

Title: To protect the safety of children on the internet.

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 Online Safety 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.

Sec.3.Duty of care.

Sec.4.Safeguards for minors.

Sec.5.Disclosure.

Sec.6.Transparency.

Sec.7.Independent research.

Sec.8.Market research.

Sec.9.Age verification study and report.

Sec.10.Guidance.

Sec.11.Enforcement.

Sec.12.Kids online safety council.

Sec.13.Effective date.

Sec.14.Relationship to other laws.

Sec.15.Severability.

SEC. 2. DEFINITIONS.

In this Act:

(1) ALGORITHMIC RECOMMENDATION SYSTEM.—The term “algorithmic recommendation system” means a fully or partially automated system used to suggest, promote, or rank information.

(2) CHILD.—The term “child” means an individual who is age 12 or younger.

(3) COVERED PLATFORM.—The term “covered platform” means a social media service, social network, video game, messaging application, video streaming service, educational service, or an online platform that connects to the internet and that is used, or is reasonably likely to be used, by a minor.

(4) MENTAL HEALTH DISORDER.—The term “mental health disorder” has the meaning given such term in the Diagnostic and Statistical Manual of Mental Health Disorders, 5th

Edition (or a successor edition).

(5) MINOR.—The term “minor” means an individual who is age 16 or younger.

(6) ONLINE PLATFORM.—The term “online platform” means any public-facing website, online service, online application, or mobile application that primarily provides a community forum for user generated content, including sharing videos, images, games, audio files, or other content.

(7) PARENT.—The term “parent” includes a legal guardian or an individual with legal custody over a minor.

(8) PERSONAL DATA.—The term “personal data” means information that identifies or is linked or reasonably linkable to an individual, household, or consumer device.

(9) COMPULSIVE USAGE.—The term “compulsive usage” means any response stimulated by external factors that causes an individual to engage in repetitive behavior reasonably likely to cause psychological distress, loss of control, anxiety, depression, or harmful stress responses.

SEC. 3. DUTY OF CARE.

(a) BEST INTERESTS.—A covered platform shall act in the best interests of a minor that uses the platform’s products or services, as described in subsection (b).

(b) PREVENTION OF HARM TO MINORS.—In acting in the best interests of minors, a covered platform shall take reasonable measures in its design and operation of products and services to prevent and mitigate—

- (1) mental health disorders or associated behaviors, including the promotion or exacerbation of self-harm, suicide, eating disorders, and substance use disorders;
- (2) patterns of use that indicate or encourage addiction-like behaviors;
- (3) physical violence, online bullying, and harassment of a minor;
- (4) sexual exploitation, including enticement, grooming, sex trafficking, and sexual abuse of minors and trafficking of online child sexual abuse material;
- (5) promotion and marketing of narcotic drugs (as defined in section 102 of the Controlled Substances Act (21 U.S.C. 802)), tobacco products, gambling, or alcohol; and
- (6) predatory, unfair, or deceptive marketing practices, or other financial harms.

SEC. 4. SAFEGUARDS FOR MINORS.

(a) SAFEGUARDS FOR MINORS.—

(1) IN GENERAL.—A covered platform shall provide a minor with readily-accessible and easy-to-use safeguards to, as applicable—

(A) limit the ability of other individuals to contact or find a minor, in particular individuals aged 17 or over with no relationship to the minor;

(B) prevent other users, whether registered or not, from viewing the minor’s personal data collected by or shared on the covered platform in particular restricting

public access to personal data

(C) limit features that increase sustain or extend use of the covered platform by a minor, such as automatic playing of media, rewards for time spent on the platform, notifications, and other features that result in compulsive usage of the covered platform by a minor;

(D) control algorithmic recommendation systems that use a minor's personal data, including the right to—

(i) opt out of such algorithmic recommendation systems; or

(ii) limit types or categories of recommendations from such systems;

(E) delete the minor's account and delete their personal data;

(F) restrict the sharing of the geolocation of a minor and provide notice regarding the tracking of a minor's geolocation; and

(G) limit the amount of time spent by a minor on the covered platform.

