AMENDMENT IN THE NATURE OF A SUBSTITUTE TO H.R. 2657

OFFERED BY MR. CARTER OF GEORGIA

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Sammy's Law".

SEC. 2. 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) COVERED NATION.—The term "covered nation" has the meaning given such term in section 4872(f) of title 10, United States Code.

(5) 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 that enables 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 a professional service; or

(bb) the sale of a commercial product; or

(II) to provide news or information in a manner in which a user of the service may not send any content directly to a child within the platform; 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), that is not otherwise available to other users of the service, to add other users, that such child may not have otherwise met, identified, or become aware of solely through the use of the service, to such message; and

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

(6) LARGE SOCIAL MEDIA PLATFORM PROVIDER.—The term "large social media platform provider" means any person who, for commercial purposes in or affecting commerce, provides, manages, operates, or controls a large social media platform.

(7) SALE.—The term "sale"—

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

(B) does not include the disclosure of user data by a third-party safety software provider to a processor or service provider that processes user data on behalf of the third-party safety software provider.

(8) 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.

(9) 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 (if the child has not yet attained 13 years of age), to interact with a relevant large social media platform to manage the online interactions, content, or account settings of the child for the sole purpose of protecting the child from harm, including physical or emotional harm.

(10) USER DATA.—The term "user data" means any information reasonably necessary for a user to have a profile or submit content on a large social media platform (including any image, video, audio, and text that is created by or sent to a child through the account of the child on such platform) but only—

(A) if the information or content is created by or sent to the child while a delegation under section 3(a)(1) 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. 3. PROVIDING ACCESS TO THIRD-PARTY SAFETY SOFTWARE PROVIDERS.

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

(1) IN GENERAL.—Not later than 180 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), a large social media platform provider shall create, maintain, and make available to a third-party safety software provider registered with the Commission under subsection (b)(3) 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 (if the child has not yet attained 13 years of age), may delegate permission to the third-party safety software provider to—

(A) manage any online interaction with, content created by or sent to, and account settings of the child on the large social media platform on the same terms as such child; and

(B) initiate a secure transfer 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 relevant third-party safety software provider on an ongoing basis until—

(A) the child (if the child made the delegation) or a 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—

(i) rejects the delegation;

(ii) receives notice that—

(I) the parent or legal guardian of such child who made the delegation no longer has legal parental rights over such child; or

(II) a temporary arrangement has been put in place by a court or legal authority; or

(iii) is de-registered by the Commission; or

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

(3) DATA SECURITY.—

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

(i) the confidentiality, integrity, and accessibility of user data transferred from the large social media platform provider to a third-party safety software

provider pursuant to a delegation under paragraph (1); and

(ii) any such user data against unauthorized access.

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

(i) consistent with the state-of-the-art administrative, technical, and physical safeguards for protecting transferred user data; and

(ii) appropriate to the nature, scope, and volume of such 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 such delegation;

(B) provide to such child and (if such parent or legal guardian made the delegation) such parent or legal guardian a summary of any user data transferred, as the case may be, to a third-party safety software provider; and

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

(5) LIMITATION.—Any management by a third-party safety software provider pursuant to paragraph (1)(A) shall be limited to such management that protects a child from harm, including any such management related to the optimization of any privacy setting on an account of the child, stated user age, and marketing settings for the account.

(6) USER CONTROL.—

(A) IN GENERAL.—If a large social media platform uses a messaging feature or service that provides security features that give a user control over access to the content of any communication of the user in a manner that renders the access of the large social media platform to such content technically infeasible without overriding such control, then the following shall apply:

(i) The large media platform may not be required to grant a third-party safety software provider access to such content through a set of third-party-accessible real-time application programming interfaces under paragraph (1).

(ii) The large social media platform, upon a delegation under paragraph (1), shall do the following:

(I) Make available and maintain a technical interface that enables contemporaneous transmission of such communication to a third-party safety software provider—

(aa) registered under subsection (b)(3); and

(bb) selected by the child (if 13 years of age or older) or the parent or legal guardian as a user-designated recipient.

(II) Maintain such security features without altering, bypassing, or overriding such features.

(III) Permit the communicating users (and any user-designated recipient) to access the content through such interface.

(IV) Not gain access to the content of such communication.

(B) RULE OF CONSTRUCTION.—Nothing in this paragraph may be construed to limit the obligations of a large social media platform under this Act with respect to

user data other than the content of communications described in this paragraph.

(b) THIRD-PARTY SAFETY SOFTWARE PROVIDERS.—

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

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

(B) establish, implement, and maintain reasonable policies, practices, and procedures (that are consistent with state-of-the-art administrative, technical, and physical safeguards related to protecting transferred user data and appropriate to the nature, scope, and volume of such user data) to protect—

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

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

(C) upon any of the provisions listed in subsection (a)(2), delete the user data of the child within 5 days.

