable to a child or teen or a parent of a child or teen (including any unique identifier) that an operator collects online from the child or teen and combines with an identifier described in this subparagraph.

“(B) EXCLUSION.—The term ‘personal information’ does not include an audio file that contains the voice of a child or teen if the operator—

“(i) does not request information via voice that would otherwise be considered personal information under this paragraph;

“(ii) provides clear notice of its collection and use of the audio file and its deletion policy in its privacy policy;

“(iii) only uses the voice contained in the audio file as a replacement for written words to perform a task or otherwise engage with a website, online service, online application, or mobile application, including by performing a search and fulfilling a verbal instruction or request;

“(iv) only maintains the audio file during the period necessary to complete the relevant task or engagement;

“(v) does not make any other use of the audio file during such period; and

“(vi) deletes the audio file at the end of such period.

“(C) SUPPORT FOR THE INTERNAL OPERATIONS OF A WEBSITE, ONLINE SERVICE, ONLINE APPLICATION, OR MOBILE APPLICATION.—

“(i) IN GENERAL.—For purposes of subparagraph (A)(vii), the term ‘support for the internal operations of a website, online service, online application, or mobile application’ means the activities necessary to such website, service, or application to—

“(I) maintain or analyze functioning;
 “(II) perform network communications;
 “(III) authenticate users;
 “(IV) personalize content;
 “(V) serve contextual advertising to users (if any persistent identifier is only used as necessary for technical purposes to serve the contextual advertisement or cap the frequency of contextual advertising);

“(VI) protect the security or integrity of the user, website, online service, online application, or mobile application;

“(VII) ensure legal or regulatory compliance, or

“(VIII) fulfill a request of a child or teen under subparagraph (A), (B), or (C) of section 1303(b)(2).

“(ii) CONDITION.—Except as specifically permitted under clause (i), information collected through the activities described in clause (i) may not be used or disclosed to contact a specific individual (including through individual-specific advertising to children or teens), to amass a profile on a specific individual, in connection with processes that encourage or prompt use of a website or online service, or for any other purpose.”;

(5) by amending paragraph (9) to read as follows:

“(9) VERIFIABLE CONSENT.—The term ‘verifiable consent’ means any reasonable effort (taking into consideration available technology) by an operator, including a request for authorization for future collection, use, and disclosure described in the notice, to ensure that a parent of a child (in the case of a child) or a teen (in the case of a teen)—

“(A) receives direct notice of the collection, use, maintenance, and disclosure practices of the operator with respect to personal information; and

“(B) before the personal information of the child or teen is collected, freely and unambiguously authorizes—

“(i) the collection, use, maintenance, and disclosure, as applicable, of the personal information; and

“(ii) any subsequent use of the personal information.”;

(6) in paragraph (10)—

(A) in the heading, by striking “WEBSITE OR ONLINE SERVICE DIRECTED TO CHILDREN” and inserting “WEBSITE, ONLINE SERVICE, ONLINE APPLICATION, OR MOBILE APPLICATION DIRECTED TO CHILDREN”;

(B) in subparagraph (A)—

(i) in the matter preceding clause (i), by striking “website or online service directed to children” and inserting “website, online service, online application, or mobile application directed to children”;

(ii) in clause (i), by striking “commercial website or online service” and inserting “website, online service, online application, or mobile application”;

(iii) in clause (ii), by striking “commercial website or online service” and inserting “website, online service, online application, or mobile application”;

(C) in subparagraph (B), by striking “commercial website or online service” each place the term appears and inserting “website, online service, online application, or mobile application”;

(D) by adding at the end the following new subparagraph:

“(C) RULE OF CONSTRUCTION.—In considering whether a website, online service, online application, or mobile application, or portion thereof, is directed to children, the Commission shall apply a totality of circumstances test and will also consider competent and reliable empirical evidence regarding audience composition and evidence regarding the intended audience of the website, online service, online application, or mobile application.”;

(7) by adding at the end the following:

“(13) CONNECTED DEVICE.—The term ‘connected device’ means a device that is capable of connecting to the internet, directly or indirectly, or to another connected device.

“(14) ONLINE APPLICATION.—The term ‘online application’—

“(A) means an internet-connected software program; and

“(B) includes a service or application offered via a connected device.

“(15) MOBILE APPLICATION.—The term ‘mobile application’—

“(A) means a software program that runs on the operating system of—

“(i) a cellular telephone;

“(ii) a tablet computer; or

“(iii) a similar portable computing device that transmits data over a wireless connection; and

“(B) includes a service or application offered via a connected device.

“(16) GEOLOCATION INFORMATION.—The term ‘geolocation information’ means information sufficient to identify a street name and name of a city or town.

“(17) TEEN.—The term ‘teen’ means an individual who has attained the age of 14 and is under the age of 18.

“(18) INDIVIDUAL-SPECIFIC ADVERTISING TO CHILDREN OR TEENS.—

“(A) IN GENERAL.—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—

“(i) personal information of—

“(I) the child or teen; or

“(II) a group of children or teens who are similar in sex, age, household income level,

race, or ethnicity to the specific child or teen to whom the product or service is marketed;

“(ii) profiling of such child or teen or group of children or teens; or

“(iii) a unique identifier of such connected device.

“(B) EXCLUSIONS.—The term ‘individual-specific advertising to children or teens’ shall not include—

“(i) advertising or marketing to an individual or to a device of an individual in response to a specific request by the individual for information or feedback, such as a search query by a child or teen;

“(ii) contextual advertising, including if an advertisement is displayed based on the content of the website, online service, online application, mobile application, or connected device on which the advertisement appears and does not vary based on personal information of an individual who views the advertisement;

“(iii) processing personal information solely for measuring or reporting advertising or content performance, reach, or frequency, including independent measurement; or

“(iv) advertising or marketing directed to a connected device used by both adult and child or teen members of a household, if such advertising or marketing is directed to a profile of an adult user.

“(C) RULE OF CONSTRUCTION.—Nothing in subparagraph (A) shall be construed to prohibit an operator with actual knowledge or an operator who should have known that a user is under the age of 18 from delivering advertising or marketing that is age-appropriate and intended for a child or teen audience, if the operator does not use any personal information other than whether the user is under the age of 18.

“(19) EDUCATIONAL AGENCY OR INSTITUTION.—The term ‘educational agency or institution’ means—

“(A) a State educational agency or a local educational agency (as such terms are defined in section 8101 of the Elementary and Secondary Education Act of 1965 (20 U.S.C. 7801)); or

“(B) an institutional day or residential school, including a public school (including a charter school) or a private school, that provides elementary or secondary education, as determined under State law.

“(20) KNOWLEDGE.—The term ‘knowledge’ means the operator has actual knowledge or should have known that a user is a child or teen.”.

(b) ONLINE COLLECTION, USE, DISCLOSURE, AND DELETION OF PERSONAL INFORMATION OF CHILDREN AND TEENS.—Section 1303 of the Children’s Online Privacy Protection Act of 1998 (15 U.S.C. 6502) is amended—

(1) by striking the heading and inserting the following: “ONLINE COLLECTION, USE, DISCLOSURE, AND DELETION OF PERSONAL INFORMATION OF CHILDREN AND TEENS.”;

(2) in subsection (a)—

(A) by amending paragraph (1) to read as follows:

“(1) IN GENERAL.—It is unlawful for an operator of a website, online service, online application, or mobile application directed to children or for any operator of a website, online service, online application, or mobile application with actual knowledge or any operator of a website, online service, online application, or mobile application who should have known that a user is a child or teen to do any of the following:

“(A) Collect personal information from a child or teen in a manner that violates the regulations promulgated under subsection (b).

“(B) Collect, use, disclose to third parties, or maintain personal information of a child

or teen for purposes of individual-specific advertising to children or teens (or to allow another person to collect, use, disclose, or maintain such information for such purpose);

“(C) Otherwise collect the personal information of a child or teen, except if the collection of the personal information is—

“(i) consistent with the context of a particular transaction or service or the relationship of the child or teen with the operator, including any collection necessary to fulfill a transaction or provide a product or service requested by the child or teen; or

“(ii) authorized or required by Federal law (including a regulation promulgated under subsection (b)) or State law.