(2) **DEFAULT SAFEGUARD SETTINGS FOR MINORS.**—A covered platform shall provide that, in the case of a user that the platform knows or reasonably believes to be a minor, the default setting for any safeguard described under paragraph (1) shall be the option available on the platform that provides the most protective level of control that is offered by the platform over privacy and safety for that user.

(b) **PARENTAL TOOLS.**—

(1) **TOOLS.**—A covered platform shall provide readily-accessible and easy-to-use tools for parents to supervise the use of the covered platform by a minor.

(2) **REQUIREMENTS.**—The tools provided by a covered platform shall include—

(A) the ability to control privacy and account settings, including the safeguards established under subsection (a)(1);

(B) the ability to restrict purchases and financial transactions by a minor, where applicable;

(C) the ability to track metrics of total time spent on the platform; and

(D) control options that allow parents to address the harms described in section 3(b).

(3) **NOTICE TO MINORS.**—A covered platform shall provide clear and conspicuous notice to a minor when tools described in this subsection are in effect.

(4) **DEFAULT TOOLS.**—A covered platform shall provide that, in the case of a user that the platform knows or reasonably believes to be a child, the tools described in this subsection shall be enabled by default.

(c) **Reporting Mechanism.**—

(1) **REPORTS SUBMITTED BY PARENTS, MINORS, AND SCHOOLS.**—A covered platform shall provide—

(A) a readily-accessible and easy-to-use means to submit reports to the covered platform of harms to minors;

- (B) an electronic point of contact specific to matters involving harms to a minor; and
- (C) confirmation of the receipt of such a report and a means to track a submitted report.

(2) **TIMING.**—A covered platform shall establish an internal process to receive and substantively respond to reports in a reasonable and timely manner, but in no case later than 14 days after the receipt of a report.

(d) **ADVERTISING ILLEGAL PRODUCTS.**—A covered platform shall not facilitate the advertising of narcotic drugs (as defined in section 102 of the Controlled Substances Act (21 U.S.C. 802)), tobacco products, gambling, or alcohol to minors.

(e) **Application.**—

(1) **ACCESSIBILITY.**—With respect to safeguards and parental controls described under subsections (a) and (b), a covered platform shall provide—

(A) information and control options in a clear and conspicuous manner that takes into consideration the differing ages, capacities, and developmental needs of the minors most likely to access the covered platform and does not encourage minors or parents to weaken or disable safeguards or parental controls;

(B) readily-accessible and easy-to-use controls to enable or disable safeguards or parental controls, as appropriate; and

(C) information and control options in the same language, form, and manner as the covered platform provides any product or service used by minors.

(2) **DARK PATTERNS PROHIBITION.**—For purposes of this section, it shall be unlawful for any covered platform to design, modify, or manipulate a user interface of a covered platform with the purpose or substantial effect of subverting or impairing user autonomy, decision-making, or choice in order to weaken or disable safeguards or parental controls.

(3) **RULES OF CONSTRUCTION.**—Nothing in this section shall be construed to—

(A) prevent a covered platform from—

(i) taking reasonable measures to limit algorithmic recommendation systems from distributing unlawful, obscene, or harmful material to minors as described in section 3(b); or

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

(B) require the disclosure of a minor’s browsing behavior, search history, messages, or other content of their communications; or

(C) restrict a covered platform’s ability to—

(i) cooperate with law enforcement agencies regarding activity that the operator reasonably and in good faith believes may violate Federal, State, or local laws, rules, or regulations;

(ii) comply with a civil, criminal, or regulatory inquiry or any investigation, subpoena, or summons by Federal, State, local, or other government authorities; or

(iii) exercise, respond to, or defend against legal claims.

SEC. 5. DISCLOSURE.

(a) Notice.—

(1) REGISTRATION.—Prior to registration, use, or purchase of a covered platform by a minor, the platform shall provide clear, conspicuous, and easy-to-understand—

(A) notice of the policies and practices of the covered platform with respect to personal data and safeguards for minors;

(B) information about how to access the safeguards and parental tools required under section 4; and

(C) notice about whether the covered platform, including any algorithmic recommendation systems used by the platform, pose any heightened risks of harms to minors.

