

116TH CONGRESS
1ST SESSION

S. 2889

To safeguard data of Americans from foreign governments that pose risks to national security by imposing data security requirements and strengthening review of foreign investments, and for other purposes.

IN THE SENATE OF THE UNITED STATES

NOVEMBER 18, 2019

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

A BILL

To safeguard data of Americans from foreign governments that pose risks to national security by imposing data security requirements and strengthening review of foreign investments, 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 “National Security and
5 Personal Data Protection Act of 2019”.

6 **SEC. 2. DEFINITIONS.**

7 In this Act:

1 (1) COMMISSION.—The term “Commission”
2 means the Federal Trade Commission.

3 (2) COUNTRY OF CONCERN.—

4 (A) IN GENERAL.—Subject to subpara-
5 graph (B)(iii), the term “country of concern”
6 means—

7 (i) the People’s Republic of China;

8 (ii) the Russian Federation; and

9 (iii) any other country designated by
10 the Secretary of State as being of concern
11 with respect to the protection of data pri-
12 vacy and security.

13 (B) DESIGNATION OF COUNTRIES OF CON-
14 CERN.—Not later than 1 year after the date of
15 enactment of this Act, and annually thereafter,
16 the Secretary of State shall—

17 (i) review the status of data privacy
18 and security requirements (including by re-
19 viewing laws, policies, practices, and regu-
20 lations related to data privacy and secu-
21 rity) in each foreign country to deter-
22 mine—

23 (I) whether it would pose a sub-
24 stantial risk to the national security
25 of the United States if the govern-

1 ment of such country gained access to
2 the user data of citizens and residents
3 of the United States; and

4 (II) whether there is a substan-
5 tial risk that the government of such
6 country will, in a manner that fails to
7 afford similar respect for civil liberties
8 and privacy as the Constitution and
9 laws of the United States, obtain user
10 data from companies that collect user
11 data;

12 (ii) designate each country that meets
13 the criteria of clause (i) as a country of
14 concern; and

15 (iii) remove the designation from any
16 country that was previously designated a
17 country of concern (regardless of whether
18 such designation was pursuant to clause (i)
19 or (ii) of subparagraph (A) or was made
20 by the Secretary of State pursuant to
21 clause (iii) of such subparagraph) if the
22 country—

23 (I) no longer meets the criteria of
24 clause (i); and

1 (II) is not at substantial risk of
2 meeting such criteria.

3 (C) REGULATIONS.—Not later than 90
4 days after the date of the enactment of this
5 Act, the Secretary of State shall prescribe regu-
6 lations—

7 (i) establishing a process for a covered
8 technology company or country of concern
9 to petition the Secretary to remove the
10 country of concern designation from a
11 country that was designated as such pur-
12 suant to subparagraph (B)(ii); and

13 (ii) setting forth the procedures and
14 criteria the Secretary will use in identi-
15 fying or removing countries under subpara-
16 graphs (A)(iii) or (B)(iii).

17 (3) COVERED TECHNOLOGY COMPANY.—The
18 term “covered technology company” means an entity
19 that provides an online data-based service such as a
20 website or internet application in or affecting inter-
21 state or foreign commerce and—

22 (A) is organized under the laws of a coun-
23 try of concern;

24 (B) in which foreign persons that are na-
25 tionals of, or companies that are organized

1 under the laws of, countries of concern have a
2 plurality or controlling equity interest;

3 (C) is a subsidiary company of an entity
4 described in subparagraph (A) or (B); or

5 (D) is otherwise subject to the jurisdiction
6 of a country of concern in a manner that allows
7 the country of concern to obtain the user data
8 of citizens and residents of the United States
9 without similar respect for civil liberties and
10 privacy as provided under the Constitution and
11 laws of the United States.

12 (4) FACIAL RECOGNITION TECHNOLOGY.—The
13 term “facial recognition technology” means tech-
14 nology that analyzes facial features in still or video
15 images and is used to identify, or facilitate identi-
16 fication of, an individual using facial physical char-
17 acteristics.

18 (5) TARGETED ADVERTISING.—

19 (A) IN GENERAL.—The term “targeted ad-
20 vertising” means a form of advertising where
21 advertisements are displayed to a user based on
22 the user’s traits, information from a profile
23 about the user that is created for the purpose
24 of selling advertisements, or the user’s previous
25 online or offline behavior.

