

119TH CONGRESS
2^D SESSION

S. 4159

To require large social media platform providers to create, maintain, and make available to third-party safety software providers a set of real-time application programming interfaces, through which a child or a parent may delegate permission to a third-party safety software provider to manage the online interactions, content, and account settings of such child on the large social media platform in the same manner as is available to the child, and for other purposes.

IN THE SENATE OF THE UNITED STATES

MARCH 20, 2026

Mr. HUSTED (for himself, Mrs. BRITT, and Mr. WARNER) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

A BILL

To require large social media platform providers to create, maintain, and make available to third-party safety software providers a set of real-time application programming interfaces, through which a child or a parent may delegate permission to a third-party safety software provider to manage the online interactions, content, and account settings of such child on the large social media platform in the same manner as is available to the child, 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,*

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as “Sammy’s Law”.

3 **SEC. 2. DEFINITIONS.**

4 In this Act:

5 (1) CHILD.—The term “child” means any indi-
6 vidual who—

7 (A) has not attained 17 years of age; and

8 (B) has registered an account with a large
9 social media platform.

10 (2) COMMERCE.—The term “commerce” has
11 the meaning given such term in section 4 of the
12 Federal Trade Commission Act (15 U.S.C. 44).

13 (3) COMMISSION.—The term “Commission”
14 means the Federal Trade Commission.

15 (4) COVERED NATION.—The term “covered na-
16 tion” has the meaning given such term in section
17 4872(f) of title 10, United States Code.

18 (5) LARGE SOCIAL MEDIA PLATFORM.—The
19 term “large social media platform”—

20 (A) means a service—

21 (i) provided through an internet
22 website or a mobile application;

23 (ii) the terms of service of which do
24 not prohibit the use of the service by a
25 child;

1 (iii) with any feature that enables a
2 child to share images, text, or video
3 through the internet with other users of
4 the service whom such child has met, iden-
5 tified, or become aware of solely through
6 the use of the service; and

7 (iv) that has more than 100,000,000
8 monthly global active users or generates
9 more than \$1,000,000,000 in gross rev-
10 enue per year, adjusted yearly for inflation;
11 and

12 (B) does not include—

13 (i) a service that primarily serves—

14 (I) to facilitate—

15 (aa) the sale or provision of
16 a professional service; or

17 (bb) the sale of a commer-
18 cial product; or

19 (II) to provide news or informa-
20 tion in a manner in which a user of
21 the service may not send any content
22 directly to a child through such serv-
23 ice; or

24 (ii) a service that—

1 (I) has a feature that enables a
2 user who communicates directly with
3 a child through a message (including
4 images, text, audio, or video mes-
5 sages) to add to such message other
6 users that such child may have met,
7 identified, or become aware of solely
8 through the use of the service; and

9 (II) does not have any feature
10 described in subparagraph (A)(iii).

11 (6) LARGE SOCIAL MEDIA PLATFORM PRO-
12 VIDER.—The term “large social media platform pro-
13 vider” means any person who, for commercial pur-
14 poses in or affecting commerce, provides, manages,
15 operates, owns, or controls a large social media plat-
16 form.

17 (7) PARENT.—The term “parent” means, with
18 respect to a child, the parent or legal guardian of
19 such child.

20 (8) SALE.—The term “sale”, with respect to
21 user data—

22 (A) means the exchange of user data for
23 monetary consideration; and

24 (B) does not include the disclosure of user
25 data by a third-party safety software provider

1 to a processor or service provider that processes
2 user data on behalf of the third-party safety
3 software provider.

4 (9) STATE.—The term “State” means each of
5 the 50 States, the District of Columbia, each com-
6 monwealth, territory, or possession of the United
7 States, and each federally recognized Indian Tribe.

8 (10) THIRD-PARTY SAFETY SOFTWARE PRO-
9 VIDER.—The term “third-party safety software pro-
10 vider” means any person who, for commercial pur-
11 poses in or affecting commerce—

12 (A) is authorized to interact with a rel-
13 evant large social media platform to manage
14 the online interactions, content, or account set-
15 tings of a child for the sole purpose of pro-
16 tecting the child from harm, including physical
17 or emotional harm; and

18 (B) has received such authorization from
19 the child, or in the case of a child who has not
20 attained 13 years of age, the parent of such
21 child.