(2) PARENTAL NOTIFICATION.—For a minor, or an individual that a covered platform reasonably believes is a minor, a covered platform shall additionally provide the notice, information, and statement described in paragraph (1) to a parent of the minor.

(3) ACKNOWLEDGMENT.—After providing the notice, information, and statement described in paragraph (1), but prior to initial use of the covered platform, the covered platform shall take reasonable steps to obtain express affirmative acknowledgment from a parent of the minor of the receipt of information related to the heightened risks of harm to minors referenced in the statement in paragraph (1)(C).

(4) RULEMAKING.—The Commission may issue rules pursuant to section 553 of title 5, United States Code, to establish standards for covered platforms to comply with this subsection, including—

(A) a minimum level of information covered platforms must provide pursuant to paragraph (1), where applicable; and

(B) processes for parental notification, which may include templates or models of short-form notices.

(b) Algorithmic Recommendation System.—A covered platform that operates algorithmic recommendation systems that use minors' personal data shall set out in its terms and conditions, in a clear, conspicuous, and easy-to-understand manner—

(1) an overview of how those algorithmic recommendation systems are used by the covered platform to provide information to users of the platform who are minors, including how such systems use the personal data of minors; and

(2) information about options for minors or their parents to control algorithmic recommendation systems that use a minor's personal data (including by opting out of such systems).

(c) ADVERTISING AND MARKETING INFORMATION AND LABELS.—

(1) INFORMATION AND LABELS.—A covered platform that facilitates advertising aimed at minors shall provide clear, conspicuous, and easy-to-understand information and labels on

advertisements and marketing material regarding—

(A) the name of the product, service, or brand and the subject matter of an advertisement or marketing material;

(B) why the minor is being targeted for a particular advertisement or marketing material if the covered platform engages in targeted advertising, including material information about how the minor's personal data was used to target the advertisement or marketing material; and

(C) whether particular media displayed to a user is an advertisement or marketing material, including disclosure of endorsements of products, services, or brands made for commercial consideration by other users of the platform.

(2) Rulemaking.—The Commission may issue rules pursuant to section 553 of title 5, United States Code, to implement this subsection, specifically establishing the minimum level of information and labels necessary for the disclosures required under paragraph (1), which may include templates or models of short-form notices.

(d) RESOURCES IN ADDITIONAL LANGUAGES.—A covered platform shall, to the extent practicable, that the disclosures required by this section are made available in the same language, form, and manner as the covered platform provides any product or service used by minors.

SEC. 6. TRANSPARENCY.

(a) IN GENERAL.—Subject to subsection (b), not less frequently than once a year, a covered platform shall issue a public report identifying the reasonably foreseeable risk of harms to minors and describing the prevention and mitigation measures taken to address such risk based on an independent, third-party audit conducted through reasonable inspection of the covered platform.

(b) Scope of Application.—The requirements of this section shall not apply to a covered platform if, for the most recent calendar year, the platform averaged less than 10,000,000 active users on a monthly basis in the United States.

(c) Content.—

(1) TRANSPARENCY.—The public reports required of a covered platform under this section shall include—

(A) an assessment of the extent to which the platform is likely to be accessed by minors;

(B) a description of the commercial interests of the covered platform in use by minors;

(C) an accounting of the number of individuals using the covered platform reasonably believed to be minors in the United States, disaggregated by the age ranges of 0-5, 6-9, 10-12, and 13-16;

(D) an accounting of the median and mean amounts of time spent on the platform by minors in the United States who have accessed the platform during the reporting year on a daily, weekly, and monthly basis, disaggregated by the age ranges of 0-5, 6-9, 10-12, and 13-16;

(E) an accounting of total reports received regarding, and the prevalence of content related to, the harms described in section 3(b), disaggregated by category of harm, as described in section 3(b), of—

(i) the total number of reports of the dissemination of illegal or harmful content involving minors; and

(ii) the prevalence of content that is illegal or harmful to minors; and

(F) a description of any material breaches of parental tools or assurances regarding minors, representations regarding the use of the personal data of minors, and other matters regarding non-compliance.

