118TH CONGRESS
1ST SESSION

S. 147

To require reporting of suspicious transmissions in order to assist in criminal investigations and counterintelligence activities relating to international terrorism, and for other purposes.

IN THE SENATE OF THE UNITED STATES

JANUARY 30, 2023

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

---

A BILL

To require reporting of suspicious transmissions in order to assist in criminal investigations and counterintelligence activities relating to international terrorism, 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 ''See Something, Say Something Online Act of 2023''.

SEC. 2. SENSE OF CONGRESS.

It is the sense of Congress that—

(1) section 230 of the Communications Act of 1934 (47 U.S.C. 230) (commonly known as the ''Communications Decency Act of 1996'') was never intended to provide legal protection for websites or interactive computer service providers that do nothing after becoming aware of instances of individuals or groups planning, committing, promoting, and facilitating terrorism, serious drug offenses, and violent crimes;

(2) it is not the intent of this Act to remove or strip all liability protection from websites or interactive computer service providers that are proactively working to resolve these issues; and

(3) should websites or interactive computer service providers fail to exercise due care in the implementation, filing of the suspicious transmission activity reports, and reporting of major crimes, Congress intends to look at removing liability protections under the Communications Decency Act of 1996 in its entirety.

SEC. 3. DEFINITIONS.

In this Act:

(1) DEPARTMENT.—The term ''Department'' means the Department of Justice.

(2) INTERACTIVE COMPUTER SERVICE.—The term ''interactive computer service'' has the meaning given the term in section 230 of the Communications Act of 1934 (47 U.S.C. 230).

(3) KNOWN SUSPICIOUS TRANSMISSION.—The term ''known suspicious transmission'' means any suspicious transmission that a provider of an interactive computer service—

(A) should have reasonably known to have occurred; or

(B) was notified of by a director, officer, employee, agent, interactive computer service user, or State or Federal law enforcement agency.

(4) MAJOR CRIME.—The term ''major crime'' means a Federal criminal offense—

(A) that is a crime of violence (as defined in section 16 of title 18, United States Code);

(B) relating to domestic or international terrorism (as those terms are defined in section 2331 of title 18, United States Code); or

(C) that is a serious drug offense (as defined in section 924(e) of title 18, United States Code).

(5) STAR.—The term ''STAR'' means a suspicious transmission activity report required to be submitted under section 3.

(6) SUSPICIOUS TRANSMISSION.—The term ''suspicious transmission'' means any public or private post, message, comment, tag, transaction, or any other user-generated content or transmission that commits, facilitates, incites, promotes, or otherwise assists the commission of a major crime.

SEC. 4. REPORTING OF SUSPICIOUS ACTIVITY.

(a) MANDATORY REPORTING OF SUSPICIOUS TRANSMISSIONS.—

(1) IN GENERAL.—If a provider of an interactive computer service detects a suspicious transmission, the provider, including any director, officer, employee, agent, or representative of the provider, shall submit to the Department a STAR describing the suspicious transmission in accordance with this section.

(2) REQUIREMENTS.—

(A) IN GENERAL.—Except as provided in subparagraph (C), a STAR required to be submitted under paragraph (1) shall be submitted not later than 30 days after the date on which

the provider of an interactive computer service—

(i) initially detects the suspicious transmission; or

(ii) is alerted to the suspicious transmission on the platform of such service.

(B) IMMEDIATE NOTIFICATION.—In the case of a suspicious transmission that requires immediate attention, such as an active sale or solicitation of sale of drugs or a threat of terrorist activity, the provider of an interactive computer service shall—

(i) immediately notify, by telephone, an appropriate law enforcement authority; and

(ii) file a STAR in accordance with this section.

(C) DELAY OF SUBMISSION.—The 30-day period described in subparagraph (A) may be extended by 30 days if the provider of an interactive computer service provides a valid reason to the agency designated or established under subsection (b)(2).

(b) REPORTING PROCESS.—

(1) IN GENERAL.—The Attorney General shall establish a process by which a provider of an interactive computer service may submit STARs under this section.

(2) DESIGNATED AGENCY.—

(A) IN GENERAL.—In carrying out this section, the Attorney General shall designate an agency within the Department, or, if the Attorney General determines appropriate, establish a new agency within the Department, to which STARs should be submitted under subsection (a).

(B) CONSUMER REPORTING.—The agency designated or established under subparagraph (A) shall establish a centralized online resource, which may be used by individual members of the public to report suspicious activity related to major crimes for investigation by the appropriate law enforcement or regulatory agency.