22 (11) USER DATA.—The term “user data”
23 means any information reasonably necessary for a
24 user to have a profile or submit content on a large
25 social media platform (including any image, text,

1 audio, or video) that is created by or sent to a child
 2 through the account of the child on such platform,
 3 but only—

4 (A) if the information or content is created
 5 by or sent to the child while a delegation under
 6 section 3(a)(1)(A) is in effect with respect to
 7 the account; and

8 (B) during a 30-day period beginning on
 9 the date on which the information or content is
 10 created by or sent to such child.

11 **SEC. 3. PROVIDING ACCESS TO THIRD-PARTY SAFETY SOFT-**
 12 **WARE PROVIDERS.**

13 (a) OBLIGATIONS OF LARGE SOCIAL MEDIA PLAT-
 14 FORM PROVIDERS.—

15 (1) AVAILABILITY OF APPLICATION PROGRAM-
 16 MING INTERFACES.—

17 (A) IN GENERAL.—Not later than the date
 18 described in subparagraph (B), a large social
 19 media platform provider shall create, maintain,
 20 and make available to a third-party safety soft-
 21 ware provider registered with the Commission
 22 under subsection (b)(3) a set of third-party-ac-
 23 cessible real-time application programming
 24 interfaces, including any information necessary
 25 to use such interfaces, by which a child (or, in

1 the case of a child who has not attained 13
2 years of age, a parent of the child) may dele-
3 gate permission to the third-party safety soft-
4 ware provider to—

5 (i) manage any online interaction with
6 or content created by or sent to the child,
7 as well as the account settings of the child
8 on the large social media platform in the
9 same manner as is available to the child;
10 and

11 (ii) initiate a secure transfer of user
12 data from the large social media platform
13 in a commonly used and machine-readable
14 format to the third-party safety software
15 provider, where the frequency of such
16 transfers may not be limited by the large
17 social media platform provider to less than
18 once per hour.

19 (B) DATE DESCRIBED.—For purposes of
20 subparagraph (A), the date described in this
21 subparagraph is—

22 (i) in the case of a service that is a
23 large social media platform on the date of
24 enactment of this Act, 180 days after such
25 date; or

1 (ii) in the case of a service that be-
2 comes a large social media platform after
3 such date of enactment, not later than 30
4 days after the date on which such service
5 becomes a large social media platform.

6 (2) REVOCATION.—Once a child or parent
7 makes a delegation under paragraph (1)(A), the
8 large social media platform provider shall make the
9 application programming interfaces and information
10 described in such paragraph available to the relevant
11 third-party safety software provider on an ongoing
12 basis until—

13 (A) the child or a parent, as applicable, re-
14 vokes the delegation;

15 (B) the child or a parent, as applicable, re-
16 vokes or disables the registration of the account
17 of such child with the large social media plat-
18 form;

19 (C) the third-party safety software pro-
20 vider—

21 (i) rejects the delegation;

22 (ii) receives notice that—

23 (I) the parent of such child who
24 made the delegation no longer has

1 legal parental rights over such child;
2 or

3 (II) a temporary arrangement
4 has been put in place by a court or
5 legal authority regarding the custody
6 of such child; or

7 (iii) is deregistered by the Commis-
8 sion; or

9 (D) the child attains the age of 17 years
10 old.

11 (3) DATA SECURITY.—

12 (A) IN GENERAL.—A large social media
13 platform provider shall establish, implement,
14 and maintain reasonable policies, practices, and
15 procedures to protect—

16 (i) the confidentiality, integrity, and
17 accessibility of user data transferred from
18 the large social media platform provider to
19 a third-party safety software provider pur-
20 suant to a delegation under paragraph
21 (1)(A); and

22 (ii) any such user data against unau-
23 thorized access.

1 (B) SCOPE.—The policies, practices, and
2 procedures required by subparagraph (A) shall
3 be—

4 (i) consistent with state-of-the-art ad-
5 ministrative, technical, and physical safe-
6 guards for protecting transferred user
7 data; and

8 (ii) appropriate to the nature, scope,
9 and volume of such user data.

10 (4) DISCLOSURE.—In the case of a delegation
11 made by a child or a parent, as applicable, under
12 paragraph (1)(A), with respect to the account of
13 such child with a large social media platform, the
14 large social media platform provider shall—

15 (A) disclose to such child or parent, as ap-
16 plicable, such delegation;

17 (B) provide to such child or parent, as ap-
18 plicable, a summary of any user data trans-
19 ferred to a third-party safety software provider;
20 and

21 (C) update such summary as necessary to
22 reflect any change to such user data.

