AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

I

119TH CONGRESS
1ST SESSION

H. R. 2657

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 or legal guardian of a child 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 on the same terms as such child, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

APRIL 3, 2025

Ms. WASSERMAN SCHULTZ (for herself, Mr. CARTER of Georgia, Ms. SCHRIER, Mrs. MILLER-MEEKS, Mr. SUOZZI, and Mr. FITZPATRICK) introduced the following bill; which was referred to the Committee on Energy and Commerce

---

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 or legal guardian of a child 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 on the same terms as such child, 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 ''Sammy's Law''.

SEC. 2. SENSE OF CONGRESS.

It is the sense of Congress that—

(1) parents and legal guardians should be empowered to use the services of third-party safety software providers to protect the children of such parents and legal guardians from certain harms on large social media platforms; and

(2) dangers like cyberbullying, human trafficking, illegal drug distribution, sexual harassment, and violence perpetrated, facilitated, or exacerbated through the use of certain large social media platforms have harmed children on such platforms.

SEC. 3. DEFINITIONS.

In this Act:

(1) CHILD.—The term ''child'' means any individual under the age of 17 years who has registered an account with a large social media platform.

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

(3) COMMISSION.—The term ''Commission'' means the Federal Trade Commission.

(4) LARGE SOCIAL MEDIA PLATFORM.—The term ''large social media platform''—

(A) means a service—

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

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

(iii) with any feature or features that enable a child to share images, text, or video through the internet with other users of the service whom such child has met, identified, or become aware of solely through the use of the service; and

(iv) that has more than 100,000,000 monthly global active users or generates more than $1,000,000,000 in gross revenue per year, adjusted yearly for inflation; and

(B) does not include—

(i) a service that primarily serves—

(I) to facilitate—

(aa) the sale or provision of professional services; or

(bb) the sale of commercial products; or

(II) to provide news or information, where the service does not offer the ability for content to be sent by a user directly to a child; or

(ii) a service that—

(I) has a feature that enables a user who communicates directly with a child through a message (including a text, audio, or video message) not otherwise available to other users of the service to add other users to that message that such child may not have otherwise met, identified, or become aware of solely through the use of the service; and

(II) does not have any feature or features described in subparagraph (A)(iii).

(5) LARGE SOCIAL MEDIA PLATFORM PROVIDER.—The term ''large social media platform provider'' means any person who, for commercial pur-

poses in or affecting commerce, provides, manages, operates, or controls a large social media platform.

(6) STATE.—The term ''State'' means each State of the United States, the District of Columbia, each commonwealth, territory, or possession of the United States, and each federally recognized Indian Tribe.

(7) THIRD-PARTY SAFETY SOFTWARE PROVIDER.—The term ''third-party safety software provider'' means any person who, for commercial purposes in or affecting commerce, is authorized by a child (if the child is 13 years of age or older) or a parent or legal guardian of a child to interact with a large social media platform to manage the online interactions, content, or account settings of such child for the sole purpose of protecting such child from harm, including physical or emotional harm.

(8) USER DATA.—The term ''user data'' means any information needed to have a profile on a large social media platform or content on a large social media platform, including images, video, audio, or text, that is created by or sent to a child on or through the account of such child with such platform, but only—

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

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

SEC. 4. PROVIDING ACCESS TO THIRD-PARTY SAFETY SOFTWARE.

(a) DUTY OF LARGE SOCIAL MEDIA PLATFORM PROVIDERS.—

(1) IN GENERAL.—Not later than 30 days after the effective date of this Act (in the case of a service that is a large social media platform on such effective date) or not later than 30 days after a service becomes a large social media platform (in the case of a service that becomes a large social media platform after such effective date), the large social media platform provider shall create, maintain, and make available to any third-party safety software provider registered with the Commission under subsection (b)(1) a set of third-party-accessible real-time application programming interfaces, including any information necessary to use such interfaces, by which a child (if the child is 13 years of age or

older) or a parent or legal guardian of a child may delegate permission to the third-party safety software provider to—

(A) manage the online interactions, content, and account settings of such child on the large social media platform on the same terms as such child; and

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

(2) REVOCATION.—Once a child or a parent or legal guardian of a child makes a delegation under paragraph (1), the large social media platform provider shall make the application programming interfaces and information described in such paragraph available to the third-party safety software provider on an ongoing basis until—

(A) the child (if the child made the delegation) or the parent or legal guardian of such child revokes the delegation;

(B) the child or a parent or legal guardian of such child revokes or disables the registration of the account of such child with the large social media platform;

(C) the third-party safety software provider rejects the delegation; or

(D) one or more of the affirmations made by the third-party safety software provider under subsection (b)(1)(A) is no longer true.