“(D) Store or transfer 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.

“(E) Retain 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, except as authorized or required by Federal or State law.”; and

(B) in paragraph (2)—

(i) in the heading, by striking “PARENT” and inserting “PARENT OR TEEN”;

(ii) by striking “Notwithstanding paragraph (1)” and inserting “Notwithstanding paragraph (1)(A)”;

(iii) by striking “of such a website or online service”; and

(iv) by striking “subsection (b)(1)(B)(iii) to the parent of a child” and inserting “subsection (b)(1)(B)(iv) to a parent of a child or under subsection (b)(1)(C)(iv) to a teen”;

(3) in subsection (b)—

(A) in paragraph (1)—

(i) in subparagraph (A)—

(I) in the matter preceding clause (i), by striking “the operator of any website” and all that follows through “from a child” and inserting “an operator of a website, online service, online application, or mobile application directed to children or for any operator of a website, online service, online application, or mobile application with actual knowledge or any operator of a website, online service, online application, or mobile application who should have known that a user is a child or teen”;

(II) in clause (i)—

(aa) by striking “notice on the website” and inserting “clear and conspicuous notice on the website, service, or application”;

(bb) by inserting “or teens” after “children”;

(cc) by striking “, and the operator’s disclosure practices” and inserting “, the disclosure practices of the operator”; and

(dd) by striking “; and” and inserting “, the rights and opportunities available to a parent of a child or teen under subparagraphs (B) and (C), and the procedures or mechanisms the operator uses to ensure that personal information is not collected from children or teens (except as permitted by the regulations promulgated under this subsection)”;

(III) in clause (ii)—

(aa) by striking “parental”;

(bb) by inserting “or teens” after “children”;

(cc) by striking the semicolon at the end and inserting “; and”; and

(IV) by inserting after clause (ii) the following new clause:

“(iii) to obtain verifiable consent from a parent of a child (in the case of a child) or from a teen (in the case of a teen) before using or disclosing personal information of the child or teen for any purpose that is a material change from the original purposes and disclosure practices specified to the par-

ent of the child or the teen under clause (i);”;

(ii) in subparagraph (B)—

(I) in the matter preceding clause (i), by striking “that website or online service” and inserting “the operator”;

(II) in clause (i), by striking “that operator” and inserting “the operator, the method by which the operator obtains the personal information, and the purposes for which the operator collects, uses, discloses, and retains the personal information”;

(III) in clause (ii)—

(aa) by inserting “to delete personal information collected from the child or content or information submitted by the child to a website, online service, online application, or mobile application and” after “the opportunity at any time”; and

(bb) by striking “; and” and inserting a semicolon;

(IV) by redesignating clause (iii) as clause (iv) and inserting after clause (ii) the following new clause:

“(iii) the opportunity to challenge the accuracy of the personal information and, if the parent of the child establishes the inaccuracy of the personal information, to have the inaccurate personal information corrected.”; and

(V) in clause (iv), as so redesignated, by inserting “, if such information is available to the operator at the time the parent makes the request” before the semicolon;

(iii) by redesignating subparagraphs (C) and (D) as subparagraphs (D) and (E), respectively;

(iv) by inserting after subparagraph (B) the following new subparagraph:

“(C) require the operator to provide, upon the request of a teen who has provided personal information to the operator, upon proper identification of the teen—

“(i) a description of the specific types of personal information collected from the teen by the operator, the method by which the operator obtained the personal information, and the purposes for which the operator collects, uses, discloses, and retains the personal information;

“(ii) the opportunity at any time to delete personal information collected from the teen or content or information submitted by the teen to a website, online service, online application, or mobile application and to refuse to permit the further use or maintenance in retrievable form, or online collection, of personal information from the teen by the operator;

“(iii) the opportunity to challenge the accuracy of the personal information and, if the teen establishes the inaccuracy of the personal information, to have the inaccurate personal information corrected; and

“(iv) a means that is reasonable under the circumstances for the teen to obtain any personal information collected from the teen, if such information is available to the operator at the time the teen makes the request.”;

(v) in subparagraph (D), as so redesignated—

(I) by striking “a child’s participation” and inserting “the participation of a child or teen”; and

(II) by inserting “or teen” after “the child”; and

(vi) by amending subparagraph (E), as so redesignated, to read as follows:

“(E) require the operator—

“(i) to establish, implement, and maintain reasonable security practices to protect the confidentiality, integrity, and accessibility of personal information of children or teens collected by the operator; and

“(ii) to protect such personal information against unauthorized access.”;

(B) in paragraph (2)—

(i) in the matter preceding subparagraph (A), by striking “verifiable parental consent” and inserting “verifiable consent”;

(ii) in subparagraph (A)—

(I) by inserting “or teen” after “collected from a child”;

(II) by inserting “or teen” after “request from the child”; and

(III) by inserting “or teen or to contact another child or teen” after “to recontact the child”;

(iii) in subparagraph (B)—

(I) by striking “parent or child” and inserting “parent or teen”; and

(II) by striking “parental consent” each place the term appears and inserting “verifiable consent”;

(iv) in subparagraph (C)—

(I) in the matter preceding clause (i), by inserting “or teen” after “child” each place the term appears;

(II) in clause (i)—

(aa) by inserting “or teen” after “child” each place the term appears; and

(bb) by inserting “or teen, as applicable,” after “parent” each place the term appears; and

(III) in clause (ii)—

(aa) by striking “without notice to the parent” and inserting “without notice to the parent or teen, as applicable.”; and

(bb) by inserting “or teen” after “child” each place the term appears; and

(v) in subparagraph (D)—

(I) in the matter preceding clause (i), by inserting “or teen” after “child” each place the term appears;

(II) in clause (ii), by inserting “or teen” after “child”; and

(III) in the flush text following clause (iii)—

(aa) by inserting “or teen, as applicable,” after “parent” each place the term appears; and

(bb) by inserting “or teen” after “child”;

(C) by redesignating paragraph (3) as paragraph (4) and inserting after paragraph (2) the following new paragraph:

“(3) APPLICATION TO OPERATORS ACTING UNDER AGREEMENTS WITH EDUCATIONAL AGENCIES OR INSTITUTIONS.—The regulations may provide that verifiable consent under paragraph (1)(A)(ii) is not required for an operator that acts under a written agreement with an educational agency or institution that, at a minimum, requires the—

“(A) operator to—

“(i) limit the collection, use, and disclosure by the operator of the personal information from a child or teen to solely educational purposes and for no other commercial purposes;

“(ii) provide the educational agency or institution with a notice of the specific types of personal information the operator will collect from the child or teen, the method by which the operator will obtain the personal information, and the purposes for which the operator will collect, use, disclose, and retain the personal information;

“(iii) provide to the educational agency or institution a link regarding the disclosure practices of the operator described in subsection (b)(1)(A)(i); and

“(iv) provide the educational agency or institution, upon request, with a means to review the personal information collected from a child or teen, to prevent further use or maintenance or future collection of personal information from a child or teen, and to delete personal information collected from a child or teen or content or information submitted by a child or teen to website, online service, online application, or mobile application of the operator;

“(B) representative of the educational agency or institution to acknowledge and agree that the representative has authority

to authorize the collection, use, and disclosure of personal information from children or teens on behalf of the educational agency or institution, along with such authorization, the name of the representative, and the title of the representative at the educational agency or institution; and

“(C) educational agency or institution to—

“(i) provide on a website of the educational agency or institution a notice that identifies the operator with which the educational agency or institution has entered into a written agreement under this subsection and provides the link described in subparagraph (A)(iii);

“(ii) upon request, provide the notice described in subparagraph (A)(ii) to a parent (in the case of a child) or a parent or teen (in the case of a teen); and

“(iii) upon the request of such a parent or teen, request the operator provide a means to review the personal information of such a child or teen and provide the parent or teen a means to review the personal information.”;

(D) by amending paragraph (4), as so redesignated, to read as follows:

“(4) TERMINATION OF SERVICE.—The regulations shall permit the operator of a website, online service, online application, or mobile application to terminate service provided to a child for whom a parent has refused or a teen who has refused (under the regulations promulgated under paragraphs (1)(B)(ii) and (1)(C)(ii), respectively) to permit the operator any further use or maintenance, in retrievable form or future online collection, of personal information from the child or teen.”; and

(E) by adding at the end the following new paragraphs:

“(5) CONTINUATION OF SERVICE.—The regulations shall prohibit an operator from discontinuing service provided to a child or teen on the basis of a request by a parent of the child or by the teen (under the regulations promulgated under subparagraph (B) or (C) of paragraph (1), respectively) to delete personal information collected from the child or teen, to the extent that the operator is capable of providing such service without such personal information.