23 (5) LIMITATION.—Any management by a third-
24 party safety software provider pursuant to para-
25 graph (1)(A)(i) shall be limited to such management

1 that protects a child from harm, including any such
2 management related to the optimization of any pri-
3 vacy setting on an account of the child, stated user
4 age, and marketing settings for the account.

5 (6) USER CONTROL.—

6 (A) IN GENERAL.—If a large social media
7 platform uses a messaging feature or service
8 that provides security features that give a user
9 control over access to the content of any com-
10 munication of the user in a manner that ren-
11 ders the access of the large social media plat-
12 form to such content technically infeasible with-
13 out overriding such control, then the following
14 shall apply:

15 (i) The large social media platform
16 may not be required to grant a third-party
17 safety software provider access to such
18 content through a set of third-party-acces-
19 sible real-time application programming
20 interfaces under paragraph (1)(A).

21 (ii) The large social media platform,
22 upon a delegation under paragraph (1)(A),
23 shall—

24 (I) make available and maintain
25 a technical interface that enables con-

1 temporaneous transmission of such
2 communication to a third-party safety
3 software provider—

4 (aa) registered under sub-
5 section (b)(3); and

6 (bb) selected by the child or
7 parent, as applicable, as a user-
8 designated recipient;

9 (II) maintain such security fea-
10 tures without altering, bypassing, or
11 overriding such features;

12 (III) permit the communicating
13 users (and any user-designated recipi-
14 ent) to access the content through
15 such interface; and

16 (IV) not gain access to the con-
17 tent of such communication.

18 (B) RULE OF CONSTRUCTION.—Nothing in
19 this paragraph may be construed to limit the
20 obligations of a large social media platform
21 under this Act with respect to user data other
22 than the content of communications described
23 in this paragraph.

24 (b) THIRD-PARTY SAFETY SOFTWARE PROVIDERS.—

1 (1) PROTECTION OF USER DATA.—A third-
2 party safety software provider shall—

3 (A) limit any collection, maintenance, and
4 processing of user data the third-party safety
5 software provider obtains pursuant to this Act
6 to what is adequate, relevant, and reasonably
7 necessary for the purposes for which the user
8 data is collected, maintained, or processed, or
9 disclosed to a parent under subsection
10 (d)(1)(C);

11 (B) establish, implement, and maintain
12 reasonable policies, practices, and procedures
13 (that are consistent with state-of-the-art admin-
14 istrative, technical, and physical safeguards re-
15 lated to protecting transferred user data and
16 appropriate to the nature, scope, and volume of
17 such user data) to protect—

18 (i) the confidentiality, integrity, and
19 accessibility of the user data received from
20 a large social media platform pursuant to
21 this Act; and

22 (ii) the user data received from a
23 large social media platform pursuant to
24 this Act against unauthorized access; and

1 (C) upon any revocation described in sub-
2 section (a)(2), delete the user data of the child
3 within 5 days.

4 (2) PROHIBITION ON SALE.—A third-party
5 safety software provider may not sell any user data
6 collected, maintained, or processed pursuant to this
7 Act.

8 (3) REGISTRATION WITH THE COMMISSION.—A
9 third-party safety software provider shall register
10 with the Commission as a condition of accessing an
11 application programming interface and any informa-
12 tion under subsection (a). In order to complete such
13 registration, the third-party safety software provider
14 shall demonstrate the following to the satisfaction of
15 the Commission:

16 (A) The third-party safety software pro-
17 vider is not operated, directly or indirectly (in-
18 cluding through a parent company, subsidiary,
19 or affiliate), by a company operated or con-
20 trolled by a covered nation.

21 (B) Such software provider will collect,
22 process, maintain, or otherwise use any user
23 data obtained under subsection (a) for the sole
24 purpose of protecting a child from harm in ac-

1 cordance with any applicable terms of service
2 and the provisions of this Act.

3 (C) Such software provider will only dis-
4 close user data obtained under subsection (a) as
5 permitted by subsection (d).

6 (D) Such software provider will not sell,
7 disclose, process, store, transfer, or otherwise
8 make available user data obtained under this
9 Act to a government of a covered nation or to
10 a company operated or controlled by a covered
11 nation.