(2) SYSTEMIC RISKS ASSESSMENT.—The public reports required of a covered platform under this section shall include—

(A) an audit of the reasonably foreseeable risk of harms to minors posed by the covered platform, including identifying any other physical, mental, developmental, or financial harms in addition to those described in section 3(b);

(B) an assessment of how algorithmic recommendation systems and targeted advertising systems can contribute to harms to minors;

(C) a description of whether and how the covered platform uses system design features to increase, sustain, or extend use of a product or service by a minor, such as automatic playing of media, rewards for time spent, and notifications;

(D) a description of whether, how, and for what purpose the platform collects or processes categories of personal data that may cause reasonably foreseeable risk of harms to minors;

(E) an evaluation of the efficacy of safeguards for minors under section 4, and any issues in delivering such safeguards and the associated parental tools; and

(F) an evaluation of any other relevant matters of public concern over risk of harms to minors.

(3) MITIGATION.—The public reports required of a covered platform under this section shall include—

(A) a description of the safeguards and parental tools available to minors and parents on the covered platform;

(B) a description of interventions by the covered platform when it had or has reason to believe that harms to minors could occur;

(C) a description of the prevention and mitigation measures intended to be taken in response to the known and emerging risks identified in its audit of system risks, including steps taken to—

(i) prevent harms to minors, including adapting or removing system design features;

(ii) provide the most protective level of control over privacy and safety by default; and

(iii) adapt algorithmic recommendation systems to prioritize the best interests of users who are minors, as described in section 3(b);

(D) a description of internal processes for handling reports and automated detection mechanisms for harms to minors, including the rate, timeliness, and effectiveness of responses under the requirement of section 4(c);

(E) the status of implementing prevention and mitigation measures identified in prior assessments; and

(F) a description of the additional measures to be taken by the covered platform to address the circumvention of safeguards for minors and parental tools.

(d) Reasonable Inspection.—In conducting an inspection of the systemic risks of harm to minors under this section, an independent, third-party auditor shall—

(1) take into consideration the function of algorithmic recommendation systems;

(2) consult parents and youth experts, including public health and mental health nonprofit organizations, child and adolescent health and development organizations, and civil society with respect to the prevention of harms to minors;

(3) conduct research based on experiences of minors that use the covered platform, including reports under section 4(c) and information provided by law enforcement;

(4) take account of research, including research regarding system design features, marketing, or product integrity, industry best practices, or outside research; and

(5) consider indicia or inferences of age of users, in addition to any self-declared information about the age of individuals.

(e) Cooperation With Independent, Third-party Audit.—To facilitate the report required by subsection (c), a covered platform shall—

(1) provide or otherwise make available to the independent third-party conducting the audit all information and material in its possession, custody, or control that is relevant to the audit;

(2) provide or otherwise make available to the independent third-party conducting the audit access to all network, systems, and assets relevant to the audit; and

(3) disclose all relevant facts to the independent third-party conducting the audit, and not misrepresent in any manner, expressly or by implication, any relevant fact. –

(f) Privacy Safeguards.—

(1) IN GENERAL.—In issuing the public reports required under this section, a covered platform shall take steps to safeguard the privacy of its users, including ensuring that data is presented in a de-identified, aggregated format.

(2) CLARIFICATION.—The section shall not be construed to require—

(A) the affirmative collection of any personal data with respect to the age of users that a covered platform is not already collecting in the normal course of business; or

(B) the covered platform to implement an age gating functionality.

(g) Location.—The public reports required under this section should be posted by a covered platform on an easy to find location on a publicly-available website.

(h) Rulemaking.—The Commission may issue rules pursuant to section 553 of title 5, United States Code to implement this section, specifically establishing processes and minimum standards for third-party auditors to identify and assess—

(1) known and emerging risks to minors; and

(2) how algorithmic recommendation systems and targeted advertising systems can contribute to harms to minors as described in section 3(b).