“(6) RULE OF CONSTRUCTION.—A request to delete or correct personal information of a child or teen (under the regulations promulgated under subparagraph (B) or (C) of paragraph (1), respectively) may not be construed to do any of the following:

“(A) Limit the authority of a law enforcement agency to obtain any content or information from an operator pursuant to a lawfully executed warrant or an order of a court of competent jurisdiction.

“(B) Require an operator or third party to delete or correct information that—

“(i) any other provision of Federal or State law requires the operator or third party to maintain; or

“(ii) was submitted to the website, online service, online application, or mobile application of the operator by any person other than the user who is attempting to erase or otherwise eliminate the content or information, including content or information submitted by the user that was republished or resubmitted by another person.

“(C) Prohibit an operator from doing any of the following:

“(i) Retaining a record of the deletion request and the minimum information necessary for the purposes of ensuring compliance with a request made pursuant to subparagraph (B) or (C) of paragraph (1).

“(ii) Preventing, detecting, protecting against, or responding to any security incident, identity theft, or fraud, or reporting a person responsible for any such action.

“(iii) Protecting the integrity or security of a website, online service, online application or mobile application.

“(iv) Ensuring that any such personal information remains deleted.

“(7) COMMON VERIFIABLE CONSENT MECHANISM.—

“(A) IN GENERAL.—

“(i) FEASIBILITY OF MECHANISM.—The Commission, with notice and public comment, shall assess the feasibility of allowing operators the option to use a common verifiable consent mechanism that fully meets the requirements of this title.

“(ii) REQUIREMENTS.—The feasibility assessment required by clause (i) shall consider whether a single operator could use a common verifiable consent mechanism to obtain the verifiable consent required by this title from a parent of a child or from a teen on behalf of multiple listed operators that provide a joint or related service.

“(B) REPORT.—Not later than 1 year after the date of the enactment of this paragraph, the Commission shall submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Energy and Commerce of the House of Representatives a report with the findings of the feasibility assessment required by subparagraph (A)(i).

“(C) REGULATIONS.—If the Commission finds that the use of a common verifiable consent mechanism is feasible and would meet the requirements of this title, the Commission shall issue regulations to permit the use of a common verifiable consent mechanism in accordance with the findings outlined in such report.”; and

(4) in subsection (c), by striking “a regulation prescribed under subsection (a)” and inserting “subparagraph (B), (C), (D), or (E) of subsection (a)(1) or of a regulation promulgated under subsection (b)”.

(c) SAFE HARBORS.—Section 1304 of the Children’s Online Privacy Protection Act of 1998 (15 U.S.C. 6503) is amended—

(1) in subsection (b)(1), by inserting “and teens” after “children”; and

(2) by adding at the end the following:

“(d) PUBLICATION.—

“(1) IN GENERAL.—Except as provided in paragraph (2), the Commission shall publish on the internet website of the Commission any report or documentation required by regulation to be submitted to the Commission to carry out this title.

“(2) RESTRICTIONS ON PUBLICATION.—Notwithstanding the publication requirement described in paragraph (1), the restrictions described in sections 6(f) and section 21 of the Federal Trade Commission Act (15 U.S.C. 46(f); 57b–2) applicable to the disclosure of information obtained by the Commission shall apply in the same manner to any publication under paragraph (1).”.

(d) ACTIONS BY STATES.—Section 1305 of the Children’s Online Privacy Protection Act of 1998 (15 U.S.C. 6504) is amended—

(1) in subsection (a)(1)—

(A) in the matter preceding subparagraph (A), by inserting “section 1303(a)(1) or” before “any regulation”; and

(B) in subparagraph (B), by inserting “section 1303(a)(1) or” before “the regulation”; and

(2) in subsection (d)—

(A) by inserting “section 1303(a)(1) or” before “any regulation”; and

(B) by inserting “section 1303(a)(1) or” before “that regulation”.

(e) ADMINISTRATION AND APPLICABILITY OF ACT.—Section 1306 of the Children’s Online Privacy Protection Act of 1998 (15 U.S.C. 6505) is amended—

(1) in subsection (b)—

(A) in paragraph (1), by striking “, in the case of” and all that follows through “the

Board of Directors of the Federal Deposit Insurance Corporation;” and inserting the following: “by the appropriate Federal banking agency with respect to any insured depository institution (as such terms are defined in section 3 of such Act (12 U.S.C. 1813));”; and

(B) by striking paragraph (2); and

(C) by redesignating paragraphs (3) through (6) as paragraphs (2) through (5), respectively;

(2) in subsection (d)—

(A) by striking “a rule of the Commission under section 1303” and inserting “section 1303(a)(1) or a regulation promulgated under section 1303(b)”; and

(B) by striking “such rule” and inserting “such section or such a regulation”; and

(3) by adding at the end the following new subsections:

“(f) RULE OF CONSTRUCTION ON AGE VERIFICATION.—Nothing in this title may be construed to require an operator to implement an age gating or age verification functionality on a website, online service, online application, or mobile application of the operator.

“(g) ADDITIONAL REQUIREMENT.—Any regulation promulgated under this title shall include a description and analysis of the impact of proposed and final rules on small entities under chapter 6 of title 5, United States Code (commonly known as the ‘Regulatory Flexibility Act’).”.

SEC. 603. STUDY AND REPORTS OF MOBILE AND ONLINE APPLICATION OVERSIGHT AND ENFORCEMENT.

(a) OVERSIGHT REPORT.—Not later than 3 years after the date of the enactment of this subtitle, the Commission shall submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Energy and Commerce of the House of Representatives a report on the processes of platforms that offer mobile and online applications for ensuring that, of those applications that are websites, online services, online applications, or mobile applications directed to children, the applications operate in accordance with—

(1) this subtitle, the amendments made by this subtitle, and regulations promulgated under this subtitle; and

(2) any regulation under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) regarding unfair or deceptive acts or practices with respect to marketing.

(b) ENFORCEMENT REPORT.—Not later than 1 year after the date of the enactment of this subtitle, and annually thereafter, the Commission shall submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Energy and Commerce of the House of Representatives a report that addresses the following:

(1) The number of actions brought by the Commission during the reporting year to enforce the Children’s Online Privacy Protection Act of 1998 (15 U.S.C. 6501 et seq.) (referred to in this subsection as the “Act”) and the outcome of each such action.

(2) The total number of investigations or inquiries into potential violations of the Act during the reporting year.

(3) The total number of open investigations or inquiries into potential violations of the Act as of the date on which the report is submitted.

(4) The number and nature of complaints received by the Commission relating to an allegation of a violation of the Act during the reporting year.

(5) Policy or legislative recommendations to strengthen online protections for children and teens.

SEC. 604. GAO STUDY.

(a) STUDY.—The Comptroller General of the United States shall conduct a study on

the privacy and mental health of teens who use financial technology products that shall do the following:

(1) Identify the type of financial technology products that teens use.

(2) Identify the potential risks to the privacy and mental health of teens that may result from the use of such financial technology products.

(3) Determine whether existing laws are sufficient to address any such risks.

(b) REPORT.—Not later than 1 year after the date of the enactment of this section, the Comptroller General shall submit to Congress a report that details the results of the study conducted under subsection (a) and recommendations for any legislative or administrative action as the Comptroller General determines appropriate.

