H. R. 1623

To require operating systems for interactive computing devices to implement secure setup modes to protect minors from harmful content, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

February 26, 2025

Mrs. Miller of Illinois (for herself, Mr. Van Drew, Mr. Brecheen, Mr. LaMalfa, Mr. Austin Scott of Georgia, Mr. Kennedy of Utah, Mr. Crane, Mr. Aderholt, Mr. Babin, and Mr. Rose) introduced the following bill; which was referred to the Committee on Energy and Commerce.

A BILL

To require operating systems for interactive computing devices to implement secure setup modes to protect minors from harmful content, and for other purposes.

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 “Shielding Children's Retinas from Egregious Exposure on the Net Act” or the “SCREEN Act”.

SEC. 2. FINDINGS; SENSE OF CONGRESS.

(a) Findings.—Congress finds the following:

(1) Over the 3 decades preceding the date of enactment of this Act, Congress has passed several bills to protect minors from access to online pornographic content, including title V of the Telecommunications Act of 1996 (Public Law 104–104) (commonly known as the “Communications Decency Act”), section 231 of the Communications Act of 1934 (47 U.S.C. 231) (commonly known as the “Child Online Protection Act”), and the Children’s Internet Protection Act (title XVII of division B of Public Law 106–554).

(2) With the exception of the Children's Internet Protection Act (title XVII of division B of Public Law 106–554), the Supreme Court of the United States has struck down the previous efforts of Congress to shield children from pornographic content, finding that such legislation constituted a “compelling government interest” but that it was not the least restrictive means to achieve such interest. In Ashcroft v. ACLU, 542 U.S. 656 (2004), the Court even suggested at the time that “blocking and filtering software” could conceivably be a “primary alternative” to the requirements passed by Congress.

(3) In the nearly 2 decades since the Supreme Court of the United States suggested the use of “blocking and filtering software”, such technology has proven to be ineffective in protecting minors from accessing online pornographic content. The Kaiser Family Foundation has found that filters do not work on 1 in 10 pornography sites accessed intentionally and 1 in 3 pornography sites that are accessed unintentionally. Further, it has been proven that children are able to bypass “blocking and filtering” software by employing strategic searches or measures to bypass the software completely.

(4) Additionally, Pew Research has revealed studies showing that only 39 percent of parents use blocking or filtering software for their minor’s online activities, meaning that 61 percent of children only have restrictions on their internet access when they are at school or at a library.

(5) 17 States have now recognized pornography as a public health hazard that leads to a broad range of individual harms, societal harms, and public health impacts.

(6) It is estimated that 80 percent of minors between the ages of 12 to 17 have been exposed to pornography, with 54 percent of teenagers seeking it out. The internet is the most common source for minors to access pornography, with pornographic websites receiving more web traffic in the United States than Twitter, Netflix, Pinterest, and LinkedIn combined.

(7) Exposure to online pornography has created unique psychological effects for minors, including anxiety, addiction, low self-esteem, body image disorders, an increase in problematic sexual activity at younger ages, and an increased desire among minors to engage in risky sexual behavior.

(8) The Supreme Court of the United States has recognized on multiple occasions that Congress has a “compelling government interest” to protect the physical and psychological well-being of minors, which includes shielding them from “indecent” content that may not necessarily be considered “obscene” by adult standards.

(9) Because “blocking and filtering software” has not produced the results envisioned nearly 2 decades ago, it is necessary for Congress to pursue alternative policies to enable the protection of the physical and psychological well-being of minors.

(10) The evolution of our technology has now enabled the use of device-level setup processes that are cost efficient, not unduly burdensome, and can be operated narrowly in a manner that ensures only adults have

unrestricted access to harmful content.

(b) Sense of Congress.—It is the sense of Congress that—

(1) shielding minors from access to online pornographic content is a compelling government interest that protects the physical and psychological well-being of minors; and

(2) requiring operating systems for interactive computing devices to implement secure, locked setup modes that enable content filtering and prohibit circumvention tools is the least restrictive means for Congress to achieve its compelling government interest.

SEC. 3. DEFINITIONS.

In this Act:

(1) CHILD PORNOGRAPHY; MINOR.—The terms “child pornography” and “minor” have the meanings given those terms in section 2256 of title 18, United States Code.

