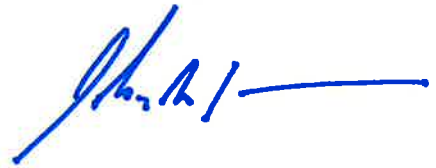


S. 737 Curtis Substitute (as modified)



AMENDMENT NO. \_\_\_\_\_ Calendar No. \_\_\_\_\_

Purpose: In the nature of a substitute.

IN THE SENATE OF THE UNITED STATES—119th Cong., 2d Sess.

**S. 737**

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.

Referred to the Committee on \_\_\_\_\_ and  
ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT IN THE NATURE OF A SUBSTITUTE intended  
to be proposed by \_\_\_\_\_

Viz:

1 Strike all after the enacting clause and insert the fol-  
2 lowing:

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Shielding Children’s  
5 Retinas from Egregious Exposure on the Net Act of  
6 2026” or the “SCREEN Act of 2026”.

7 **SEC. 2. DEFINITIONS.**

8 In this Act:

9 (1) COMMISSION.—The term “Commission”

10 means the Federal Trade Commission.

1           (2) COVERED PLATFORM.—The term “covered  
2 platform” means a website or other online plat-  
3 form—

4           (A) that is engaged in interstate or foreign  
5 commerce; and

6           (B) with respect to which more than one-  
7 third of the material made available thereon is  
8 sexual material harmful to minors.

9           (3) MINOR.—The terms “minor” has the mean-  
10 ing given that term in section 2256 of title 18,  
11 United States Code.

12           (4) SEXUAL ACT; SEXUAL CONTACT.—The  
13 terms “sexual act” and “sexual contact” have the  
14 meanings given those terms in section 2246 of title  
15 18, United States Code.

16           (5) SEXUAL MATERIAL HARMFUL TO MINORS.—  
17 The term “sexual material harmful to minors”  
18 means a picture, image, graphic image file, film, vid-  
19 eotape, or other visual depiction that—

20           (A) the average individual applying con-  
21 temporary community standards would find,  
22 taking the material as a whole and with respect  
23 to minors, is designed to appeal to or pander to  
24 the prurient interest;

1 (B) in a manner patently offensive with re-  
2 spect to minors, exploits, is devoted to, or prin-  
3 cipally consists of a description of, an actual,  
4 simulated, or animated display or depiction of a  
5 sexual act or sexual contact; and

6 (C) taken as a whole, lacks serious literary,  
7 artistic, political, or scientific value for minors.

8 (6) STATE.—The term “State” means each  
9 State of the United States, the District of Columbia,  
10 each commonwealth, territory, or possession of the  
11 United States, and each federally recognized Indian  
12 Tribe.

13 (7) TECHNOLOGY VERIFICATION MEASURE.—  
14 The term “technology verification measure” means  
15 technology that employs a system or process to de-  
16 termine whether it is more likely than not that a  
17 user attempting to access a covered platform is a  
18 minor.

19 (8) TECHNOLOGY VERIFICATION MEASURE  
20 DATA.—The term “technology verification measure  
21 data” means data that—

22 (A) is collected or processed for the pur-  
23 pose of fulfilling a request by an individual to  
24 access a covered platform or material on a cov-  
25 ered platform; and

1 (B) is collected or processed for the pur-  
2 pose of utilizing or providing a technology  
3 verification measure pursuant to this Act.

4 **SEC. 3. TECHNOLOGY VERIFICATION MEASURES.**

5 (a) COVERED PLATFORM REQUIREMENTS.—Begin-  
6 ning on the date that is 1 year after the date of the enact-  
7 ment of this Act, a provider of a covered platform shall—

8 (1) adopt and utilize commercially available  
9 technology verification measures with respect to the  
10 covered platform of such provider to identify wheth-  
11 er a user attempting to access the covered platform  
12 is a minor; and

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

16 (b) ADDITIONAL REQUIREMENTS FOR COMPLI-  
17 ANCE.—In order to comply with subsection (a), a provider  
18 of a covered platform shall, with respect to a covered plat-  
19 form of the provider, carry out the following:

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

22 (2) Provide that a user confirming that the user  
23 is not a minor is not sufficient to comply with para-  
24 graph (1).

1           (3) Provide a clear and conspicuous notice con-  
2           taining information on the technology verification  
3           measures and other policies and procedures related  
4           to the technology verification measure data used to  
5           comply with this Act.

6           (4) Take reasonable measures to address cir-  
7           cumvention of technology verification measures, in-  
8           cluding use of known virtual private network IP ad-  
9           dresses.

10          (5) Not transfer, disclose, or retain any tech-  
11          nology verification measure data beyond what is  
12          strictly necessary to use a technology verification  
13          measure pursuant to this Act or what is minimally  
14          necessary to demonstrate compliance with the obli-  
15          gations under this Act.

16          (6) Not collect or use technology verification  
17          measure data for any purpose beyond what is strict-  
18          ly necessary to utilize a technology verification meas-  
19          ure pursuant to this Act.

20          (c) USE OF THIRD PARTIES.—

21               (1) IN GENERAL.—A provider of a covered plat-  
22               form may contract with a third party to use tech-  
23               nology verification measures for purposes of com-  
24               plying with this section.

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

5       (d) CHOICE OF VERIFICATION MEASURES.—A pro-  
6       vider of a covered platform may choose the specific tech-  
7       nology verification measures to utilize for purposes of com-  
8       plying with subsection (a), if such measures satisfy sub-  
9       section (b).

10       (e) TECHNOLOGY VERIFICATION MEASURE DATA SE-  
11       curity.—A provider of a covered platform shall establish,  
12       implement, and maintain reasonable administrative, tech-  
13       nical, and physical data security practices to protect—

14           (1) the confidentiality, integrity, and availability  
15       of technology verification measure data collected  
16       with respect to the covered platform of such pro-  
17       vider; and

18           (2) such technology verification measure data  
19       against unauthorized access.