(3) SECURE TRANSFER OF USER DATA.—A large social media platform provider shall establish and implement reasonable policies, practices, and procedures regarding the secure transfer of user data pursuant to a delegation under paragraph (1) from the large social media platform to a third-party safety software provider in order to mitigate any risks related to user data.

(4) DISCLOSURE.—In the case of a delegation made by a child or a parent or legal guardian of a child under paragraph (1) with respect to the account of such child with a large social media platform, the large social media platform provider shall—

(A) disclose to such child and (if the parent or legal guardian made the delegation) the

parent or legal guardian the fact that the delegation has been made;

(B) provide to such child and (if such parent or legal guardian made the delegation) such parent or legal guardian a summary of the user data that is transferred to the third-party safety software provider; and

(C) update the summary provided under subparagraph (B) as necessary to reflect any change to the user data that is transferred to the third-party safety software provider.

(5) LIMITATION.—Any management by a third-party safety software provider of online interactions, content, and account settings of a child under this subsection shall be limited to such management that protects such child from harm, including the optimization of the privacy settings of the account, stated user age, and marketing settings of the child.

(b) THIRD-PARTY SAFETY SOFTWARE PROVIDERS.—

(1) REGISTRATION WITH COMMISSION.—A third-party safety software provider shall register with the Commission as a condition of accessing an application programming interface and any information under subsection (a). As a condition of such

registration, the third-party safety software provider shall—

(A) satisfactorily demonstrate to the Commission that the third-party safety software provider—

(i) is a company based in the United States;

(ii) is not a subsidiary of any foreign-owned company or otherwise controlled by a foreign person or persons;

(iii) will solely use any user data obtained under subsection (a) for the purpose of protecting a child from harm in accordance with any applicable terms of service and the provisions of this Act;

(iv) will only disclose user data obtained under subsection (a) as permitted by subsection (f);

(v) will process and maintain all user data obtained under subsection (a) and copies of any communications generated in relation thereto exclusively on hardware and devices located within the territorial boundaries of the United States;

(vi)(I) will delete any user data obtained under this section as soon as possible but not later than 14 days after receiving such data from the large social media platform, not including any data the third-party safety software provider discloses under subsection (f);

(II) for any data disclosed under subsection (f)(1)(C), will maintain such data until the child or a parent or legal guardian of the child who made a delegation under subsection (a) and whose data is at issue requests that the third-party safety software provider delete such data; and

(III) in the event that the child or a parent or legal guardian of the child who made a delegation under subsection (a) cancels their account with the third-party safety software provider, will delete all applicable user data no later than 30 days after the request for account cancellation has been made; and

(vii) will disclose, in an easy-to-understand, human-readable format, to each child with respect to whose account with a

large social media platform the service of the third-party safety software provider is operating and (if a parent or legal guardian of the child made the delegation under subsection (a) with respect to the account) to the parent or legal guardian, sufficient information detailing the operation of the service and what information the third-party safety software provider is collecting to enable such child and (if applicable) such parent or legal guardian to make informed decisions regarding the use of the service; and

(B) as part of the registration process, undergo a security review in such form as the Commission may proscribe but which may include requiring that a qualified independent auditing firm conduct such a review to independently verify and confirm via a written report (which shall be exempt from disclosure under section 552(b)(3) of title 5, United States Code) that the third-party safety software provider—

(i) is in compliance, or has the ability to comply, with the requirements of subparagraph (A);

(ii) is able to provide services in accordance with any applicable terms of service and any relevant disclosures made to any consumer, including whether such terms and disclosures are clear and conspicuous and are written in plain and easy-to-understand English;

(iii) has taken appropriate steps to assess potential risks and to protect the confidentiality, integrity, and security of any user data, including a determination of the adequacy of business and technology-related controls, policies, procedures, and other safeguards employed by the third-party safety software provider based on guidance issued by the Commission and other industry standards and best practices; and

(iv) assesses compliance with applicable Federal law, including the requirements of this Act.