1 (B) LIMITATION.—Such term shall not in-
2 clude advertising chosen because of the context
3 of the internet service, such as—

4 (i) advertising that is directed to a
5 user based on the content of the website,
6 online service, online application, or mobile
7 application that the user is connected to;
8 or

9 (ii) advertising that is directed to a
10 user by the operator of a website, online
11 service, online application, or mobile appli-
12 cation based on the search terms that the
13 user used to arrive at such website, service,
14 or application.

15 (6) USER DATA.—The term “user data” means
16 any information obtained by an entity that provides
17 a data-based service such as a website or internet
18 application that identifies, relates to, describes, is
19 capable of being associated with, or could reasonably
20 be linked with an individual who is a citizen or resi-
21 dent of the United States without regard to whether
22 such information is directly submitted by the indi-
23 vidual to the entity, is derived by the entity from the
24 observed activity of the individual, or is obtained by
25 the entity by any other means.

1 **SEC. 3. DATA SECURITY REQUIREMENTS FOR COVERED**
2 **TECHNOLOGY COMPANIES.**

3 (a) IN GENERAL.—The following requirements shall
4 apply to a covered technology company:

5 (1) MINIMAL COLLECTION OF DATA.—The com-
6 pany shall not collect any more user data than is
7 necessary for the operation of the website, service, or
8 application of the company.

9 (2) PROHIBITION ON SECONDARY USES.—The
10 company shall not use any user data collected under
11 paragraph (1) for any purpose that is secondary to
12 the operation of the website, service, or application
13 of the company, including providing targeted adver-
14 tising, unnecessarily sharing such data with a third
15 party, or unnecessarily facilitating facial recognition
16 technology.

17 (3) RIGHT TO VIEW AND DELETE DATA.—The
18 company shall allow an individual to—

19 (A) view any user data held by the com-
20 pany that relates to the individual; and

21 (B) permanently delete any user data held
22 by the company that has been collected, directly
23 or indirectly, from the individual.

24 (4) PROHIBITION ON TRANSFER TO COUNTRIES
25 OF CONCERN.—The company shall not transfer any
26 user data or information needed to decipher that

1 data, such as encryption keys, to any country of con-
2 cern (including indirectly through a third country
3 that is not a country of concern).

4 (5) DATA STORAGE REQUIREMENT.—The com-
5 pany shall not store any user data collected from
6 citizens or residents of the United States or informa-
7 tion needed to decipher that data, such as
8 encryption keys, on a server or other data storage
9 device that is located outside of the United States or
10 a country that maintains an agreement with the
11 United States to share data with law enforcement
12 agencies through a process established by law.

13 (6) REPORTING REQUIREMENT.—Not less fre-
14 quently than annually, the chief executive officer or
15 equivalent officer of the company shall submit,
16 under penalty of perjury, a report to the Commis-
17 sion, the Attorney General of the United States, and
18 the Attorney General of each State certifying compli-
19 ance with the requirements of this section.

20 (b) EXCEPTIONS.—

21 (1) EXCEPTION FOR LAW ENFORCEMENT AND
22 MILITARY.—The requirements of paragraphs (1)
23 through (4) of subsection (a) shall not apply where
24 data is collected, used, retained, stored, or shared by
25 a covered technology company solely for the purpose

1 of assisting a law enforcement or military agency
2 that is not affiliated with a country of concern.

3 (2) TRANSFER OF SHARED CONTENT.—The re-
4 quirements of paragraph (4) and (5) of subsection
5 (a) shall not apply to user data that is content pro-
6 duced by a user for the purpose of sharing with
7 other users (such as social media posts, emails, or
8 data related to a transaction involving the user) or
9 information needed to decipher that data provided
10 that the transfer and any storage necessary to enact
11 the transfer is conducted solely to carry out the
12 user’s intent to share such data with individual
13 users in other countries and that necessary storage
14 occurs only on the intended recipient’s individual de-
15 vice.

16 (c) EFFECTIVE DATE.—The requirements of this sec-
17 tion shall take effect 90 days after the date of enactment
18 of this Act.

19 **SEC. 4. DATA SECURITY REQUIREMENTS FOR OTHER TECH-**
20 **NOLOGY COMPANIES.**

21 (a) IN GENERAL.—The following requirements shall
22 apply to any company operating in or affecting interstate
23 or foreign commerce that provides a data-based service
24 such as a website or internet application but is not a cov-
25 ered technology company:

1 (1) PROHIBITION ON TRANSFER TO COUNTRIES
2 OF CONCERN.—The company shall not transfer any
3 user data collected from an individual in the United
4 States or information needed to decipher that data,
5 such as encryption keys, to any country of concern
6 (including indirectly through a third country that is
7 not a country of concern).