SEC. 605. SEVERABILITY.

If any provision of this subtitle, or any amendment made by this subtitle, is determined to be unenforceable or invalid, the remaining provisions of and amendments made by this subtitle shall not be affected.

Subtitle B—Data Broker Disclosures

SEC. 611. DEFINITIONS.

In this subtitle:

(1) COVERED DATA BROKER.—

(A) IN GENERAL.—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 brokers 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.

(B) EXCEPTION.—The term “covered data broker” does not include an entity to the extent that the entity does any of the following:

(i) Transmits personal data of an individual, including any communication of such individual, at the request or direction of such individual.

(ii) Provides, maintains, or offers a product or service with respect to which personal data, or access to such data, is not the product or service.

(iii) Reports or publishes news or information that concerns local, national, or international events or other matters of public interest.

(iv) Acts as a service provider.

(2) KNOWS.—The term “knows” means to have actual knowledge or willful disregard.

(3) MINOR.—The term “minor” means an individual under the age of 18 years.

(4) PERSONAL DATA.—The term “personal data” has the meaning given the term “personal information” in section 1302 of the Children’s Online Privacy Protection Act of 1998 (15 U.S.C. 6501) (as amended by section 602(a)(4) of this Act).

(5) SERVICE PROVIDER.—The term “service provider” means an entity that—

(A) collects, processes, or transfers personal data on behalf of and at the direction of—

(i) the minor to whom such information pertains;

(ii) a parent of such a minor;

(iii) a Federal, State, or local government entity; or

(iv) an entity acting as a covered data broker or another service provider; and

(B) receives data from or on behalf of an individual or entity described in subparagraph (A).

SEC. 612. REGISTRATION REQUIREMENT.

(a) DATA BROKER REGISTRATION.—Not later than 12 months after the date of the enactment of this subtitle, and annually thereafter, a covered data broker shall register with the Commission by paying the registra-

tion fee set by the Commission under subsection (c) and by filing a registration statement that includes the following information:

(1) The legal name of the covered data broker.

(2) A contact person and the primary physical address, human-monitored email address, human-monitored 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.

(5) A description of any incident of unauthorized access to personal data that the covered data broker has 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 and, if known, the total number of consumers affected by each previously reported incident of such unauthorized access.

(b) DATA BROKER REGISTRY.—Not later than 18 months after the date of the enactment of this subtitle, the Commission shall establish and maintain on a publicly available website of the Commission a searchable, central registry of covered data brokers registered under subsection (a) that includes—

(1) a search feature that allows members of the public to search for and identify covered data brokers; and

(2) for each covered data broker, the information required by paragraphs (1) through (5) of subsection (a).

(c) ANNUAL REGISTRATION FEE.—The Commission may charge a covered data broker an annual registration fee of at least \$22,500 (as adjusted on January 1 each year by the percentage increase (if any), during the preceding 12-month period, in the Consumer Price Index for All Urban Consumers published by the Bureau of Labor Statistics).

SEC. 613. RULE OF CONSTRUCTION.

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

SEC. 701. ENFORCEMENT.

(a) ENFORCEMENT BY COMMISSION.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of this Act shall be treated as a violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) regarding unfair or deceptive acts or practices.

(2) POWERS OF COMMISSION.—The Commission shall enforce this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act, and any person who violates this Act shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act.

(3) AUTHORITY PRESERVED.—Nothing in this title may be construed to limit the authority of the Commission under any other provision of law.

(b) ACTIONS BY STATES.—

(1) IN GENERAL.—In any case in which the attorney general of a State, or an official or agency of a State, has reason to believe that an interest of the residents of such State has been or is threatened or adversely affected by an act or practice in violation of this Act, the State, as *parens patriae*, may bring a civil action on behalf of the residents of the State in an appropriate district court of the United States to—

(A) enjoin such act or practice;

(B) enforce compliance with this Act;

(C) obtain damages, restitution, or other compensation on behalf of residents of the State; or

(D) obtain such other legal and equitable relief as the court may consider to be appropriate.

(2) NOTICE.—Before filing an action under this subsection, the attorney general, official, or agency of the State involved shall provide to the Commission a written notice of such action and a copy of the complaint for such action. If the attorney general, official, or agency determines that it is not feasible to provide the notice described in this paragraph before the filing of the action, the attorney general, official, or agency shall provide written notice of the action and a copy of the complaint to the Commission immediately upon the filing of the action.

(3) AUTHORITY OF COMMISSION.—

(A) IN GENERAL.—On receiving notice under paragraph (2) of an action under this subsection, the Commission shall have the right—

(i) to intervene in the action;

(ii) upon so intervening—

(I) to be heard on all matters arising therein; and

(II) to file petitions for appeal.

(B) LIMITATION ON STATE ACTION WHILE FEDERAL ACTION IS PENDING.—If the Commission or the Attorney General of the United States has instituted a civil action for violation of this Act (referred to in this subparagraph as the “Federal action”), no State attorney general, official, or agency may bring an action under this subsection during the pendency of the Federal action against any defendant named in the complaint in the Federal action for any violation of this Act alleged in such complaint.

(4) RULE OF CONSTRUCTION.—For purposes of bringing a civil action under this subsection, nothing in this Act may be construed to prevent an attorney general, official, or agency of a State from exercising the powers conferred on the attorney general, official, or agency by the laws of such State to conduct investigations, administer oaths and affirmations, or compel the attendance of witnesses or the production of documentary and other evidence.

SEC. 702. JUDICIAL REVIEW.

The United States 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.

SEC. 703. RULES OF CONSTRUCTION.

Nothing in this Act may be construed to do any of the following:

(1) Allow a governmental entity to enforce this Act based on a viewpoint expressed by or through any speech, expression, or information protected by the First Amendment to the Constitution of the United States.

(2) Prevent—

(A) the taking of reasonable measures to block or filter spam, prevent criminal activity, or protect the security of a platform or service; or

(B) compliance with the duties and reporting requirements set forth in 18 U.S.C. 2258A.

(3) Require the disclosure of the browsing behavior, search history, messages, contact list, or other content or metadata of the communications of a minor.

(4) Limit or impair the Children’s Online Privacy Protection Act of 1998 (15 U.S.C. 6501 et seq.) or any rule or regulation promulgated under such Act.

(5) Expand, limit the scope of, or alter the meaning of section 230 of the Communications Act of 1934 (47 U.S.C. 230).

(6) Restrict the ability to do any of the following:

(A) Cooperate with a law enforcement agency regarding activity reasonably and in good faith believed to violate a Federal, State, or local law, rule, or regulation.

(B) Comply with a lawful civil, criminal, or regulatory inquiry, subpoena, or summons from a Federal, State, local, or other governmental authority.

(C) Investigate, establish, exercise, respond to, or defend against a legal claim.

(D) Prevent, detect, or respond to a security incident, identity theft, fraud, harassment, or any other malicious, deceptive, or illegal activity.

(E) Investigate or report a person responsible for an activity described in subparagraph (D).

(7) Decrypt or ensure an ability to decrypt an encrypted communication of a user.

(8) Preclude the use of any form of encryption, including end-to-end encryption, for any communication of a user.

(9) Require indefinite retention of data of a user.

(10) Require the affirmative collection of any personal information with respect to age that is not already collected in the normal course of business.

SEC. 704. RELATIONSHIP TO STATE LAWS.

(a) IN GENERAL.—The provisions of this Act shall preempt any law, rule, requirement, or regulation of a State, or a political subdivision of a State, only to the extent that such law, rule, requirement, or regulation conflicts with a provision of this Act.

(b) EXCEPTION.—Notwithstanding subsection (a), nothing in this Act may be construed—

(1) to preempt any law, rule, requirement, or regulation of a State, or political subdivision of a State, with respect to contract, tort, or product liability; or

(2) to prohibit a State, or a political subdivision of a State, from enacting or enforcing any law, rule, requirement, or regulation that provides greater protection to minors than the protection provided by the provisions of this Act.