SEC. 7. INDEPENDENT RESEARCH.

(a) Definitions.—In this section:

(1) ASSISTANT SECRETARY.—The term “Assistant Secretary” means the Assistant Secretary of Commerce for Communications and Information.

(2) DE-IDENTIFIED DATA.—The term “de-identified data” means information—

(A) that does not identify and is not linked or reasonably linkable to an individual or an individual’s device; and

(B) with respect to which a covered platform or researcher takes reasonable technical and contractual measures to ensure that the information is not used to re-identify any individual or individual’s device.

(3) ELIGIBLE RESEARCHER.—The term “eligible researcher” means an individual or group of individuals affiliated with or employed by—

(A) an institution of higher education (as defined in section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001)); or

(B) a nonprofit organization described in section 501(c)(3) of the Internal Revenue Code of 1986.

(4) PROGRAM.—The term “Program” means the program established under subsection (b)(1).

(5) PUBLIC INTEREST RESEARCH.—The term “public interest research” means the scientific or historical analysis of information that is performed for the primary purpose of advancing a broadly recognized public interest.

(6) QUALIFIED RESEARCHER.—The term “qualified researcher” means an eligible researcher who is approved by the Assistant Secretary to conduct public interest research regarding harms to minors under the Program.

(b) Public Interest Research Program Relating to Identified Harms to Minors.—

(1) ESTABLISHMENT.—Subject to paragraph (2), the Assistant Secretary shall establish a program, with public notice and an opportunity to comment, under which an eligible researcher may apply for, and a covered platform shall provide, access to data assets from the covered platform for the sole purpose of conducting public interest research regarding the harms described in section 3(b).

(2) SCOPE OF APPLICATION.—The requirements of this subsection shall not apply to a covered platform if, for the most recent calendar year, the platform averaged ~~had~~ less than 10,000,000 active users on a monthly basis in the United States.

(3) PROCESSES, PROCEDURES, AND STANDARDS.—Not later than 1 year after the date of enactment of this Act, the Assistant Secretary shall establish for the program established under this subsection—

(A) definitions for data assets (related to harms described in section 3(b)) that qualify for disclosure to researchers under the program and standards of access for data assets to be provided under the program;

(B) a process by which an eligible researcher may submit an application described in paragraph (1);

(C) an appeals process for eligible researchers to appeal adverse decisions on applications described in paragraph (1) (including a decision to grant an appeal under paragraph (4)(C));

(D) procedures for implementation of the program, including methods for—

(i) participation by covered platforms; and

(ii) verification by the Assistant Secretary of the credentials of eligible researchers and processes for the application or disqualification to participate in the program;

(E) standards for privacy, security, and confidentiality required to participate in the program;

(F) a mechanism to allow individuals to control the use of their personal data under the program, including the ability to opt out of the program;

(G) standards for transparency regarding the operation and administration of the program; and

(H) rules to prevent requests for data assets that present financial conflicts of interest, including efforts by covered platforms to gain a competitive advantage by directly funding data access requests, the use of qualified researcher status for commercial gain, or efforts by covered platforms to obtain access to intellectual property that is otherwise protected by law.

(4) DUTIES AND RIGHTS OF COVERED PLATFORMS.—

(A) ACCESS TO DATA ASSETS.—

(i) IN GENERAL.—If the Assistant Secretary approves an application under paragraph (1) with respect to a covered platform, the covered platform shall, in a timely manner, provide the qualified researcher with access to data assets necessary to conduct public interest research described in that paragraph.

(ii) LIMITATIONS.—Nothing in this section shall be construed to require a covered platform to provide access to data assets that are intellectual property protected by Federal law, trade secrets, or commercial or financial information.

(iii) FORM OF ACCESS.—A covered platform shall provide to a qualified

researcher access to data assets under clause (i) through online databases, application programming interfaces, and data files as appropriate.