8 (2) PROHIBITION ON STORING DATA IN COUN-
9 TRIES OF CONCERN.—The company shall not store
10 any user data collected from an individual in the
11 United States or information needed to decipher
12 that data, such as encryption keys, on a server or
13 other data storage device that is located in any
14 country of concern.

15 (b) EXCEPTIONS.—

16 (1) EXCEPTION FOR LAW ENFORCEMENT AND
17 MILITARY.—The requirements of subsection (a) shall
18 not apply where data is collected, used, retained,
19 stored, or shared by a covered technology company
20 solely for the purpose of assisting a law enforcement
21 or military agency that is not affiliated with a coun-
22 try of concern.

23 (2) TRANSFER OF SHARED CONTENT.—The re-
24 quirements of subsection (a) shall not apply to user
25 data that is content produced by a user for the pur-

pose of sharing with other users (such as social media posts, emails, or data related to a transaction involving the user) or information needed to decipher that data provided that the transfer and any storage necessary to enact the transfer is conducted solely to carry out the user's intent to share such data with individual users in other countries and that necessary storage occurs only on the intended recipient's individual device.

(c) EFFECTIVE DATE.—The requirements of this section shall take effect 90 days after the date of enactment of this Act.

SEC. 5. ENFORCEMENT OF DATA SECURITY REQUIREMENTS.

(a) ENFORCEMENT BY THE COMMISSION.—

(1) IN GENERAL.—Except as otherwise provided, sections 3 and 4 shall be enforced by the Commission under the Federal Trade Commission Act (15 U.S.C. 41 et seq.).

(2) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of section 3 or 4 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)).

1 (3) ACTIONS BY THE COMMISSION.—Except as
2 otherwise provided, the Commission shall prevent
3 any person from violating section 3 or 4 in the same
4 manner, by the same means, and with the same ju-
5 risdiction, powers, and duties as though all applica-
6 ble terms and provisions of the Federal Trade Com-
7 mission Act (15 U.S.C. 41 et seq.) were incor-
8 porated into and made a part of this Act, and any
9 person who violates such section shall be subject to
10 the penalties and entitled to the privileges and im-
11 munities provided in the Federal Trade Commission
12 Act.

13 (4) AUTHORITY PRESERVED.—Nothing in this
14 Act shall be construed to limit the authority of the
15 Commission under any other provision of law.

16 (b) CRIMINAL PENALTY.—

17 (1) OFFENSE.—It shall be unlawful to know-
18 ingly cause a technology company to violate a re-
19 quirement of section 3 or 4.

20 (2) PENALTY.—Any person who violates para-
21 graph (1) shall be imprisoned for not more than 5
22 years, fined under title 18, United States Code, or
23 both.

24 (c) ENFORCEMENT BY STATE ATTORNEYS GEN-
25 ERAL.—

1 (1) IN GENERAL.—

2 (A) CIVIL ACTIONS.—In any case in which
3 the attorney general of a State has reason to
4 believe that an interest of the residents of that
5 State has been or is threatened or adversely af-
6 fected by the engagement of any person in a
7 practice that violates section 3 or 4, the State,
8 as *parens patriae*, may bring a civil action on
9 behalf of the residents of the State in a district
10 court of the United States or a State court of
11 appropriate jurisdiction to—

12 (i) enjoin that practice;

13 (ii) enforce compliance with such sec-
14 tion;

15 (iii) on behalf of residents of the
16 State, obtain damages, statutory damages,
17 restitution, or other compensation, each of
18 which shall be distributed in accordance
19 with State law; or

20 (iv) obtain such other relief as the
21 court may consider to be appropriate.

22 (B) NOTICE.—

23 (i) IN GENERAL.—Before filing an ac-
24 tion under subparagraph (A), the attorney

1 general of the State involved shall provide
2 to the Commission—

3 (I) written notice of that action;

4 and

5 (II) a copy of the complaint for
6 that action.

7 (ii) EXEMPTION.—

8 (I) IN GENERAL.—Clause (i)
9 shall not apply with respect to the fil-
10 ing of an action by an attorney gen-
11 eral of a State under this paragraph
12 if the attorney general of the State
13 determines that it is not feasible to
14 provide the notice described in that
15 clause before the filing of the action.