(c) CHILDREN'S ONLINE PRIVACY PROTECTION ACT.—Section 1303 of the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6502) is amended by striking subsection (d) and inserting the following:

“(d) RELATIONSHIP TO STATE LAW.—

“(1) IN GENERAL.—The provisions of this title shall preempt any law, rule, requirement, or regulation of a State, or a political subdivision of a State, only to the extent that such law, rule, requirement, or regulation conflicts with a provision of this title.

“(2) EXCEPTION.—Notwithstanding paragraph (1), nothing in this title may be construed—

“(A) to preempt any law, rule, requirement, or regulation of a State, or political subdivision of a State, with respect to contract, tort, or product liability; or

“(B) to prohibit a State, or a political subdivision of a State, from enacting or enforcing any law, rule, requirement, or regulation that provides greater protection to minors than the protection provided by the provisions of this title.”.

SEC. 705. SEVERABILITY.

If any provision of this Act or the application of this Act to any person or circumstance is held to be unconstitutional, the remaining provisions of this Act and the application of this Act to other persons or circumstances shall not be affected.

SEC. 706. EFFECTIVE DATE.

Except as otherwise provided in this Act, this Act shall take effect on the date that is 1 year after the date of the enactment of this Act.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Kentucky (Mr. GUTHRIE) and the gentleman from New Jersey (Mr. PALLONE) each will control 20 minutes.

The Chair recognizes the gentleman from Kentucky.

GENERAL LEAVE

Mr. GUTHRIE. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days to revise and extend their remarks and include extraneous material on H.R. 7757.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Kentucky?

There was no objection.

Mr. GUTHRIE. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I rise today in strong support of H.R. 7757, the Kids Internet and Digital Safety Act, or the KIDS Act.

This legislation is the most comprehensive, impactful children's online safety package Congress has considered.

I thank Ranking Member PALLONE for his partnership and leadership on this issue. Protecting children should not be a partisan issue, and I appreciate his commitment and working with us to find common ground to address the very real challenges facing families today.

Before I continue, I will recognize two parents who are with us in the gallery today: Deb Schmill, mother of Becca, and Maurine Molak, mother of David. They have experienced every parent's worst nightmare: losing a child because of online harms.

Mr. Speaker, I thank them for their courage in sharing their stories and for turning unimaginable loss into tireless advocacy to help protect other children and families. Their presence here today reminds us of what is at stake, and their voices have helped shape this legislation.

A key part of our approach was negotiating a package of impactful provisions. We worked hard to reach a workable compromise. The KIDS Act incorporates 13 bipartisan Member priorities from across the House to empower parents, protect children's and teens' privacy, and hold Big Tech and online forums accountable.

The bill requires platforms to protect kids by default, including limiting addictive and dangerous design features and risky messaging functions.

It gives parents stronger tools to monitor and manage their children's online experiences, establishes safeguards for AI chatbots, creates new protections in online gaming environments, and requires age verification for pornography websites to ensure kids cannot access explicit content.

The legislation also modernizes children's privacy protections by requiring parental consent before collecting information from children under 14 and extending important new privacy protections to teenagers under 18.

At its core, this legislation sends a simple message: Children deserve a

safer online experience, parents deserve a greater voice in their children's digital lives, and technology companies must be held accountable when they fail to protect young users.

While no single bill will solve every challenge facing families online, this legislation represents a significant and long-overdue step forward in establishing meaningful safeguards. It is an important milestone, not a finish line, in the effort to better protect children online and hold bad actors accountable.

Mr. Speaker, I urge my colleagues to support this bipartisan legislation, and I reserve the balance of my time.

The SPEAKER pro tempore. Members are reminded not to refer to persons in the gallery.

Mr. PALLONE. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I rise today in strong support of the KIDS Act, which is, as my chairman has mentioned, bipartisan legislation to protect kids online and rein in Big Tech. I thank Chairman GUTHRIE for all his work on this.

The internet, social media, and now artificial intelligence have profoundly changed how kids and teens connect with families and friends, how they learn about what is happening around them, and how they participate in an ever-changing online world.

While there have been positive advancements, our kids are also suffering from Big Tech's choke hold on their attention and their relentless pursuit to keep them connected to their platforms. Big Tech is using reckless practices to surveil our kids and teens, exploit vulnerabilities to turn a profit, and promote engagement regardless of the consequences.

For too long, Big Tech has had a free pass while kids and teens face real harm online, including predatory design features, dangerous AI chatbots, and data brokers profiting off of their personal information.

We simply cannot allow this to continue. It is long past time for Congress to step in and pass legislation that protects our kids and teens and reins in Big Tech.

Now, the bipartisan KIDS Act does just that. It is a comprehensive bill that addresses a problem everyone in Congress cares deeply about, and that is keeping kids and teens safe online.

The KIDS Act mandates safeguards, parental tools, and policies across video games and social media platforms, including social gaming platforms like Roblox and chatbots. Platforms are required to limit addictive design features, restrict sharing minors' geolocation data, turn off personalized recommendation systems that drive user engagement, and a lot more.

The KIDS Act also changes the business incentives driving Big Tech's desire to keep kids on their platforms by protecting minors' data and expanding these critical privacy protections from the current age of 12 to teens up to the age of 17.

The bill also bans targeted advertising to kids and teens and ensures

that websites can collect and retain only limited kids' data that is necessary to provide a product or service.

It also requires data brokers that sell minors' data to register with the Federal Trade Commission and pay an annual fee, bringing transparency to a secretive process and a crucial first step toward ending the practice of data brokers selling kids' data.

Mr. Speaker, I can't express enough gratitude to all the parents who have shared their stories and fought for Congress to come together to take action to save other parents from ever experiencing what they went through.

I know there are parents who would like Congress to go even further in the KIDS Act. I will be clear: The KIDS Act is a floor, not a ceiling. The preemption language in the KIDS Act is written with the explicit intent of ensuring that States have the authority to pass and enforce stronger State laws, including those with a duty of care. It is also intended to ensure that ongoing lawsuits against social media companies, chatbot providers, and social gaming companies brought by State attorneys general and attorneys on behalf of parents and kids can continue, including those based on a duty of care and consumer protection laws.

I am proud to lead this legislation alongside Chairman GUTHRIE. For many months now, the Energy and Commerce Committee has been working on legislative solutions to protect our kids and teens online, and this comprehensive, bipartisan bill is the result of those ongoing negotiations. This is an example of the Energy and Commerce Committee at its best.

Mr. Speaker, I am also grateful for the tireless work of Representative CASTOR, a senior committee member, who has been a steadfast champion of the strongest possible protection for kids online.

Mr. Speaker, I urge my colleagues to vote "yes" on the KIDS Act to make the internet a safer place for our kids and teens, and I reserve the balance of my time.

□ 1540

Mr. GUTHRIE. Mr. Speaker, I yield 4 minutes to the gentleman from Florida (Mr. BILIRAKIS), my good friend who is the author and chairman of the subcommittee who has worked tirelessly on this piece of legislation.

Mr. BILIRAKIS. Mr. Speaker, I rise today to speak in strong support of H.R. 7757, the Kids Internet and Digital Safety Act, or the KIDS Act.

This package will finally give parents real tools to protect their kids online. A key provision in the KIDS Act is my Kids Online Safety Act, or KOSA. I have been working on KOSA, Mr. Speaker, for 3 years, and I am proud to see it finally reach the House floor.

The need for action has never been clearer. Nearly half of American teenagers say they are online almost constantly, about half spend 4 or more

hours a day on screens for leisure, and 95 percent have a smartphone in their pocket, placing them in a digital environment that too often prioritizes engagement and profit over safety.

Big Tech platforms are not neutral. Their algorithms are designed to maximize attention, not protect kids.

Mr. Speaker, kids are pushed toward harmful content, targeted by predatory actors, and funneled into design features built to keep them scrolling longer.

Families across the country have paid the price, Mr. Speaker, from exploitation and harassment to content that fuels anxiety, depression, eating disorders, and self-harm, unfortunately. That is why this bill and KOSA, in particular, are so very important.

It establishes clear, targeted obligations for large online platforms to take steps to prevent and mitigate specific harms to minors.