12 (E)(i) Such software provider will delete
13 any user data obtained under this Act as soon
14 as possible—

15 (I) but not later than 5 days after re-
16 ceiving such data from a large social media
17 platform; and

18 (II) not including any data the soft-
19 ware provider discloses under subsection
20 (d).

21 (ii) For any data disclosed under sub-
22 section (d)(1)(C), such software provider will
23 maintain such data until—

24 (I) the child or parent who made a
25 delegation under subsection (a)(1)(A), and

1 whose data is at issue, requests that the
2 third-party safety software provider delete
3 such data;

4 (II) the child attains 17 years of age;
5 or

6 (III) the third-party safety software
7 provider is deregistered by the Commis-
8 sion.

9 (iii) In the event that the child or parent
10 who made a delegation under subsection
11 (a)(1)(A) revokes the delegation, such software
12 provider will delete all applicable user data not
13 later than 15 days after the date of such rev-
14 ocation.

15 (F) Such software provider will disclose, in
16 an easy-to-understand, human-readable format,
17 to each child with respect to whose account
18 with a large social media platform the service of
19 the third-party safety software provider is oper-
20 ating and (if a parent made the delegation
21 under subsection (a)(1)(A) with respect to the
22 account) to the parent, sufficient information
23 detailing the operation of the service and what
24 information the software provider is collecting
25 to enable such child or parent, as applicable, to

1 make informed decisions regarding the use of
2 the service.

3 (G) Such software provider will disclose, in
4 an easy-to-understand format to each child or
5 parent who made a delegation under subsection
6 (a)(1)(A) notice of any material changes in how
7 the third-party safety software provider pro-
8 vides services.

9 (H) Such software provider is able to pro-
10 vide services in accordance with any applicable
11 terms of service and any relevant disclosures
12 made to any consumer, including by ensuring
13 such terms and disclosures are clear and con-
14 spicuous and are written in plain and easy-to-
15 understand English.

16 (I) Such software provider has established,
17 implemented, and maintained reasonable poli-
18 cies, practices, and procedures to protect the
19 confidentiality, integrity, and accessibility of
20 any user data collected or processed pursuant
21 to this Act and that the policies, practices, and
22 procedures are appropriate to ensure a level of
23 security appropriate to the risk to such user
24 data, the cost of implementing such policies,

1 practices, and procedures, and the nature,
2 scope, and volume of such user data.

3 (J) Such software provider assesses com-
4 pliance with applicable Federal law, including
5 the requirements of this Act.

6 (K) Such software provider is in compli-
7 ance with the requirements of this Act.

8 (4) ANNUAL AUDIT.—

9 (A) AUDIT PROCESS; AUDIT REPORT.—For
10 each year or partial year during which a third-
11 party safety software provider is registered with
12 the Commission under paragraph (3), the third-
13 party safety software provider shall retain the
14 services of a qualified independent auditing firm
15 to complete an annual audit and write an audit
16 report (which shall be exempt from disclosure
17 under section 552(b)(3) of title 5, United
18 States Code) that includes—

19 (i) a review and assessment of such
20 registration and any subsequent written re-
21 ports, including whether the third-party
22 safety software provider has remained in
23 compliance with the conditions described in
24 paragraph (3); and

1 (ii) an identification of whether the
2 third-party safety software provider has
3 made any material changes in how the
4 third-party safety software provider pro-
5 vides services, and in the event of any such
6 material changes—

7 (I) an explanation as to how such
8 changes have impacted users; and

9 (II) any information relating to
10 whether such users were notified of
11 the material change at the time the
12 material change was implemented.

13 (B) SUBMISSION TO THE COMMISSION.—

14 Not later than 30 days after the date on which
15 an audit report is written under subparagraph
16 (A), a third-party safety software provider shall
17 submit to the Commission—

18 (i) a full copy of such audit report;

19 and

20 (ii) a summary of such audit report
21 that may contain redactions to protect the
22 confidential business information and trade
23 secrets of the third-party safety software
24 provider.

1 (C) AUDIT REVIEW BY THE COMMISS-
2 SION.—The Commission shall—

3 (i) review each audit report submitted
4 by a third-party safety software provider
5 under subparagraph (B)(i) to verify com-
6 pliance with the requirements of this Act;

7 (ii) make a copy of the summary of
8 such audit report submitted under sub-
9 paragraph (B)(ii) available to the public;
10 and

11 (iii) in the event an audit required
12 under subparagraph (A) detects an un-
13 usual finding, and prior to any adverse ac-
14 tion taken by the Commission under para-
15 graph (5), direct a third-party safety soft-
16 ware provider to promptly investigate and
17 resolve the matter.