16 (II) NOTIFICATION.—In an ac-
17 tion described in subclause (I), the at-
18 torney general of a State shall provide
19 notice and a copy of the complaint to
20 the Commission at the same time as
21 the attorney general files the action.

22 (2) INTERVENTION.—

23 (A) IN GENERAL.—On receiving notice
24 under paragraph (1)(B), the Commission shall

1 have the right to intervene in the action that is
2 the subject of the notice.

3 (B) EFFECT OF INTERVENTION.—If the
4 Commission intervenes in an action under para-
5 graph (1), it shall have the right—

6 (i) to be heard with respect to any
7 matter that arises in that action; and

8 (ii) to file a petition for appeal.

9 (3) CONSTRUCTION.—For purposes of bringing
10 any civil action under paragraph (1), nothing in this
11 Act shall be construed to prevent an attorney gen-
12 eral of a State from exercising the powers conferred
13 on the attorney general by the laws of that State
14 to—

15 (A) conduct investigations;

16 (B) administer oaths or affirmations; or

17 (C) compel the attendance of witnesses or
18 the production of documentary and other evi-
19 dence.

20 (4) ACTIONS BY THE COMMISSION.—In any
21 case in which an action is instituted by or on behalf
22 of the Commission for violation of section 3 or 4, no
23 State may, during the pendency of that action, insti-
24 tute an action under paragraph (1) against any de-
25 fendant named in the complaint in the action insti-

1 tuted by or on behalf of the Commission for that
2 violation.

3 (5) VENUE; SERVICE OF PROCESS.—

4 (A) VENUE.—Any action brought under
5 paragraph (1) may be brought in—

6 (i) the district court of the United
7 States that meets applicable requirements
8 relating to venue under section 1391 of
9 title 28, United States Code; or

10 (ii) a State court of competent juris-
11 diction.

12 (B) SERVICE OF PROCESS.—In an action
13 brought under paragraph (1) in a district court
14 of the United States, process may be served
15 wherever defendant—

16 (i) is an inhabitant; or

17 (ii) may be found.

18 (d) PRIVATE RIGHT OF ACTION.—

19 (1) IN GENERAL.—Any individual who suffers
20 injury as a result of an act, practice, or omission of
21 a covered technology company that violates section 3
22 may bring a civil action against such company in
23 any court of competent jurisdiction.

24 (2) RELIEF.—In a civil action brought under
25 paragraph (1) in which the plaintiff prevails, the

1 court may award such plaintiff up to \$1,000 for
 2 each day that such plaintiff was affected by a viola-
 3 tion of section 3 (up to a maximum of \$15,000 per
 4 each such violation per plaintiff).

5 **SEC. 6. REQUIREMENT FOR APPROVAL OF COMMITTEE ON**
 6 **FOREIGN INVESTMENT IN THE UNITED**
 7 **STATES OF CERTAIN TRANSACTIONS.**

8 Section 721(b) of the Defense Production Act of
 9 1950 (50 U.S.C. 4565(b)) is amended by adding at the
 10 end the following:

11 “(9) APPROVAL REQUIRED FOR CERTAIN
 12 TRANSACTIONS.—

13 “(A) IN GENERAL.—A covered transaction
 14 described in subparagraph (C) is prohibited un-
 15 less the Committee—

16 “(i) reviews the transaction under this
 17 subsection; and

18 “(ii) determines that the transaction
 19 does not pose a risk to the national secu-
 20 rity of the United States.

21 “(B) MITIGATION.—The Committee, or a
 22 lead agency on behalf of the Committee, may
 23 negotiate, enter into or impose, and enforce an
 24 agreement or condition under subsection (1)(3)
 25 with any party to a covered transaction de-

1 scribed in subparagraph (C) to mitigate any
2 risk to the national security of the United
3 States that arises as a result of the covered
4 transaction.

5 “(C) COVERED TRANSACTION DE-
6 SCRIBED.—A covered transaction described in
7 this subparagraph is a transaction that could
8 result in foreign control of a United States
9 company—

10 “(i) that collects, sells, buys, or proc-
11 esses user data (as defined in section 2 of
12 the National Security and Personal Data
13 Protection Act of 2019) and whose busi-
14 ness consists substantially more of trans-
15 ferring data than manufacturing, deliv-
16 ering, repairing, or servicing physical goods
17 or providing physical services; or

18 “(ii) that operates a social media plat-
19 form or website.”.

○