(2) ANNUAL AUDIT.—

(A) AUDIT PROCESS; AUDIT REPORT.—For each year or partial year during which a third-party safety software provider is registered with the Commission under paragraph (1), the third-party safety software provider shall retain the services of a qualified independent auditing firm to complete an annual audit and write an audit report (which shall be exempt from disclosure under section 552(b)(3) of title 5, United States Code), and such audit report shall—

(i) include a review and assessment of the third-party safety software provider's initial security review and any subsequent written reports, including whether the third-party safety software provider has remained in compliance with the requirements described in paragraph (1)(B); and

(ii) identify whether the third-party safety software provider has made any material changes in how the third-party safety software provider provides services, and in the event of any such material changes, provide an explanation as to how such changes have impacted users.

(B) SUBMISSION TO COMMISSION.—Not later than 30 days after the date on which an audit report is written under subparagraph (A), a third-party safety software provider shall submit to the Commission—

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

(ii) a summary of such audit report that may contain redactions to protect the proprietary information and trade secrets of the third-party safety software provider.

(C) AUDIT REVIEW BY COMMISSION.—The Commission shall—

(i) review each audit report submitted by a third-party safety software provider under subparagraph (B)(i) to verify compliance;

(ii) make a copy of the summary of such audit report submitted by a third-party safety software provider under subparagraph (B)(ii) available to the public; and

(iii) in the event an audit required under subparagraph (A) detects an unusual finding, direct a third-party safety

software provider to promptly investigate and resolve the matter.

(3) ADDITIONAL AUTHORITY OF COMMISSION.—In addition to the jurisdiction, powers, and duties of the Commission otherwise provided under this Act and any other provision of law, the Commission may take an adverse action against a third-party safety software provider, including by—

(A) denying an initial registration for the third-party safety software provider under paragraph (1);

(B) permanently de-registering the third-party safety software provider; and

(C) suspending the registration of the third-party safety software provider due to an audit finding of a material risk to the security of the data or safety of the public, including for—

(i) willful misconduct or gross negligence by the third-party safety software provider;

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

(iii) failure by the third-party safety software provider to comply with any requirements of this Act or failure to operate in accordance with the affirmations, assertions, representations, or terms of any security review, audit, terms of services, or consumer disclosures;

(iv) failure by the third-party safety software provider to respond to an unusual finding in an annual audit completed under paragraph (2)(A); and

(v) failure by the third-party safety software provider to adhere to or implement guidance issued by the Commission.

(4) RIGHTS OF THIRD-PARTY SAFETY SOFTWARE PROVIDERS.—

(A) IN GENERAL.—In the event the Commission takes an adverse action against a third-party safety software provider under paragraph (3), the Commission shall give the third-party safety software provider—

(i) the opportunity to appeal the findings of the auditor or such action of the Commission; and

(ii) the opportunity to remediate any deficiencies, except in the case of a finding of—

(I) willful misconduct;

(II) gross negligence; or

(III) a demonstrated history of multiple failures in relation to the types of material risk described in paragraph (3)(C)(ii) through (3)(C)(v).

(B) EXCEPTION.—The rights described in subparagraph (A) shall not prevent the Commission from suspending the registration of a third-party safety software provider to protect the public from ongoing material risk for the period during which the third-party safety software provider is in the process of exercising the rights described in paragraph (4).

(c) AUTHENTICATION.—Not later than 180 days after the date of the enactment of this Act, the Commission shall issue guidance to facilitate the ability of a third-party safety software provider to obtain user data or access under subsection (a) in a manner that ensures that a request for user data or access on behalf of a child is a verifiable request.

(d) GUIDANCE AND CONSUMER EDUCATION.—The Commission shall—

(1) not later than 180 days after the date of the enactment of this Act, issue guidance for large social media platform providers and third-party safety software providers regarding the maintenance of reasonable safety standards to protect user data; and

(2) educate consumers regarding the rights of consumers under this Act.

(e) INDEMNIFICATION.—In any civil action in Federal or State court (other than an action brought by the Commission), a large social media platform provider may not be held liable for damages arising out of the transfer of user data to a third-party safety software provider under subsection (a), if the large social media platform provider has in good faith complied with the requirements of this Act and the guidance issued by the Commission under this Act.