(B) NONDISCLOSURE AGREEMENT.—A covered platform may require, as a condition of access to the data assets of the covered platform, that a qualified researcher enter into a nondisclosure agreement restricting the release of data assets, provided that—

(i) the agreement does not restrict the publication or discussion regarding the qualified researcher’s findings; and

(ii) the terms of the agreement allow the qualified researcher to provide the original agreement or a copy of the agreement to the Assistant Secretary.

(C) APPEAL.—

(i) AGENCY APPEAL.—A covered platform may appeal the granting of an application under paragraph (1) on the grounds that, and the Assistant Secretary shall grant such appeal if—

(I) the covered platform does not have access to the requested data assets or the requested data assets are not reasonably tailored to application; or

(II) providing access to the data assets will lead to material vulnerabilities for the privacy of users or the security of the covered platform’s service or create a significant risk of the violation of Federal or state law.

(ii) JUDICIAL REVIEW.—A decision of the Assistant Secretary with respect to an appeal under clause (i) shall be considered to be a final agency action for purposes of judicial review under chapter 7 of title 5, United States Code.

(D) TIMING.—A covered platform for which this provision applies shall participate no later than two years after enactment of this Act.

(5) APPLICATION REQUIREMENTS.—In order to be approved to access data assets from a covered platform, an eligible researcher shall, in the application submitted under paragraph (1)—

(A) commit to conduct the research for noncommercial purposes;

(B) demonstrate a proven record of expertise on the proposed research topic and related research methodologies;

(C) if the eligible researcher is seeking access to data assets that include personal data, show a reasonable need for access to data assets that would be considered personal data, such as by demonstrating that the research cannot reasonably be accomplished using de-identified data or aggregated information; and

(D) commit to fulfill, and demonstrate a capacity to fulfill, the specific data security and confidentiality requirements corresponding to the application.

(6) PRIVACY AND DUTY OF CONFIDENTIALITY.—

(A) RESEARCHER CONFIDENTIALITY.—To protect user privacy, a qualified researcher shall keep data assets provided by a covered platform under the program confidential and secure.

(B) PLATFORM CONFIDENTIALITY.—A covered platform shall use reasonable measures to enable researcher access to data assets under the program in a secure and privacy-protective manner, including through the de-identification of personal data or use of other privacy-enhancing technologies.

(C) FEDERAL AGENCIES.—Nothing in this subsection shall be construed to authorize a Federal agency to seek access to the data of a covered platform through the ~~Program~~ program.

(c) SAFE HARBOR FOR COLLECTION OF DATA FOR PUBLIC INTEREST RESEARCH Regarding Identified Harms to Minors.—If, in the course of conducting public interest research regarding harms described in section 3(b) (without regard to whether such research is conducted under the program), an eligible researcher collects or uses data from a covered platform in a manner that violates the terms of service of the platform, no cause of action based on such violation shall lie or be maintained in any court against such researcher unless the violation relates to the failure of the researcher to take reasonable measures to protect user privacy and security.

(d) RULEMAKING.—The Assistant Secretary, in consultation with the Secretary of Commerce, the Director of the National Institute of Standards and Technology, the Director of the National Science Foundation, and the Director of the National Institutes of Health shall promulgate rules in accordance with section 553 of title 5, United States Code, as necessary to implement this section.

SEC. 8. MARKET RESEARCH.

(a) Market Research by Covered Platforms.—The Federal Trade Commission, in consultation with the Secretary of Commerce, shall establish guidance for covered platforms seeking to conduct market- and product-focused research on minors or individuals it reasonably believes to be minors. Such guidance shall include—

(1) a standard consent form that provides minors and their parents a clear, conspicuous, and easy-to-understand explanation of the scope and purpose of the research to be conducted, and provides an opportunity for informed consent; and

(2) recommendations for research practices for studies that may include minors, disaggregated by the age ranges of 0-5, 6-9, 10-12, and 13 -16.

(b) Guidelines.—The Federal Trade Commission shall promulgate such guidelines not later than 18 months after the date of enactment of this Act. In doing so, they shall seek input from members of the public and the representatives of the Kids Online Safety Council established under section 12.

SEC. 9. AGE VERIFICATION STUDY AND REPORT.