18 (5) ADDITIONAL OVERSIGHT OF THIRD-PARTY
19 SAFETY SOFTWARE PROVIDERS.—In addition to the
20 jurisdiction, powers, and duties of the Commission
21 otherwise provided under this Act and any other
22 provision of law, the Commission may take an ad-
23 verse action against a third-party safety software
24 provider, including by—

1 (A) denying registration of the third-party
2 safety software provider under paragraph (3);

3 (B) permanently deregistering the third-
4 party safety software provider; and

5 (C) suspending the registration of the
6 third-party safety software provider due to a
7 finding by the Commission of a material risk to
8 the security of the data or safety of the public,
9 including for—

10 (i) willful misconduct or gross neg-
11 ligence by the third-party safety software
12 provider;

13 (ii) a material misrepresentation made
14 by a third-party safety software provider to
15 the Commission or to any consumer;

16 (iii) failure by the third-party safety
17 software provider to comply with any re-
18 quirements of this Act or failure to operate
19 in accordance with the affirmations, asser-
20 tions, representations, or terms of any se-
21 curity review, audit, terms of services, or
22 consumer disclosures; or

23 (iv) failure by the third-party safety
24 software provider to respond to an unusual

1 finding in an annual audit completed
2 under paragraph (4).

3 (6) RIGHTS OF THIRD-PARTY SAFETY SOFT-
4 WARE PROVIDERS.—

5 (A) IN GENERAL.—In the event the Com-
6 mission takes an adverse action against a third-
7 party safety software provider under paragraph
8 (5), the Commission shall give the third-party
9 safety software provider the opportunity to—

10 (i) appeal such adverse action; and

11 (ii) remediate any deficiency described
12 in an annual audit completed under para-
13 graph (4) within 45 days (if the third-
14 party safety software provider dem-
15 onstrates the third-party safety software
16 provider has remediated any such defi-
17 ciency and has taken satisfactory action to
18 ensure such deficiency shall not reoccur),
19 except in the case of a finding of—

20 (I) willful misconduct;

21 (II) gross negligence; or

22 (III) a demonstrated history of
23 multiple failures in relation to the
24 types of material risk described in
25 paragraph (5)(C).

1 (B) EXCEPTION.—The rights described in
2 subparagraph (A) shall not prevent the Com-
3 mission from suspending the registration of a
4 third-party safety software provider to protect
5 the public from ongoing material risk for the
6 period during which the third-party safety soft-
7 ware provider is in the process of exercising
8 such rights.

9 (c) INDEMNIFICATION.—In any civil action in Fed-
10 eral or State court (other than an action brought by the
11 Commission), a large social media platform provider may
12 not be held liable for damages arising from transferring
13 user data to a third-party safety software provider under
14 subsection (a) if the large social media platform provider
15 has complied with the requirements of this Act in good
16 faith.

17 (d) USER DATA DISCLOSURE.—

18 (1) PERMITTED DISCLOSURES.—A third-party
19 safety software provider may not disclose any user
20 data obtained under subsection (a) to any other per-
21 son, except—

22 (A) pursuant to a lawful request from a
23 government body, including for law enforcement
24 purposes or for judicial or administrative pro-
25 ceedings, by means of a court order or a court-

1 ordered warrant, a subpoena or summons
2 issued by a judicial officer, or a grand jury sub-
3 poena;

4 (B) to the extent that such disclosure is re-
5 quired by law and such disclosure complies with
6 and is limited to the relevant requirements of
7 such law;

8 (C) to a child who made a delegation
9 under subsection (a)(1)(A) and whose data is at
10 issue, the parent of such child, or to a parent
11 who made such a delegation and whose child's
12 data is at issue, with such third-party safety
13 software provider making a good faith effort to
14 ensure that such disclosure includes only the
15 user data necessary for a reasonable parent to
16 understand that such child is experiencing (or
17 is at foreseeable risk to experience)—

18 (i) suicide;

19 (ii) anxiety;

20 (iii) depression;

21 (iv) an eating disorder;

22 (v) violence, including being the victim
23 of or planning to commit or facilitate as-
24 sault;

25 (vi) substance abuse;

1 (vii) fraud;