(C) COOPERATION WITH INDUSTRY.—The agency designated or established under subparagraph (A)—

(i) may conduct training for enforcement agencies and for providers of inter-

active computer services on how to cooperate in reporting suspicious activity;

(ii) may develop relationships for promotion of reporting mechanisms and resources available on the centralized online resource required to be established under subparagraph (B); and

(iii) shall coordinate with the National White Collar Crime Center to convene experts to design training programs for State and local law enforcement agencies, which may include using social media, online ads, paid placements, and partnering with expert non-profit organizations to promote awareness and engage with the public.

(c) CONTENTS.—Each STAR submitted under this section shall contain, at a minimum—

(1) the name, location, and other such identification information as submitted by the user to the provider of the interactive computer service;

(2) the date and nature of the post, message, comment, tag, transaction, or other user-generated content or transmission detected for suspicious activity such as time, origin, and destination; and

(3) any relevant text, information, and metadata related to the suspicious transmission.

(d) RETENTION OF RECORDS AND NONDISCLOSURE.—

(1) RETENTION OF RECORDS.—Each provider of an interactive computer service shall—

(A) maintain a copy of any STAR submitted under this section and the original record equivalent of any supporting documentation for the 5-year period beginning on the date on which the STAR was submitted;

(B) make all supporting documentation available to the Department and any appropriate law enforcement agencies upon request; and

(C) not later than 30 days after the date on which the provider submits a STAR under this section, take action against the website or account reported unless the provider receives a notification from a law enforcement agency that the website or account should remain open.

(2) NONDISCLOSURE.—Except as otherwise prescribed by the Attorney General, no provider of an interactive computer service, or officer, director, employee, or agent of such a provider, subject to an

order under subsection (a) may disclose the existence of, or terms of, the order to any person.

(e) DISCLOSURE TO OTHER AGENCIES.—

(1) IN GENERAL.—Subject to paragraph (2), the Attorney General shall—

(A) ensure that STARs submitted under this section and reports from the public submitted under subsection (b)(2)(B) are referred as necessary to the appropriate Federal, State, or local law enforcement or regulatory agency;

(B) make information in a STAR submitted under this section available to an agency, including any State financial institutions supervisory agency or United States intelligence agency, upon request of the head of the agency; and

(C) develop a strategy to disseminate relevant information in a STAR submitted under this section in a timely manner to other law enforcement and government agencies, as appropriate, and coordinate with relevant nongovernmental entities, such as the National Center for Missing and Exploited Children.

(2) LIMITATION.—The Attorney General may only make a STAR available under paragraph (1) for law enforcement purposes.

(f) COMPLIANCE.—Any provider of an interactive computer service that fails to report a known suspicious transmission shall not be immune from civil or criminal liability for such transmission under section 230(c) of the Communications Act of 1934 (47 U.S.C. 230(c)).

(g) APPLICATION OF FOIA.—Any STAR submitted under this section, and any information therein or record thereof, shall be exempt from disclosure under section 552 of title 5, United States Code, or any similar State, local, Tribal, or territorial law.

(h) RULEMAKING AUTHORITY.—Not later than 180 days after the date of enactment of this Act, the Attorney General shall promulgate regulations to carry out this section.

(i) REPORT.—Not later than 180 days after the date of enactment of this Act, the Attorney General shall submit to Congress a report describing the plan of the Department for implementation of this Act, including a breakdown of the costs associated with implementation.

(j) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Attorney General such sums as may be necessary to carry out this Act.

SEC. 5. AMENDMENT TO COMMUNICATIONS DECENCY ACT.

Section 230(e) of the Communications Act of 1934 (47 U.S.C. 230(e)) is amended by adding at the end the following:

''(6) LOSS OF LIABILITY PROTECTION FOR FAILURE TO SUBMIT SUSPICIOUS TRANSMISSION ACTIVITY REPORT.—

''(A) DEFINITIONS.—In this paragraph, the terms 'known suspicious transmission' and 'suspicious transmission' have the meanings given those terms in section 3 of the See Something, Say Something Online Act of 2023.

''(B) REQUIREMENT.—Any provider of an interactive computer service shall take reasonable steps to prevent or address unlawful users of the service through the reporting of suspicious transmissions.

''(C) FAILURE TO COMPLY.—Any provider of an interactive computer service that fails to report a known suspicious transmission may be held liable as a publisher for the related suspicious transmission.

''(D) RULE OF CONSTRUCTION.—Nothing in this paragraph shall be construed to impair or limit any claim or cause of action arising from the failure of a provider of an interactive

computer service to report a suspicious transmission.''.

○