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

(3) COVERED DEVICE.—The term “covered device” means any interactive computing device, including smartphones, tablets, laptops, and personal computers, that is capable of accessing the internet and is manufactured, sold, or distributed for consumer use in interstate commerce.

(4) HARMFUL TO MINORS.—The term “harmful to minors”, with respect to a picture, image, graphic image file, film, videotape, or other visual depiction, means that the picture, image, graphic image file, film, videotape, or other depiction—

(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;

(B) is obscene; or

(C) is child pornography.

(5) INTERACTIVE COMPUTING DEVICE.—The term “interactive computing device” means any hardware device that enables users to interact with online content through an operating system.

(6) OPERATING SYSTEM.—The term “operating system” means the software that manages hardware and software resources on a covered device and provides common services for programs.

(7) SECURE SETUP MODE.—The term “secure setup mode” means a device configuration process that—

(A) offers parental selection of an adult or child mode during initial activation;

(B) locks the selected mode based on verified user age until a flash factory reset or age of majority; and

(C) in child mode, employs integrated filtering to block access to content harmful to minors and disables location-obfuscation tools.

(8) 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.

(9) COMMISSION-APPROVED CLASSIFIERS.—The term “Commission-approved classifiers” means machine learning or algorithmic tools certified by the Commission as meeting the following criteria: (A) achieving at least 95 percent accuracy in identifying content harmful to minors, as validated through independent third-party testing; (B) minimizing false positives for educational, scientific, or artistic content; (C) operating entirely on device without external data transmission; and (D) complying with standards issued under section 6(b).

(10) LOCATION-OBFUSCATION TOOLS.—The term “location-obfuscation tools” means any software or service that masks, spoofs, or alters a device's apparent geographic location or internet protocol address, including virtual private networks, proxy servers, Tor networks, or similar anonymity services.

(11) REASONABLE DATA SECURITY.—The term “reasonable data security” means security measures that conform to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (version 2.0 or successor) and include, at minimum, encryption of stored data using AES-256 or equivalent, access controls via multi-factor authentication, and regular vulnerability assessments.

(12) REGULAR AUDITS.—The term “regular audits” means audits conducted at least annually by the Commission or its designated third-party agents.

SEC. 4. SECURE SETUP MODE REQUIREMENTS.

(a) Operating System Requirements.—Beginning on the date that is 1 year after the date of enactment of this Act, each operating system distributed or installed on a covered device in the United States shall implement a secure setup mode during initial device activation to ensure that—

(1) minors are prevented from accessing content harmful to minors; and

(2) users in child mode cannot circumvent protections without a full device reset.

(b) Requirements for Secure Setup Modes.—The secure setup mode implemented by an operating system shall—

(1) present a mandatory dual-path selection during initial activation, consisting of—

(A) an adult mode providing unrestricted access; and

(B) a child mode requiring parental input of the childs date of birth via a secure on-device process, defined as multi-factor authentication using biometric or hardware-based verification or local document verification via on-device optical character recognition without data transmission;

(2) lock the selected mode irrevocably until—

(A) the device is flash reset to factory conditions, erasing all data and requiring re-setup; or

(B) the verified birthdate indicates the user has reached 18 years of age, triggering an automated handover with parental confirmation;

(3) in child mode—

(A) automatically enable content filters using integrated, Commission-approved classifiers to block access to material harmful to minors;

(B) prohibit installation, activation, or use of location-obfuscation tools except as permitted by the parent;

(C) enforce device-level safeguards, including geofencing for compliance without external data transmission; and

(D) process all data locally, with no cloud verification or retention beyond what is necessary for mode enforcement;

(4) recommend child mode as the default for devices marketed to families; and

(5) make publicly available the setup process and compliance documentation.

(c) Choice of Implementation.—An operating system provider may select specific technologies for secure setup modes, provided they meet the requirements of subsection (b) and effectively prohibit minors from accessing harmful content.

(d) Use of Third Parties.—An operating system provider may contract with third parties for components of the secure setup mode but remains responsible for full compliance and liability under this Act.

(e) Rule of Construction.—Nothing in this section requires submission to the Commission of information identifying or linkable to a user or device.

(f) Data Security.—An operating system provider shall—

(1) establish, implement, and maintain reasonable data security to protect the confidentiality, integrity, and accessibility of data collected during setup, against unauthorized access; and

(2) retain such data no longer than reasonably necessary for mode enforcement or compliance demonstration.