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

(3) 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), and as a condition of such registration, the third-party safety software provider shall satisfactorily demonstrate to the Commission the following with respect to the third-party safety software provider:

(A) Is not operated, directly or indirectly (including through a parent company, subsidiary, or affiliate), by a company operated or controlled by a covered nation.

(B) Will collect, process, maintain, or otherwise use any user data obtained under subsection (a) for the sole purpose of protecting a child from harm in accordance with any applicable terms of service and the provisions of this Act.

(C) Will only disclose user data obtained under subsection (a) as permitted by subsection (d).

(D) Will not sell, disclose, process, store, transfer, or otherwise make available user data obtained under this Act to a government of a covered nation or to a company operated or controlled by a covered nation.

(E) (i) Will delete any user data obtained under this Act as soon as possible—

(I) but not later than 5 days after receiving such data from a large social media platform; and

(II) not including any data the third-party safety software provider discloses under subsection (d).

(ii) For any data disclosed under subsection (d)(1)(C), will maintain such data until—

(I) the child or a parent or legal guardian of the child who made a delegation under subsection (a)(1) and whose data is at issue requests that the third-party safety software provider delete such data;

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

(III) the third-party safety software provider is de-registered by the Commission.

(iii) In the event that the child or a parent or legal guardian of the child who made a delegation under subsection (a)(1) revokes the delegation, will delete all applicable user data not later than 15 days after the date of such revocation.

(F) 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)(1) 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.

(G) Will disclose, in an easy-to-understand format to each child or a parent or legal guardian of the child who made a delegation under subsection (a)(1) notice of any material changes in how the third-party safety software provider provides services.

(H) Is able to provide services in accordance with any applicable terms of service and any relevant disclosures made to any consumer, including by ensuring such terms and disclosures are clear and conspicuous and are written in plain and easy-to-understand English.

(I) Has established, implemented, and maintained reasonable policies, practices, and procedures to protect the confidentiality, integrity, and accessibility of any user data collected or processed pursuant to this Act and that the policies, practices, and procedures are appropriate to the state of the art necessary to ensure a level of security appropriate to the risk to such user data, the cost of

implementing such policies, practices, and procedures, and the nature, scope, and volume of such user data.

(J) Assesses compliance with applicable Federal law, including the requirements of this Act.

(K) Is in compliance with the requirements of this Act.

(4) 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 (3), 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) that includes—

(i) a review and assessment of such registration and any subsequent written reports, including whether the third-party safety software provider has remained in compliance with the conditions described in paragraph (3); and

(ii) an identification 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—

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

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

(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 confidential business 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, and prior to any adverse action taken by the Commission under paragraph (5), direct a third-party safety software provider to promptly investigate and resolve the matter.

(5) ADDITIONAL OVERSIGHT OF THIRD PARTY SAFETY SOFTWARE PROVIDERS.—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 registration of the third-party safety software provider under paragraph (3);

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

(C) suspending the registration of the third-party safety software provider due to a finding by the Commission 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; and

(iv) failure by the third-party safety software provider to respond to an unusual finding in an annual audit completed under paragraph (4).

(6) 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 (5), the Commission shall give the third-party safety software provider—

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

(ii) the opportunity to remediate any deficiency described in an annual audit completed under paragraph (4) within 45 days (if the third-party safety software provider demonstrates the third-party safety software provider has remediated any such deficiency and has taken satisfactory action to ensure such deficiency shall not reoccur), 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 (5)(C).

(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 such rights.

(c) 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 from transferring user data to a third-party safety software provider under subsection (a) if the large social media platform provider has complied with the requirements of this Act in good faith.

(d) 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 subsection (a)(1) 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)—

(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 such terms are 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) 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 good faith determination that disclosure is necessary to prevent or lessen a reasonably foreseeable serious and imminent threat to the health or safety of any individual or group of individuals, 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 paragraphs (1)(A), (1)(B), (1)(D), or (1)(E) shall promptly inform the child or a parent or legal guardian of the child who made a delegation under subsection (a)(1) that such a disclosure has been or will be made, except if the third-party safety software provider—

(A) in the exercise of professional judgment, determines informing such child or parent or legal guardian would place such child at risk of serious harm; or

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

(3) CHILD EXPLOITATION.—A third-party safety software provider and large social media platform retains the duty to report pursuant to section 2258A of title 18, United States Code.

SEC. 4. 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) COMPLIANCE ASSESSMENT.—The Commission, on a biannual basis, shall assess compliance by large social media platform providers with the provisions of this Act.

(c) 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. 5. 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 for the purposes of child online safety, 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 general applicability 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.