It focuses on addressing documented risks, such as sexual exploitation, drug and alcohol abuse, eating disorders, and self-harm content that can be amplified through algorithmic recommendation systems and engagement-driven design.

KOSA requires platforms to put in place concrete safeguards, limiting harmful design features, improving transparency around how systems impact children, and giving parents strong tools to understand and manage their children's online experiences.

It also ensures Big Tech is held accountable for their decisions through FTC enforcement and State attorneys general.

Mr. Speaker, I thank the chairman of the full committee and the excellent staff. We never gave up. We persevered, and we have a good product, thanks to them.

I thank the ranking member as well, Mr. PALLONE, and Ms. CASTOR, for working with me on this piece of legislation. Again, the chairman gives me credit, but he is responsible as well. The goal is to protect the kids, and I appreciate all the input from the parents over the years.

Mr. Speaker, let's get this across the finish line and protect our children.

Mr. PALLONE. Mr. Speaker, I yield 3 minutes to the gentlewoman from Virginia (Ms. MCCLELLAN), a member of our committee.

Ms. MCCLELLAN. Mr. Speaker, I rise today in support of H.R. 7757, the bipartisan Kids Internet and Digital Safety Act, or the KIDS Act.

As a member of Gen X, who is a mom to a Gen Z teen and Gen Alpha tween, I struggle every day to find the balance between giving our kids the freedom they need to develop and grow and keeping them safe. I see every day that the digital world kids face today is unlike anything previous generations have faced before.

Every day innovators launch new technologies, applications, and online platforms that create incredible opportunities for learning, creativity, and

connection. Those same innovations also create new opportunities for those who would do our kids harm. New risks for invasive data collection, cyberbullying, online exploitation, and harmful content.

It is much harder for parents or other trusted adults today to protect kids from these harms that they often don't see in an ecosystem they often don't understand.

It is past time for Congress to act before more children are put at risk. We are probably 20 years too late. We can't wait anymore.

The KIDS Act closes critical gaps in Federal law by strengthening privacy protections for children and teens; banning targeted advertising to minors; limiting unnecessary data collection, giving parents and teens greater control over personal information; increasing transparency for data brokers; and requiring online platforms to implement stronger default safety tools that reduce harmful interactions. Notably, it preserves every State's ability to go even further.

While this package does not include everything that we would like to see, we cannot let the perfect become the enemy of the good, and this bill is a critical first step.

Our children deserve to enjoy the benefits of technology without sacrificing their privacy, their safety, or mental health.

Mr. Speaker, I thank Ranking Member PALLONE and Chairman GUTHRIE for bringing Democrats and Republicans on the committee together to produce this significant bipartisan legislation at a time when most people believe bipartisanship is dead.

Mr. GUTHRIE. Mr. Speaker, I yield 3 minutes to the gentlewoman from Iowa (Mrs. MILLER-MEEKS), a good friend who is a fantastic member of our committee and has worked hard on these issues protecting children.

Mrs. MILLER-MEEKS. Mr. Speaker, I thank Chairman GUTHRIE, who has done a fabulous job of shepherding this through the Committee on Energy and Commerce in a bipartisan manner.

Protecting children and teens online is one of the most urgent responsibilities we face as policymakers. As digital platforms become central to how young people learn, communicate, innovate, and navigate the world, we must ensure that these spaces are safe, transparent, and designed with their well-being as the driving priority.

My bill, the SPY Kids Act, included in title II of the KIDS Act, takes an important step toward that goal by prohibiting online platforms from conducting market research or product-focused research on children under 13 and by requiring verifiable parental consent before such research can be conducted on teenagers.

The bill applies to user-generated content platforms that use engagement-driven design features and personal data to tailor ads or recommendations, such as social media

companies and social gaming platforms.

This legislation matters because the online environment our kids encounter today is fundamentally different from anything previous generations experienced.

Platforms are engineered to capture attention, collect sensitive information, shape behavior, force content, and it is in ways that young users may not recognize or be able to navigate safely.

Children and teens should not be profiled, studied, or targeted for commercial advantage, especially without parental oversight.

By limiting how platforms can analyze and monetize minors' data, the SPY Kids Act helps reduce the risk of manipulative marketing practices, strengthens privacy protections, and reinforces the principle that the well-being of America's youth must come before the business models of technology companies.

Our goal is simple: to build an online ecosystem where children can grow, learn, innovate, and connect without being exploited in the process.

Mr. Speaker, I urge my colleagues to vote "yes" on the bill.

Mr. PALLONE. Mr. Speaker, I yield 3 minutes to the gentlewoman from Massachusetts (Mrs. TRAHAN), a member of our committee.

Mrs. TRAHAN. Mr. Speaker, I thank the ranking member for yielding and for his strong leadership on this vitally important issue.

When I joined the Energy and Commerce Committee 6 years ago, I committed to doing everything in my power to make the internet a safer place for my children, my two young daughters, specifically.

In the years since, I have sat in hearing after hearing where we have talked about doing something to deliver on that promise.

I met with parents who have lived every family's worst nightmare, parents whose children harmed themselves and even ended their lives because executives in Silicon Valley cared more about their stock price than the safety of our children.

I looked those parents in the eye. I cried with them as they told their story. Then I went home to have hard conversations with my two girls about how the apps they use, Instagram, TikTok, and others, are engineered to make them doubt their image and question their worth.

For years, this crisis has gone unanswered, decades at this point. Our children have been left to navigate one of the most powerful and manipulative technologies ever built, and they have been left to do it alone.

□ 1550

This bill ends that.

To be clear, Mr. Speaker, the KIDS Act doesn't solve every problem, but it makes one heck of a dent. It finally gives kids and teens overdue privacy protections. It forces platforms to turn

on safeguards by default instead of burying them where no parent can find them. It puts tools in the hands of moms and dads, and it makes companies answer for the worst harms that they allow on their platforms.

Is it everything I want? No. I have heard from parents and advocates who believe we should go further, and they are right that this fight isn't over. We can and we must continue to build upon this progress, but I refuse to tell families to wait for a better political moment or for a perfect bill that may never come when meaningful protections are in front of us right now.

Critically, these are protections built to last, not ones written to be struck down in court on the day they take effect.

I thank Ranking Member PALLONE for his commitment to these negotiations, and I acknowledge the work of leaders on the committee on this issue, including Congresswoman KATHY CASTOR and Congresswoman YVETTE CLARKE.

Today, we pass the KIDS Act. Tomorrow, we keep fighting for safer digital spaces for every child, especially with the rise of artificial intelligence.

Mr. Speaker, I urge my colleagues to vote "yes."

Mr. GUTHRIE. Mr. Speaker, I yield 3 minutes to the gentlewoman from Florida (Ms. LEE), who not only is a great committee member on our committee, but is also one of the judicial minds on our committee who is a great legal scholar.

Ms. LEE of Florida. Mr. Speaker, I rise today in support of H.R. 7757, the Kids Internet and Digital Safety Act, or the KIDS Act.

Children today are growing up in a digital world that looks dramatically different than it did just a generation ago.

While technology has created tremendous opportunities to learn and to connect, it has also exposed young people to online predators, sexual exploitation, privacy violations, and increasingly sophisticated threats driven by artificial intelligence.

Parents are doing everything they can to protect their children online but should not have to navigate these challenges alone.

This legislation includes two bipartisan bills that I have been honored to lead. The first is the Promoting a Safer Internet for Minors Act.

I thank the gentleman from Florida (Mr. SOTO), my colleague and fellow Floridian, for his support and partnership on this legislation.

This bill recognizes that education is one of the strongest tools we have to protect children before they become victims.

It directs the Federal Trade Commission to establish a nationwide public awareness campaign that equips parents, educators, and communities with practical, up-to-date guidance on helping children navigate the internet safely and responsibly.

The second is COPPA 2.0, which I am proud to lead along with Congressman TIM WALBERG.

When Congress enacted the Children's Online Privacy Protection Act nearly three decades ago, social media did not exist, and online platforms were not collecting massive amounts of personal information to build user profiles and deliver targeted advertising.