(g) Parental Override Mechanism and Content Ratings.—

(1) Universal Digital Content Ratings (UDCR) Requirement.—

(A) Not later than 180 days after enactment, the Commission shall establish a voluntary but incentivized UDCR system, modeled on established rating frameworks such as the Motion Picture Association ratings or TV Parental Guidelines, for websites, applications, and online media accessible via covered devices. Ratings shall classify content by age-appropriateness (e.g., All Ages, Parental Guidance, Mature 17+) and include descriptors for themes like violence (V), sexual content (S), nudity (N), and misinformation (M—indicating unsubstantiated or misleading claims that could harm minors' physical, psychological, or civic well-being, as defined in Commission guidance).

(B) Covered platforms (websites/apps hosting user-generated or commercial content) must self-apply UDCR labels, verified through Commission-approved third-party auditors, with non-compliance treated as a violation under section 7. Operating systems shall prioritize UDCR metadata in classifiers under section 3(9), achieving seamless integration for automated filtering.

(C) The Commission shall provide guidance minimizing burdens on small creators, with safe harbors for educational/artistic content rated via independent review.

(2) Device-to-Device Override Process.—

In child mode, if integrated classifiers block content lacking a UDCR label or flagged as potentially harmful:

(A) The device shall generate a secure, ephemeral request notification to the parent-verified guardian device (paired during setup via local encryption, e.g., end-to-end Bluetooth or WiFi Direct, with no external transmission);

(B) The notification includes content preview (e.g., URL snippet, UDCR if available) and proposed access parameters (e.g., one-time, duration-limited);

(C) Upon guardian approval—via multi-factor biometric or hardware authentication—the override grants temporary access, logged locally for family review only; denials auto-escalate to full block;

(D) Overrides expire automatically (default: 24 hours) and require re-verification for repeats; no override shall disable core protections; parental override for location-obfuscation shall include options for temporary or until revoked.

(E) Providers shall ensure overrides comply with reasonable data security under section 3(11), with data deletion post-session.

(3) Enforcement of Ratings Integrity.—

(A) Willful falsification, manipulation, or gaming of UDCR labels (e.g., underrating harmful content to evade filters) shall be treated as a violation of section 4 and subject to enforcement under section 7, including civil penalties not exceeding $1,000,000 per violation (adjusted for inflation), sanctions such as mandatory re-labeling or temporary platform delisting, and corrective actions like public disclosures of non-compliance.

(B) The Commission shall conduct random audits of at least 5% of rated platforms annually, using third-party verifiers, and publish aggregate findings to deter abuse. Repeat offenders (3+ violations in 24 months) face enhanced penalties, up to twice the base fine.

(C) Platforms may appeal ratings via an expedited Commission process, with protections for good-faith errors

SEC. 5. CONSULTATION REQUIREMENTS.

In enforcing the requirements under section 4, the Commission shall consult with—

(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 victimized by online exploitation;

(3) individuals with experience in consumer protection and online privacy;

(4) individuals who supply secure setup or filtering technologies; and

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

SEC. 6. COMMISSION REQUIREMENTS.

(a) In General.—The Commission shall—

(1) conduct regular audits of operating system providers to ensure compliance with section 4;

(2) make public the terms and processes for audits, including third-party processes;

(3) establish a process for providers to submit necessary documents for audits; and

(4) prescribe documents or measures to demonstrate compliance.

(b) Guidance.—

(1) In General.—Not later than 180 days after enactment, the Commission shall issue guidance to assist compliance with section 4, including specific criteria for approving classifiers under section 3(9).

(2) Limitations.—Guidance does not confer rights, bind the Commission, or form the basis for enforcement absent a specific violation of this Act.

SEC. 7. ENFORCEMENT.

(a) Unfair or Deceptive Act or Practice.—A violation of section 4 shall be treated as a violation of a rule defining an unfair or deceptive act or practice under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) and subject to enforcement by the Commission.

(b) Civil Penalty.—Any operating system provider who violates section 4 shall be liable for a civil penalty of not more than $43,792 per violation, as adjusted under section 4.9 of title 16, Code of Federal Regulations.

(c) Savings Clause.—Nothing in this Act affects or limits the application of any other Federal, State, or local law.