(f) USER DATA DISCLOSURE.—

(1) PERMITTED DISCLOSURES.—A third-party safety software provider may not disclose any user data obtained under subsection (a) to any other person except—

(A) pursuant to a lawful request from a government body, including for law enforcement purposes or for judicial or administrative proceedings by means of a court order or a court-ordered warrant, a subpoena or summons issued by a judicial officer, or a grand jury subpoena;

(B) to the extent that such disclosure is required by law and such disclosure complies with and is limited to the relevant requirements of such law;

(C) to the child or a parent or legal guardian of the child who made a delegation under such subsection and whose data is at issue, with such third-party safety software provider making a good faith effort to ensure that such disclosure includes only the user data necessary for a reasonable parent or caregiver to understand that such child is experiencing (or is at foreseeable risk to experience) the following harms—

(i) suicide;

(ii) anxiety;

(iii) depression;

(iv) eating disorders;

(v) violence, including being the victim of or planning to commit or facilitate assault;

(vi) substance abuse;

(vii) fraud;

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

(ix) sexual abuse;

(x) physical injury;

(xi) harassment;

(xii) sexually explicit conduct or child pornography (as defined in section 2256 of title 18, United States Code);

(xiii) terrorism (as defined in section 140(d) of the Foreign Relations Authorization Act, Fiscal Years 1988 and 1989 (22 U.S.C. 2656f(d))), including communications with or in support of a foreign terrorist organization (as designated by the Secretary of State under section 219(a) of the Immigration and Nationality Act (8 U.S.C. 1189(a)));

(xiv) academic dishonesty, including cheating, plagiarism, and other forms of academic dishonesty that are intended to gain an unfair academic advantage; and

(xv) sharing personal information, limited to—

(I) home address;

(II) phone number;

(III) social security number; and

(IV) personal banking information;

(D) in the case of a reasonably foreseeable serious and imminent threat to the health or safety of any individual, if the disclosure is made to a person or persons reasonably able to prevent or lessen the threat; or

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

(2) DISCLOSURE REPORTING.—A third-party safety software provider that makes a disclosure permitted by paragraph (1)(A), (1)(B), (1)(D), or (1)(E) shall promptly inform the child with respect to whose account with a large social media platform the delegation was made under subsection (a) and

(if a parent or legal guardian of the child made the delegation) the parent or legal guardian that such a disclosure has been or will be made, except if—

(A) the third-party safety software provider, in the exercise of professional judgment, believes informing such child or parent or legal guardian would place such child at risk of serious harm; or

(B) the third-party safety software provider is prohibited by law (including a valid order by a court or administrative body) from informing such child or parent or legal guardian.

SEC. 5. IMPLEMENTATION AND ENFORCEMENT.

(a) ENFORCEMENT.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of 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 COMMISSION.—

(A) IN GENERAL.—The Commission shall enforce 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 who violates 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.).

(3) PRESERVATION OF AUTHORITY.—Nothing in this Act may be construed to limit the authority of the Commission under any other provision of law.

(b) FTC GUIDANCE.—Not later than 180 days after the date of the enactment of this Act, the Commission shall issue guidance to assist large social media platform providers and third-party safety software providers in complying with this Act.

(c) COMPLIANCE ASSESSMENT.—The Commission, on a biannual basis, shall assess compliance by large social media platform providers and third-party safety software providers with the provisions of this Act.

(d) COMPLAINTS.—The Commission shall establish procedures under which a child, or the parent or legal guardian of such child, a large social media platform provider, or a third-party safety software provider may file

a complaint alleging that a large social media platform provider or a third-party safety software provider has violated this Act.

SEC. 6. ONE NATIONAL STANDARD.

(a) IN GENERAL.—No State or political subdivision of a State may maintain, enforce, prescribe, or continue in effect any law, rule, regulation, requirement, standard, or other provision having the force and effect of law of the State, or political subdivision of a State, related to requiring 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 or legal guardian of a child may delegate permission to a third-party safety software provider to manage the online interactions, content, and account settings of such child on a large social media platform on the same terms as such child.

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

(1) limit the enforcement of any consumer protection law of a State or political subdivision of a State;

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

(3) preempt the applicability of any State law to the extent that the law relates to acts of fraud, unauthorized access to personal information, or notification of unauthorized access to personal information.

SEC. 7. EFFECTIVE DATE.

This Act shall take effect on the date on which the Commission issues guidance under section 5(b).

○