

116TH CONGRESS
2D SESSION

S. 4758

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

SEPTEMBER 29, 2020

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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “See Something, Say
5 Something Online Act of 2020”.

6 **SEC. 2. SENSE OF CONGRESS.**

7 It is the sense of Congress that—

1 (1) section 230 of the Communications Act of
2 1934 (47 U.S.C. 230) (commonly known as the
3 “Communications Decency Act of 1996”) was never
4 intended to provide legal protection for websites or
5 interactive computer services that do nothing after
6 becoming aware of instances of individuals or groups
7 planning, committing, promoting, and facilitating
8 terrorism, serious drug offenses, and violent crimes;

9 (2) it is not the intent of this Act to remove or
10 strip all liability protection from websites or inter-
11 active computer services that are proactively working
12 to resolve these issues; and

13 (3) should websites or interactive service pro-
14 viders fail to exercise due care in the implementa-
15 tion, filing of the suspicious transmission activity re-
16 ports, and reporting of major crimes, Congress in-
17 tends to look at removing liability protections under
18 the Communications Decency Act of 1996 in its en-
19 tirety.

20 **SEC. 3. DEFINITIONS.**

21 In this Act:

22 (1) DEPARTMENT.—The term “Department”
23 means the Department of Justice.

24 (2) INTERACTIVE COMPUTER SERVICE.—The
25 term “interactive computer service” has the meaning

1 given the term in section 230 of the Communica-
2 tions Act of 1934 (47 U.S.C. 230).

3 (3) KNOWN SUSPICIOUS TRANSMISSION.—The
4 term “known suspicious transmission” is any sus-
5 picious transmission that an interactive computer
6 service should have reasonably known to have oc-
7 curred or have been notified of by a director, officer,
8 employee, agent, interactive computer service user,
9 or State or Federal law enforcement agency.

10 (4) MAJOR CRIME.—The term “major crime”
11 means a Federal criminal offense—

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

14 (B) relating to domestic or international
15 terrorism (as those terms are defined in section
16 2331 of title 18, United States Code); and

17 (C) that is a serious drug offense (as de-
18 fined in section 924(e) of title 18, United
19 States Code).

20 (5) STAR.—The term “STAR” means a sus-
21 picious transmission activity report required to be
22 submitted under section 3.

23 (6) SUSPICIOUS TRANSMISSION.—The term
24 “suspicious transmission” means any public or pri-
25 vate post, message, comment, tag, transaction, or

1 any other user-generated content or transmission
2 that commits, facilitates, incites, promotes, or other-
3 wise assists the commission of a major crime.

4 **SEC. 4. REPORTING OF SUSPICIOUS ACTIVITY.**

5 (a) **MANDATORY REPORTING OF SUSPICIOUS TRANS-**
6 **MISSIONS.—**

7 (1) **IN GENERAL.—**If a provider of an inter-
8 active computer service detects a suspicious trans-
9 mission, the interactive computer service, including
10 any director, officer, employee, agent, or representa-
11 tive of such provider, shall submit to the Depart-
12 ment a STAR describing the suspicious transmission
13 in accordance with this section.

14 (2) **REQUIREMENTS.—**

15 (A) **IN GENERAL.—**Except as provided in
16 subparagraph (C), a STAR required to be sub-
17 mitted under paragraph (1) shall be submitted
18 not later than 30 days after the date on which
19 the interactive computer service—

20 (i) initially detects the suspicious
21 transmission; or

22 (ii) is alerted to the suspicious trans-
23 mission on the platform of such service.

24 (B) **IMMEDIATE NOTIFICATION.—**In the
25 case of a suspicious transmission that requires

1 immediate attention, such as an active sale or
2 solicitation of sale of drugs or a threat of ter-
3 rorist activity, the provider of an interactive
4 computer service shall—

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

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

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

16 (b) REPORTING PROCESS.—

17 (1) IN GENERAL.—The Attorney General shall
18 establish a process by which a provider of an inter-
19 active computer service may submit STARs under
20 this section.

21 (2) DESIGNATED AGENCY.—

22 (A) IN GENERAL.—In carrying out this
23 section, the Attorney General shall designate an
24 agency within the Department, or, if the Attor-
25 ney General determines appropriate, establish a

1 new agency within the Department, to which
2 STARS should be submitted under subsection
3 (a).