(a) Study.—The Director of the National Institute of Standards and Technology, in coordination with the Federal Communications Commission, Federal Trade Commission, and the Secretary of Commerce, shall conduct a study evaluating the most technologically feasible methods and options for developing systems to verify age at the device or operating system level.

(b) Contents.—Such study shall consider —

(1) the benefits of creating a device or operating system level age verification system;

(2) what information may need to be collected to create this type of age verification system;

(3) the accuracy of such systems and their impact or steps to improve accessibility, including for individuals with disabilities;

(4) how such a system or systems could verify age while mitigating risks to user privacy and data security and safeguarding minors' personal data, emphasizing minimizing the amount of data collected and processed by covered platforms for such a system; and

(5) the technical feasibility, including the need for potential hardware and software changes, including for devices currently in commerce and owned by consumers.

(c) Report.—Not later than 1 year after the date of enactment of this Act, the agencies described in subsection (a) shall submit a report containing the results of the study conducted under such subsection to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Energy and Commerce of the House of Representatives.

SEC. 10. GUIDANCE.

Not later than 1 year after the date of enactment of this Act, the Federal Trade Commission, in consultation with the Kids Online Safety Council established under section 12, shall issue guidance to—

(1) assist elementary or secondary schools in using the notice, safeguards and tools provided under this Act and facilitate compliance with student privacy laws; and

(2) provide information and examples for covered platforms and auditors regarding—

(A) identifying features that are used to increase, sustain, or extend use of the covered platform by a minor;

(B) safeguarding minors against the possible misuse of parental tools;

(C) best practices in providing minors and parents the most protective level of control over privacy and safety;

(D) using indicia or inferences of age of users for assessing use of the covered platform by minors;

(E) methods for evaluating the efficacy of safeguards; and

(F) providing additional control options that allow parents to address the harms described in section 3(b).

(3) outline conduct that does not have the purpose or substantial effect of subverting or impairing user autonomy, decision-making, or choice, or of causing, increasing, or encouraging compulsive usage for a minor, such as—

(A) de minimis user interface changes derived from testing consumer preferences, including different styles, layouts, or text, where such changes are not done with the purpose of weakening or disabling safeguards or parental controls;

(B) algorithms or data outputs outside the control of a covered platform; and

(C) establishing default settings that provide enhances privacy protection to users or

otherwise enhance their autonomy and decision-making ability.

SEC. 11. ENFORCEMENT.

(a) Enforcement by Federal Trade Commission.—

(1) UNFAIR AND DECEPTIVE ACTS OR PRACTICES.—A violation of this Act or a regulation promulgated under this Act shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

(2) POWERS OF THE COMMISSION.—

(A) IN GENERAL.—Except as provided in subsection (b), the Federal Trade Commission (referred to in this section as the “Commission”) shall enforce this Act and any regulation promulgated under 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.

(B) PRIVILEGES AND IMMUNITIES.—Any person that violates this Act or a regulation promulgated under this Act shall be subject to the penalties, and entitled to the privileges and immunities, provided in the Federal Trade Commission Act (15 U.S.C. 41 et seq.).

(4) AUTHORITY PRESERVED.—Nothing in this Act shall be construed to limit the authority of the Commission under any other provision of law.

(b) Enforcement by State Attorneys General.—

(1) IN GENERAL.—

(A) CIVIL ACTIONS.—In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the engagement of any person in a practice that violates this Act or a regulation promulgated under this Act, the State, as *parens patriae*, may bring a civil action on behalf of the residents of the State in a district court of the United States or a State court of appropriate jurisdiction to—

(i) enjoin that practice;

(ii) enforce compliance with this Act or such regulation;

(iii) on behalf of residents of the State, obtain damages, restitution, or other compensation, each of which shall be distributed in accordance with State law; or

(iv) obtain such other relief as the court may consider to be appropriate.

(B) NOTICE.—

(i) IN GENERAL.—Before filing an action under subparagraph (A), the attorney general of the State involved shall provide to the Commission—

(I) written notice of that action; and

(II) a copy of the complaint for that action.