This bill brings our privacy laws into the modern era by extending important protections to teenagers, limiting unnecessary data collection, prohibiting targeted advertising to children and to teens, creating clear expectations for tech platforms, and giving families greater control over their personal information.

Together, these provisions reflect a simple principle: Protecting children online requires both empowering families with the information they need and ensuring that online platforms handle children's personal information responsibly.

Technology will continue to evolve, and our laws must evolve with it.

I am grateful to Chairman GUTHRIE, Subcommittee Chairman BILIRAKIS, and my colleagues on the committee for their partnership in advancing this legislation. I urge all of my colleagues to support the KIDS Act.

Mr. PALLONE. Mr. Speaker, I yield 3 minutes to the gentlewoman from Washington (Ms. SCHRIER), who is another member of our committee.

Ms. SCHRIER. Mr. Speaker, as a mom, a pediatrician, and a Member of Congress, I rise today to support the advancement of the KIDS Act to take some serious steps to protect our kids and their data online and hold Big Tech accountable.

The KIDS Act includes my bill, the Kids Online Safety Act, which will ensure that social media companies provide protections and guardrails for kids online and are held accountable for the many harms they are causing to our kids, from sleeplessness, to eating disorders, to self-harm, and even harm from others.

Social media companies have gone largely unregulated for decades, all while they have become an omnipresent and bigger and bigger part of everyday life, including for kids.

In my 20 years as a pediatrician, I have seen the rise of mental and behavioral health concerns for kids and teens coincide directly with the rise of screen time and social media.

It is long past time to hold Big Tech and social media accountable.

This package includes many useful tools for parents to keep their kids safe online, but parents can't do it alone. This package isn't perfect, and I wish to see even more come out of negotiations with the Senate. That is why I am continuing to call for a duty of care and language that goes further to hold social media companies accountable for the many harms that their platforms are causing, including serious mental health issues, like anxiety, depression, addiction, eating disorders, and suicidality.

But this package represents the first time in decades that we have had a chance in the House to take a step forward, to finally passing comprehensive legislation to protect our kids. I strongly urge my colleagues to support it today so we can make it even stronger.

Mr. GUTHRIE. Mr. Speaker, I yield 5 minutes to the gentlewoman from Illinois (Mrs. MILLER), my good friend who has worked really hard to be an important part of this package.

Mrs. MILLER of Illinois. Mr. Speaker, I thank Chairman GUTHRIE for his important leadership.

Mr. Speaker, the statistics are alarming. The average age of a child's first exposure to pornography is just 12 years old, and nearly 80 percent of America's children between 12 and 17 have already been exposed to it.

Not only has the sexual content become intentionally easier to access, but it has also become increasingly violent, abusive, normalizing sexual assault, physical violence, and non-consensual acts for young, impressionable minds. The consequences are devastating.

Research has linked early exposure to pornography with anxiety, addiction, depression, low self-esteem, body image disorders, and an increased likelihood that minors will engage in risky and harmful sexual behavior.

States across America have recognized this crisis. More than a dozen have declared children's exposure to pornography a public health crisis, and more than two dozen States have enacted age verification requirements for adult websites.

Last year, the Supreme Court upheld Texas' age verification law. The court ruled that the burden placed on adults to verify one's age is incidental when the intent is to protect the innocence of the children.

For that reason, I am grateful that Chairman GUTHRIE included the SCREEN Act in this legislative package.

Senator MIKE LEE and I drafted this legislation to establish age verification requirements for adult websites, creating a minimum requirement that every State must meet while allowing flexibility to enact stronger protections for children.

I am a strong supporter of the First Amendment, but constitutional law has long recognized that its protections do not extend to obscenity.

Our laws already require age verification to purchase alcohol, tobacco, firearms, or to enter a casino.

□ 1600

We recognize that some products and activities are simply inappropriate for children. Pornography should be no different. The SCREEN Act is one of the most consequential bills to protect children in the digital age.

Today, we have an opportunity to make the internet safer for the next generation, and I urge all my colleagues to support this legislation.

I thank Chairman GUTHRIE for including my bill in this package.

Mr. PALLONE. Mr. Speaker, I yield 4 minutes to the gentlewoman from Florida (Ms. CASTOR), another member of our committee who also happens to be the ranking member of our Energy Subcommittee and has been very much involved with this issue and the KIDS Act from the very beginning.

Ms. CASTOR of Florida. Mr. Speaker, I thank the ranking member for yielding me time.

Mr. Speaker, this is a very important step forward to protect our kids online. I really arrived here more as a parent than a Member of Congress, watching two daughters grow up at a time when the internet and social media was evolving, and I just understood from a very personal level what was happening.

Being here in Congress, listening to parents whose children had suffered online harms, whether that was suicide or cyberbullying, the evidence really is overwhelming now about the online risks and the physical and mental harms suffered by kids.

Over 40 percent of kids under 12 are exposed to inappropriate material within their first month on social media: cyberbullying and violent and graphic content.

Excessive screen time is linked to significantly higher rates of anxiety and depression among teens. Those spending 4 or more hours online daily are more than twice as likely to report symptoms of both.

My colleagues on the Energy and Commerce Committee and I have spent many Congresses—a number of Congresses—working with advocacy groups and parents about the best way to combat the harms experienced by young people online.

The underlying record is replete with evidence from psychologists, pediatricians, and teachers about the impact that Big Tech has on our kids. I have submitted their stories, reports, and research for the RECORD as we update the Children's Online Privacy Protection Act, a law that is outdated, that now will cover teens and provide much greater safety and privacy for young people.

Mr. Speaker, I include in the RECORD all of these stories and everything by reference here today. This includes the testimonies, coalition letters, and advisory from the Surgeon General, all showing that compulsive social media use is harmful to the health of our kids. The documents can be found at the following links: Anxious Generation: The Evidence (2026) <https://www.anxiousgeneration.com/research/the-evidence>; Master Complaint in Meta Lawsuit (2025) <https://www.motleyrice.com/sites/default/files/documents/Less-Redacted-Omnibus-Opinion-Brief.pdf>; Pew Research Center Report: Teens, Social Media and Mental Health (2025) <https://www.pewresearch.org/wp-content/uploads/sites/20/2025/04/>

PI_2025.04.22_teens-social-media-mental-health_REPORT.pdf; Fairplay: Teen Accounts: Broken Promises, How Instagram is Failing to Protect Minors (2025) <https://fairplayforkids.org/wp-content/uploads/2025/09/Teen-Accounts-Broken-Promises-How-Instagram-is-failing-to-protect-minors.pdf>; FTC Report: A Look Behind the Screens, Examining the Data Practices of Social Media and Video Streaming Services (2024); https://www.ftc.gov/system/files/ftc_gov/pdf/Social-Media-6b-Report-9-911-2024.pdf; U.S. Surgeon General's Advisory on Social Media and Youth Mental Health (2023) https://www.ncbi.nlm.nih.gov/books/NBK594761/pdf/Bookshelf_NBK594761.pdf; American Psychological Association: Health Advisory on Social Media Use in Adolescence (2023) <https://www.apa.org/topics/social-media-internet/health-advisory-adolescent-social-media-use.pdf>

As digital threats evolve, so must our laws. The bipartisan KIDS Act before us today responds to these realities with strong, commonsense safeguards.

This has been a long time coming, and I really thank Chairman GUTHRIE for bringing it in for a landing. My good friend, Chairman GUS BILIRAKIS, and I have worked on KOSA. I appreciate the support from my allies on privacy, Representative WALBERG and now Representative LEE who came on this Congress.

I appreciate the work of Ranking Member PALLONE, Representative TRAHAN, and the professional staff who really listened to the parents. I know it is not the be all-end all, and they have my commitment to keep pressing for the strongest privacy protections and design code protections.

I hope the Senate adopts a very strong bill. It is there. The ball is going to be in their court now after the House passes the KIDS Act today, but this is an important step for kids, parents, and families in America. How do we keep up with the technological innovations? How do we keep up with what Big Tech wants to do to monetize children's time online? They deserve the protections here today. They deserve this strong step forward, and I again thank my colleagues and urge a strong "yes" vote.