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

11 (C) COOPERATION WITH INDUSTRY.—The
12 agency designated or established under sub-
13 paragraph (A)—

14 (i) may conduct training for enforce-
15 ment agencies and for providers of inter-
16 active computer services on how to cooper-
17 ate in reporting suspicious activity;

18 (ii) may develop relationships for pro-
19 motion of reporting mechanisms and re-
20 sources available on the centralized online
21 resource required to be established under
22 subparagraph (B); and

23 (iii) shall coordinate with the National
24 White Collar Crime Center to convene ex-
25 perts to design training programs for State

1 and local law enforcement agencies, which
2 may include using social media, online ads,
3 paid placements, and partnering with ex-
4 pert nonprofit organizations to promote
5 awareness and engage with the public.

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

8 (1) the name, location, and other such identi-
9 fication information as submitted by the user to the
10 provider of the interactive computer service;

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

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

17 (d) RETENTION OF RECORDS AND NONDISCLO-
18 SURE.—

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

21 (A) maintain a copy of any STAR sub-
22 mitted under this section and the original
23 record equivalent of any supporting documenta-
24 tion for the 5-year period beginning on the date
25 on which the STAR was submitted;

1 (B) make all supporting documentation
2 available to the Department and any appro-
3 priate law enforcement agencies upon request;
4 and

5 (C) not later than 30 days after the date
6 on which the interactive computer service sub-
7 mits a STAR under this section, take action
8 against the website or account reported unless
9 the provider of an interactive computer service
10 receives a notification from a law enforcement
11 agency that the website or account should re-
12 main open.

13 (2) NONDISCLOSURE.—Except as otherwise
14 prescribed by the Attorney General, no provider of
15 an interactive computer service, or officer, director,
16 employee, or agent of such a provider, subject to an
17 order under subsection (a) may disclose the exist-
18 ence of, or terms of, the order to any person.

19 (e) DISCLOSURE TO OTHER AGENCIES.—

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

22 (A) ensure that STARS submitted under
23 this section and reports from the public sub-
24 mitted under subsection (b)(2)(B) are referred

1 as necessary to the appropriate Federal, State,
2 or local law enforcement or regulatory agency;

3 (B) make information in a STAR sub-
4 mitted under this section available to an agen-
5 cy, including any State financial institutions su-
6 pervisory agency or United States intelligence
7 agency, upon request of the head of the agency;
8 and

9 (C) develop a strategy to disseminate rel-
10 evant information in a STAR submitted under
11 this section in a timely manner to other law en-
12 forcement and government agencies, as appro-
13 priate, and coordinate with relevant nongovern-
14 mental entities, such as the National Center for
15 Missing and Exploited Children.

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

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

24 (g) APPLICATION OF FOIA.—Any STAR submitted
25 under this section, and any information therein or record

1 thereof, shall be exempt from disclosure under section 552
2 of title 5, United States Code, or any similar State, local,
3 Tribal, or territorial law.

4 (h) RULEMAKING AUTHORITY.—Not later than 180
5 days after the date of enactment of this Act, the Attorney
6 General shall promulgate regulations to carry out this sec-
7 tion.

8 (i) REPORT.—Not later than 180 days after the date
9 of enactment of this Act, the Attorney General shall sub-
10 mit to Congress a report describing the plan of the De-
11 partment for implementation of this Act, including a
12 breakdown of the costs associated with implementation.

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

16 **SEC. 5. AMENDMENT TO COMMUNICATIONS DECENCY ACT.**

17 Section 230(e) of the Communications Act of 1934
18 (47 U.S.C. 230(e)) is amended by adding at the end the
19 following:

20 “(6) LOSS OF LIABILITY PROTECTION FOR
21 FAILURE TO SUBMIT SUSPICIOUS TRANSMISSION AC-
22 TIVITY REPORT.—

23 “(A) REQUIREMENT.—Any provider of an
24 interactive computer service shall take reason-
25 able steps to prevent or address unlawful users

1 of the service through the reporting of sus-
2 picious transmissions.

3 “(B) FAILURE TO COMPLY.—Any provider
4 of an interactive computer service that fails to
5 report a known suspicious transmission may be
6 held liable as a publisher for the related sus-
7 picious transmission.

8 “(C) RULE OF CONSTRUCTION.—Nothing
9 in this paragraph shall be construed to impair
10 or limit any claim or cause of action arising
11 from the failure of a provider of an interactive
12 computer service to report a suspicious trans-
13 mission.”.

○