2 (viii) severe forms of trafficking in
3 persons (as defined in section 103 of the
4 Trafficking Victims Protection Act of 2000
5 (22 U.S.C. 7102));

6 (ix) sexual abuse;

7 (x) physical injury;

8 (xi) harassment;

9 (xii) sexually explicit conduct or child
10 pornography (as such terms are defined in
11 section 2256 of title 18, United States
12 Code);

13 (xiii) terrorism (as defined in section
14 140(d) of the Foreign Relations Authoriza-
15 tion Act, Fiscal Years 1988 and 1989 (22
16 U.S.C. 2656f(d))), including communica-
17 tions with or in support of a foreign ter-
18 rorist organization (as designated by the
19 Secretary of State under section 219(a) of
20 the Immigration and Nationality Act (8
21 U.S.C. 1189(a))); or

22 (xiv) the sharing of personal informa-
23 tion, limited to—

24 (I) home address;

25 (II) phone number;

1 (III) social security number; and

2 (IV) personal banking informa-
3 tion;

4 (D) in the case of a good faith determina-
5 tion that disclosure is necessary to prevent or
6 lessen a reasonably foreseeable serious and im-
7 minent threat to the health or safety of any in-
8 dividual, if the disclosure is made to a person
9 reasonably able to prevent or lessen the threat;
10 or

11 (E) to a public health authority or other
12 appropriate government authority authorized by
13 law to receive reports of child abuse or neglect.

14 (2) DISCLOSURE REPORTING.—A third-party
15 safety software provider that makes a disclosure per-
16 mitted by subparagraphs (A), (B), (D), or (E) of
17 paragraph (1) shall promptly inform the child or
18 parent who made a delegation under subsection
19 (a)(1)(A) that such a disclosure has been or will be
20 made, except if the third-party safety software pro-
21 vider—

22 (A) in the exercise of professional judg-
23 ment, determines informing such child or par-
24 ent would place such child at risk of serious
25 harm; or

1 (B) is prohibited by law (including through
2 a valid order by a court or administrative body)
3 from informing such child or parent.

4 (3) CHILD EXPLOITATION.—Nothing in this Act
5 shall be construed to relieve a third-party safety
6 software provider or a large social media platform
7 from their duty to report pursuant to section 2258A
8 of title 18, United States Code.

9 **SEC. 4. IMPLEMENTATION AND ENFORCEMENT.**

10 (a) ENFORCEMENT.—

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

17 (2) POWERS OF THE COMMISSION.—

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

1 (B) PRIVILEGES AND IMMUNITIES.—Any
2 person who violates this Act 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 (3) PRESERVATION OF AUTHORITY.—Nothing
7 in this Act may be construed to limit the authority
8 of the Commission under any other provision of law.

9 (b) COMPLIANCE ASSESSMENT.—The Commission,
10 on a biannual basis, shall assess compliance by large social
11 media platform providers with the provisions of this Act.

12 (c) COMPLAINTS.—Not later than 180 days after the
13 date of enactment of this Act, the Commission shall estab-
14 lish procedures under which a child (or the parent of such
15 child), a large social media platform provider, or a third-
16 party safety software provider may file a complaint alleg-
17 ing that a large social media platform provider or a third-
18 party safety software provider has violated this Act.

19 **SEC. 5. ONE NATIONAL STANDARD.**

20 (a) IN GENERAL.—No State or political subdivision
21 of a State may maintain, enforce, prescribe, or continue
22 in effect any law, rule, regulation, requirement, standard,
23 or other provision having the force and effect of law of
24 the State, or political subdivision of a State, related to
25 requiring large social media platform providers to create,

1 maintain, and make available to third-party safety soft-
2 ware providers a set of real-time application programming
3 interfaces for the purposes of child online safety, through
4 which a child or a parent of a child may delegate permis-
5 sion to a third-party safety software provider to manage
6 the online interactions, content, and account settings of
7 such child on a large social media platform in the same
8 manner as is available to the child.

9 (b) RULE OF CONSTRUCTION.—This section may not
10 be construed to—

11 (1) limit the enforcement of any consumer pro-
12 tection law of general applicability of a State or po-
13 litical subdivision of a State;

14 (2) preempt the applicability of State trespass,
15 contract, or tort law; or

16 (3) preempt the applicability of any State law
17 to the extent that the law relates to acts of fraud,
18 unauthorized access to personal information, or noti-
19 fication of unauthorized access to personal informa-
20 tion.

○