118TH CONGRESS
1ST SESSION

To require certain interactive computer services to adopt and operate technology verification measures to ensure that users of the platform are not minors, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. Lee introduced the following bill; which was read twice and referred to the Committee on

A BILL

To require certain interactive computer services to adopt and operate technology verification measures to ensure that users of the platform are not minors, and for other purposes.

1 Be it enacted by the Senate and House of Representa-
2 tives of the United States of America in Congress assembled,

3 SECTION 1. SHORT TITLE.

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

5 SEC. 2. FINDINGS; SENSE OF CONGRESS.

6 (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 age verification technology that is cost efficient, not unduly burdensome, and can be operated narrowly in a manner that ensures only
adults have access to a website’s online pornographic 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 interactive computer services that are in the business of creating, hosting, or making available pornographic content to enact technological measures that shield minors from accessing pornographic content on their platforms 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 platform.—The term “covered platform”—
(A) means an entity—

(i) that is an interactive computer service;

(ii) that—

(I) is engaged in interstate or foreign commerce; or

(II) purposefully avails itself of the United States market or a portion thereof; and

(iii) for which it is in the regular course of the trade or business of the entity to create, host, or make available content that meets the definition of harmful to minors under paragraph (4) and that is provided by the entity, a user, or other information content provider, with the objective of earning a profit; and

(B) includes an entity described in subparagraph (A) regardless of whether—

(i) the entity earns a profit on the activities described in subparagraph (A)(iii); or

(ii) creating, hosting, or making available content that meets the definition of harmful to minors under paragraph (4) is
the sole source of income or principal business of the entity.

(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) INFORMATION CONTENT PROVIDER; INTERACTIVE COMPUTER SERVICE.—The terms "information content provider" and "interactive computer service" have the meanings given those terms in sec-
tion 230(f) of the Communications Act of 1934 (47 U.S.C. 230(f)).

(6) 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.

(7) Technology verification measure.—The term “technology verification measure” means technology that—

(A) employs a system or process to determine whether it is more likely than not that a user of a covered platform is a minor; and

(B) prevents access by minors to any content on a covered platform.

(8) Technology verification measure data.—The term “technology verification measure data” means information that—

(A) identifies, is linked to, or is reasonably linkable to an individual or a device that identifies, is linked to, or is reasonably linkable to an individual;

(B) is collected or processed for the purpose of fulfilling a request by an individual to access any content on a covered platform; and
(C) is collected and processed solely for the purpose of utilizing a technology verification measure and meeting the obligations imposed under this Act.

SEC. 4. TECHNOLOGY VERIFICATION MEASURES.

(a) COVERED PLATFORM REQUIREMENTS.—Beginning on the date that is 1 year after the date of enactment of this Act, a covered platform shall adopt and utilize technology verification measures on the platform to ensure that—

(1) users of the covered platform are not minors; and

(2) minors are prevented from accessing any content on the covered platform that is harmful to minors.

(b) REQUIREMENTS FOR AGE VERIFICATION MEASURES.—In order to comply with the requirement of subsection (a), the technology verification measures adopted and utilized by a covered platform shall do the following:

(1) Use a technology verification measure in order to verify a user’s age.

(2) Provide that requiring a user to confirm that the user is not a minor shall not be sufficient to satisfy the requirement of subsection (a).
(3) Make publicly available the verification process that the covered platform is employing to comply with the requirements under this Act.

(4) Subject the Internet Protocol (IP) addresses, including known virtual proxy network IP addresses, of all users of a covered platform to the technology verification measure described in paragraph (1) unless the covered platform determines based on available technology that a user is not located within the United States.

(c) Choice of Verification Measures.—A covered platform may choose the specific technology verification measures to employ for purposes of complying with subsection (a), provided that the technology verification measure employed by the covered platform meets the requirements of subsection (b) and prohibits a minor from accessing the platform or any information on the platform that is obscene, child pornography, or harmful to minors.

(d) Use of Third Parties.—A covered platform may contract with a third party to employ technology verification measures for purposes of complying with subsection (a) but the use of such a third party shall not relieve the covered platform of its obligations under this Act or from liability under this Act.
(c) Rule of Construction.—Nothing in this section shall be construed to require a covered platform to submit to the Commission any information that identifies, is linked to, or is reasonably linkable to a user of the covered platform or a device that identifies, is linked to, or is reasonably linkable to a user of the covered platform.

(f) Technology Verification Measure Data Security.—A covered platform shall—

(1) establish, implement, and maintain reasonable data security to—

(A) protect the confidentiality, integrity, and accessibility of technology verification measure data collected by the covered platform or a third party employed by the covered platform; and

(B) protect such technology verification measure data against unauthorized access; and

(2) retain the technology verification measure data for no longer than is reasonably necessary to utilize a technology verification measure or what is minimally necessary to demonstrate compliance with the obligations under this Act.

SEC. 5. CONSULTATION REQUIREMENTS.

In enforcing the requirements under section 4, 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 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 measure solutions.

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

SEC. 6. COMMISSION REQUIREMENTS.

(a) IN GENERAL.—The Commission shall—
(1) conduct regular audits of covered platforms
to ensure compliance with the requirements of sec-
tion 4;

(2) make public the terms and processes for the
audits conducted under paragraph (1), including the
processes for any third party conducting an audit on
behalf of the Commission;
(3) establish a process for each covered platform to submit only such documents or other materials as are necessary for the Commission to ensure full compliance with the requirements of section 4 when conducting audits under this section; and

(4) prescribe the appropriate documents, materials, or other measures required to demonstrate full compliance with the requirements of section 4.

(b) GUIDANCE.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Commission shall issue guidance to assist covered platforms in complying with the requirements of section 4.

(2) LIMITATIONS ON GUIDANCE.—No guidance issued by the Commission with respect to this Act shall confer any rights on any person, State, or locality, nor shall operate to bind the Commission or any person to the approach recommended in such guidance. In any enforcement action brought pursuant to this Act, the Commission shall allege a specific violation of a provision of this Act. The Commission may not base an enforcement action on, or execute a consent order based on, practices that are alleged to be inconsistent with any such guidelines,
unless the practices allegedly violate a provision 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)).

(b) POWERS OF THE COMMISSION.—

(1) IN GENERAL.—The Commission shall enforce section 4 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 title.

(2) PRIVILEGES AND IMMUNITIES.—Any person who violates section 4 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.).

(3) AUTHORITY PRESERVED.—Nothing in this Act shall be construed to limit the authority of the Commission under any other provision of law.
SEC. 8. GAO REPORT.

Not later than 2 years after the date on which covered platforms are required to comply with the requirement of section 4(a), the Comptroller General of the United States shall submit to Congress a report that includes—

(1) an analysis of the effectiveness of the technology verification measures required under such section;

(2) an analysis of rates of compliance with such section among covered platforms;

(3) an analysis of the data security measures used by covered platforms in the age verification process;

(4) an analysis of the behavioral, economic, psychological, and societal effects of implementing technology verification measures;

(5) recommendations to the Commission on improving enforcement of section 4(a), if any; and

(6) recommendations to Congress on potential legislative improvements to this Act, if any.

SEC. 9. SEVERABILITY CLAUSE.

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