20       **SEC. 4. CONSULTATION REQUIREMENTS.**

21       In carrying out this Act, the Commission shall con-  
22       sult with the following individuals, including with respect  
23       to the applicable standards and metrics for making a de-  
24       termination regarding whether a user of a covered plat-  
25       form is a minor:

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

3           (2) Individuals with experience in—

4                 (A) advocating for online child safety; or

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

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

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

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

14 **SEC. 5. GAO REPORT.**

15       Not later than 3 years after the date of the enact-  
16 ment of this Act, the Comptroller General of the United  
17 States shall submit to Congress a report that includes the  
18 following:

19           (1) An analysis of the effectiveness of the tech-  
20 nology verification measures required by section 3.

21           (2) An analysis of the rate of compliance with  
22 such section by providers of covered platforms and  
23 third parties contracted by such providers with re-  
24 spect to such covered platforms.

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

4           (4) An analysis of the expression, speech, be-  
5           havioral, economic, psychological, and societal effects  
6           of the technology verification measures required by  
7           section 3.

8           (5) Recommendations, if any, to the Commis-  
9           sion on improving the enforcement of this Act.

10 **SEC. 6. ENFORCEMENT.**

11       (a) **ENFORCEMENT BY COMMISSION.**—

12           (1) **UNFAIR OR DECEPTIVE ACTS OR PRAC-**  
13           **TICES.**—A violation of section 3 shall be treated as  
14           a violation of a rule defining an unfair or deceptive  
15           act or practice under section 18(a)(1)(B) of the Fed-  
16           eral Trade Commission Act (15 U.S.C.  
17           57a(a)(1)(B)).

18           (2) **POWERS OF COMMISSION.**—

19           (A) **IN GENERAL.**—The Commission shall  
20           enforce section 3 in the same manner, by the  
21           same means, and with the same jurisdiction,  
22           powers, and duties as though all applicable  
23           terms and provisions of the Federal Trade  
24           Commission Act (15 U.S.C. 41 et seq.) were in-  
25           corporated into and made a part of this Act.



1 (B) PRIVILEGES AND IMMUNITIES.—Any  
2 person who violates section 3 shall be subject to  
3 the penalties and entitled to the privileges and  
4 immunities provided in the Federal Trade Com-  
5 mission Act (15 U.S.C. 41 et seq.).

6 (C) AUTHORITY PRESERVED.—Nothing in  
7 this Act may be construed to limit the authority  
8 of the Commission under any other provision of  
9 law.

10 (b) ACTIONS BY STATES.—

11 (1) IN GENERAL.—In any case in which the at-  
12 torney general of a State, or an official or agency of  
13 a State, has reason to believe that an interest of the  
14 residents of such State has been or is threatened or  
15 adversely affected by an act or practice in violation  
16 of section 3, the State, as *parens patriae*, may bring  
17 a civil action on behalf of the residents of the State  
18 in an appropriate district court of the United States  
19 to—

20 (A) enjoin such act or practice;

21 (B) enforce compliance with this Act;

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

1 (D) obtain such other legal and equitable  
2 relief as the court may consider to be appro-  
3 priate.

4 (2) NOTICE.—Before filing an action under this  
5 subsection, the attorney general, official, or agency  
6 of the State involved shall provide to the Commis-  
7 sion a written notice of such action and a copy of  
8 the complaint for such action. If the attorney gen-  
9 eral, official, or agency determines that it is not fea-  
10 sible to provide the notice described in this para-  
11 graph before the filing of the action, the attorney  
12 general, official, or agency shall provide written no-  
13 tice of the action and a copy of the complaint to the  
14 Commission immediately upon the filing of the ac-  
15 tion.

16 (3) AUTHORITY OF COMMISSION.—

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

21 (i) to intervene in the action; and

22 (ii) upon so intervening—

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

25 (II) to file petitions for appeal.

1 (B) LIMITATION ON STATE ACTION WHILE  
2 FEDERAL ACTION IS PENDING.—If the Commis-  
3 sion has instituted a civil action for violation of  
4 this Act (referred to in this subparagraph as  
5 the “Federal action”), no State attorney gen-  
6 eral, official, or agency may bring an action  
7 under this subsection during the pendency of  
8 the Federal action against any defendant  
9 named in the complaint in the Federal action  
10 for any violation of this Act alleged in such  
11 complaint.

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

21 **SEC. 7. RULES OF CONSTRUCTION.**

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

24 (1) Prevent—

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

5 (B) compliance with the duties and report-  
6 ing requirements set forth in section 2258A of  
7 title18, United States Code.

8 (2) Restrict the ability to do any of the fol-  
9 lowing:

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

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

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

20 (D) Prevent, detect, or respond to a secu-  
21 rity incident, identity theft, fraud, harassment,  
22 or any other malicious, deceptive, or illegal ac-  
23 tivity.

1 (E) Investigate or report a person respon-  
2 sible for an activity described in subparagraph  
3 (D).

4 (3) Decrypt or ensure an ability to decrypt an  
5 encrypted communication of a user.

6 (4) Preclude the use of any form of encryption,  
7 including end-to-end encryption, for any communica-  
8 tion of a user.

9 (5) Require indefinite retention of the data of  
10 a user.

11 **SEC. 8. SEVERABILITY.**

12 If any provision of this Act or the application of this  
13 Act to any person or circumstance is held to be unconstitu-  
14 tional, the remaining provisions of this Act and the appli-  
15 cation of this Act to other persons or circumstances shall  
16 not be affected.

17 **SEC. 9. EFFECTIVE DATE.**

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