(ii) EXEMPTION.—

(I) IN GENERAL.—Clause (i) shall not apply with respect to the filing of an action by an attorney general of a State under this paragraph if the attorney general of the State determines that it is not feasible to provide the notice described in that clause before the filing of the action.

(II) NOTIFICATION.—In an action described in subclause (I), the attorney general of a State shall provide notice and a copy of the complaint to the Commission at the same time as the attorney general files the action.

(2) INTERVENTION.—

(A) IN GENERAL.—On receiving notice under paragraph (1)(B), the Commission shall have the right to intervene in the action that is the subject of the notice.

(B) EFFECT OF INTERVENTION.—If the Commission intervenes in an action under paragraph (1), it shall have the right—

- (i) to be heard with respect to any matter that arises in that action; and
- (ii) to file a petition for appeal.

(3) CONSTRUCTION.—For purposes of bringing any civil action under paragraph (1), nothing in this Act shall be construed to prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State to—

- (A) conduct investigations;
- (B) administer oaths or affirmations; or
- (C) compel the attendance of witnesses or the production of documentary and other evidence.

(4) ACTIONS BY THE COMMISSION.—In any case in which an action is instituted by or on behalf of the Commission for violation of this Act or a regulation promulgated under this Act, no State may, during the pendency of that action, institute a separate action under paragraph (1) against any defendant named in the complaint in the action instituted by or on behalf of the Commission for that violation.

(5) VENUE; SERVICE OF PROCESS.—

(A) VENUE.—Any action brought under paragraph (1) may be brought in—

- (i) the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code; or
- (ii) a State court of competent jurisdiction.

(B) SERVICE OF PROCESS.—In an action brought under paragraph (1) in a district court of the United States, process may be served wherever defendant—

- (i) is an inhabitant; or
- (ii) may be found.

SEC. 12. KIDS ONLINE SAFETY COUNCIL.

(a) Establishment.—Not later than 180 days after the date of enactment of this Act, the Secretary of Commerce shall establish and convene the Kids Online Safety Council for the purpose of providing advice on matters related to this Act.

(b) Participation.—The Kids Online Safety Council shall include diverse participation from—

(1) academic experts, health professionals, and members of civil society with expertise in mental health and the prevention of harms to minors;

(2) representatives in academia and civil society with specific expertise in privacy and civil liberties;

(3) parents and youth representation;

(4) representatives of covered platforms;

(5) representatives of the National Telecommunications and Information Administration, the National Institute of Standards and Technology, the Federal Trade Commission, the Department of Justice, and the Department of Health and Human Services; and

(6) State attorneys general or their Designees acting in State or local government; and

(7) representatives of communities of socially disadvantaged individuals (as defined in section 8 of the Small Business Act (15 U.S.C. 637)).

(c) ACTIVITIES.—THE MATTERS TO BE ADDRESSED BY THE KIDS ONLINE SAFETY COUNCIL SHALL INCLUDE—

(1) identifying emerging or current risks of harms to minors associated with online platforms;

(2) recommending measures and methods for assessing, preventing, and mitigating harms to minors online;

(3) recommending methods and themes for conducting research regarding online harms to minors; and,

(4) recommending best practices and clear, consensus-based technical standards for transparency reports and audits, as required under this Act.

The recommended standards for reports and audits under paragraph (4) shall include methods, criteria, and scope to promote overall accountability.

SEC. 13. EFFECTIVE DATE.

Except as otherwise provided in this Act, this Act shall take effect on the date that is 18 months after the date of enactment of this Act.

SEC. 14. RELATIONSHIP TO OTHER LAWS.

Nothing in this Act shall be construed to—

(1) preempt section 444 of the General Education Provisions Act (20 U.S.C. 1232g, commonly known as the “Family Educational Rights and Privacy Act of 1974”) or other Federal or State laws governing student privacy; or

(2) authorize any action that would conflict with section 18(h) of the Federal Trade

Commission Act (15 U.S.C. 57a(h)).

SEC. 15. SEVERABILITY.

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