Mr. GUTHRIE. Mr. Speaker, I have no further speakers, and I reserve the balance of my time.

Mr. PALLONE. Mr. Speaker, I yield myself the balance of my time.

Mr. Speaker, I want everyone to understand that this KIDS Act mandates safeguards, parental tools, and policies to keep kids safe across the internet, from social media to video games to chatbots.

Secondly, the bill adds data minimization language, and this is so important. It minimizes the amount of data that can be collected. This is to prevent excessive data collection for kids and teens, provides rights to delete access and correct data to teens

and parents of children, and bans targeted advertising to kids and teens.

This bill reflects months of bipartisan negotiation between myself and Energy and Commerce Committee Chairman GUTHRIE, Mr. BILIRAKIS, and Ms. CASTOR to arrive at a package of bills that will provide meaningful baseline protections for kids online without stopping further progress in the States. We do not preempt the States from taking further action.

Mr. Speaker, I strongly believe this bill provides a path to passage here in the House and also in the Senate.

I ask Members on a bipartisan basis to support the bill, and I yield back the balance of my time.

Mr. GUTHRIE. Mr. Speaker, I yield myself the balance of my time.

Mr. Speaker, I thank the ranking member for those data protections. That has been very important and a big part of the negotiations, and the gentleman has been a great advocate for that. I really appreciate it.

I mentioned Ms. Schmill and Ms. Molak when we first started. I should mention the staff and their hard work. They had countless hours meeting with different groups. Members were meeting with different groups and working hard on this, but the staff has, as well.

When I first took the chairmanship, very early in my chairmanship when my colleagues asked me to chair this committee, we sat down with a group of people to determine our priorities.

Number one was this bill. Number one was this effort. Number one was this issue. People talk a lot of times about how we have so many young staffers on Capitol Hill. They are, and they are also young parents. I have seen from both sides of the aisle, a couple of our staff members have different opinions on other issues but sit down and put that all aside when it comes to their children, America's children.

Mr. Speaker, I really appreciate the hard, hard work. I really encourage my colleagues to vote for this bill tonight. I really encourage my colleagues to vote for this bill tonight because when we vote for this bill tonight, the House will put its imprint—and we have worked with the Senate, but the House will put its imprint to make sure that children are protected, parents are empowered, and Big Tech is held accountable.

Mr. Speaker, I yield back the balance of my time.

The SPEAKER pro tempore (Mr. MORAN). The question is on the motion offered by the gentleman from Kentucky (Mr. GUTHRIE) that the House suspend the rules and pass the bill, H.R. 7757, as amended.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds being in the affirmative, the yeas have it.

Mr. GUTHRIE. Mr. Speaker, on that I demand the yeas and nays.

The yeas and nays were ordered.

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX, further pro-

ceedings on this motion will be postponed.

SECURING COMMUNITY UPGRADES FOR A RESILIENT GRID ACT

Mr. GUTHRIE. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 7257) to amend the Energy Policy and Conservation Act to require States to include supporting the physical security, cybersecurity, and resilience of local distribution systems in State energy security plans, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 7257

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Securing Community Upgrades for a Resilient Grid Act" or the "SECURE Grid Act".

SEC. 2. CONSIDERATION OF THE SECURITY OF LOCAL DISTRIBUTION SYSTEMS IN STATE ENERGY SECURITY PLANS.

Section 366 of the Energy Policy and Conservation Act (42 U.S.C. 6326) is amended—

(1) in subsection (a), by adding at the end the following:

"(3) LOCAL DISTRIBUTION SYSTEM.—The term 'local distribution system' means any energy infrastructure owned and operated by an electric utility at a voltage of 100 kilovolts or less.;"

(2) in subsection (b)(2), by inserting " and suppliers of equipment for the generation, transmission, and distribution of electricity to," after "owners and operators of";

(3) in subsection (c)—

(A) by amending paragraph (3) to read as follows:

"(3) address potential hazards to each energy sector or system, including—

"(A) physical threats and vulnerabilities, including—

"(i) weather-related threats and vulnerabilities;

"(ii) physical attacks on local distribution systems and the bulk-power system; and

"(iii) supply chain risks for equipment for the generation, transmission, and distribution of electricity; and

"(B) cybersecurity threats and vulnerabilities, including threats to, and vulnerabilities of, local distribution systems that may impact the bulk-power system.;" and

(B) by amending paragraph (5) to read as follows:

"(5) provide a risk mitigation approach to enhance reliability and end-use resilience, including methods of responding to, mitigating, and recovering from potential hazards described in paragraph (3); and"

(4) in subsection (d)(3)—

(A) in subparagraph (A), by striking "and" at the end;

(B) by redesignating subparagraph (B) as subparagraph (C); and

(C) by inserting after subparagraph (A) the following:

"(B) supplying equipment for the generation, transmission, and distribution of electricity; and"

(5) in subsection (e)—

(A) by striking "A State is not eligible" and inserting the following:

"(1) SUBMISSION REQUIRED.—A State is not eligible";

(B) in paragraph (2), by redesignating subparagraphs (A) and (B) as clauses (i) and (ii), respectively;

(C) by redesignating paragraphs (1) and (2) as subparagraphs (A) and (B), respectively (and by moving the margins accordingly); and

(D) by adding at the end the following:

"(2) STATE DETERMINATION.—A submission under paragraph (1) is not required to be approved by the Secretary.;"

(6) in subsection (f), by striking "may" and inserting "shall";

(7) in subsection (h), by inserting " local distribution system," after "electric utility"; and

(8) by striking subsection (i) and inserting the following:

"(i) SUNSET.—This section shall expire on September 30, 2031."

SEC. 3. GAO REPORT.

(a) IN GENERAL.—Not later than September 30, 2030, the Comptroller General shall submit to the Committee on Energy and Commerce of the House of Representatives and the Committee on Energy and Natural Resources of the Senate a report on the efficacy of State energy security plans that includes—

(1) an evaluation of whether and how State energy security plans have improved the ability of States to identify, assess, and mitigate risks to energy infrastructure and supply chains and to plan for, respond to, and recover from events that disrupt energy supply;

(2) recommendations for—

(A) improving the ability of States described in paragraph (1); and

(B) actions the Secretary of Energy may take to improve coordination with States with respect to identifying, assessing, and mitigating risks to energy infrastructure and supply chains and planning for, responding to, and recovering from events that disrupt energy supply;

(3) information on Federal financial assistance made available to States under part D of title III of the Energy Policy and Conservation Act (42 U.S.C. 6321 et seq.) that was used to implement State energy security plans;

(4) information on activities carried out by States using such financial assistance;

(5) an analysis of the efficacy of the implementation of section 366 of the Energy Policy and Conservation Act (42 U.S.C. 6326), as amended by this Act; and

(6) information on State use of assistance provided under section 366(f) of the Energy Policy and Conservation Act (42 U.S.C. 6326(f)) (as amended by this Act), including any revisions of State energy security plans made by States resulting from assistance provided under such section 366(f).

(b) PROTECTED INFORMATION.—The report required under subsection (a) shall be submitted in a form that may be made available to the public, except that any information protected from disclosure under section 366(h) of the Energy Policy and Conservation Act (42 U.S.C. 6326(h)) shall be included in the report in an annex that shall not be publicly disclosed, consistent with such section.

(c) STATE ENERGY SECURITY PLAN DEFINED.—In this section, the term "State energy security plan" has the meaning given such term in section 366(a) of the Energy Policy and Conservation Act (42 U.S.C. 6326(a)).

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Kentucky (Mr. GUTHRIE) and the gentleman from New Jersey (Mr. PALLONE) each will control 20 minutes.

The Chair recognizes the gentleman from Kentucky.

GENERAL LEAVE

Mr. GUTHRIE. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days to revise and extend their remarks and include extraneous material on H.R. 7257.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Kentucky?

There was no objection.

Mr. GUTHRIE. Mr. Speaker, I yield myself such time as I may consume.