Title: 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.

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 "National Security and Personal Data Protection Act of 2019".

SEC. 2. DEFINITIONS.

In this Act:

(1) COMMISSION.—The term "Commission" means the Federal Trade Commission.

(2) COUNTRY OF CONCERN.—

(A) IN GENERAL.—Subject to subparagraph (B)(iii), the term "country of concern" means—

(i) the People's Republic of China;

(ii) the Russian Federation; and

(iii) any other country designated by the Secretary of State as being of concern with respect to the protection of data privacy and security.

(B) DESIGNATION OF COUNTRIES OF CONCERN.—Not later than 1 year after the date of enactment of this Act, and annually thereafter, the Secretary of State shall—

(i) review the status of data privacy and security requirements (including by reviewing laws, policies, practices, and regulations related to data privacy and security) in each foreign country to determine—

(I) whether it would pose a substantial risk to the national security of the United States if the government of such country gained access to the user data of citizens and residents of the United States; and

(II) whether there is a substantial risk that the government of such country will, in a manner that fails to afford similar respect for civil liberties and privacy as the Constitution and laws of the United States, obtain user data from companies that collect user data;

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

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

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

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

(C) REGULATIONS.—Not later than 90 days after the date of the enactment of this Act, the Secretary of State shall prescribe regulations—

(i) establishing a process for a covered technology company or country of concern to petition the Secretary to remove the country of concern designation from a country that was designated as such pursuant to subparagraph (B)(ii); and

(ii) setting forth the procedures and criteria the Secretary will use in identifying or removing countries under subparagraphs (A)(iii) or (B)(iii).

(3) COVERED TECHNOLOGY COMPANY.—The term "covered technology company" means an entity that provides an online data-based service such as a website or internet application in or affecting interstate or foreign commerce and—

(A) is organized under the laws of a country of concern;

(B) in which foreign persons that are nationals of, or companies that are organized under the laws of, countries of concern have a plurality or controlling equity interest;

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

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

(4) FACIAL RECOGNITION TECHNOLOGY.—The term "facial recognition technology" means technology that analyzes facial features in still or video images and is used to identify, or facilitate identification of, an individual using facial physical characteristics.

(5) TARGETED ADVERTISING.—

(A) IN GENERAL.—The term "targeted advertising" means a form of advertising where advertisements are displayed to a user based on the user's traits, information from a profile about the user that is created for the purpose of selling advertisements, or the user's previous online or offline behavior.

(B) LIMITATION.—Such term shall not include advertising chosen because of the context of the internet service, such as—

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

(ii) advertising that is directed to a user by the operator of a website, online service, online application, or mobile application based on the search terms that the user used to arrive at such website, service, or application.

(6) USER DATA.—The term "user data" means any information obtained by an entity that provides a data-based service such as a website or internet application that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked with an individual who is a citizen or resident of the United States without regard to whether such information is directly submitted by the individual to the entity, is derived by the entity

from the observed activity of the individual, or is obtained by the entity by any other means.

SEC. 3. DATA SECURITY REQUIREMENTS FOR COVERED TECHNOLOGY COMPANIES.

(a) In General.—The following requirements shall apply to a covered technology company:

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

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

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

(A) view any user data held by the company that relates to the individual; and

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

(4) PROHIBITION ON TRANSFER TO COUNTRIES OF CONCERN.—The company shall not transfer any user data or information needed to decipher that data, such as encryption keys, to any country of concern (including indirectly through a third country that is not a country of concern).

(5) DATA STORAGE REQUIREMENT.—The company shall not store any user data collected from citizens or residents of the United States or information needed to decipher that data, such as encryption keys, on a server or other data storage device that is located outside of the United States or a country that maintains an agreement with the United States to share data with law enforcement agencies through a process established by law.

(6) REPORTING REQUIREMENT.—Not less frequently than annually, the chief executive officer or equivalent officer of the company shall submit, under penalty of perjury, a report to the Federal Trade Commission, the Attorney General of the United States, and the Attorney General of each State certifying compliance with the requirements of this section.

(b) Exceptions.—

(1) EXCEPTION FOR LAW ENFORCEMENT AND MILITARY.—The requirements of paragraphs (1) through (4) of subsection (a) shall not apply where data is collected, used, retained, stored, or shared by a covered technology company solely for the purpose of assisting a law enforcement or military agency that is not affiliated with a country of concern.

(2) TRANSFER OF SHARED CONTENT.—The requirements of paragraph (4) and (5) of subsection (a) shall not apply to user data that is content produced by a user for the purpose 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. 4. DATA SECURITY REQUIREMENTS FOR OTHER TECHNOLOGY COMPANIES.

(a) In General.—The following requirements shall apply to any company operating in or affecting interstate or foreign commerce that provides a data-based service such as a website or internet application but is not a covered technology company:

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

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

(b) Exceptions.—

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

(2) TRANSFER OF SHARED CONTENT.—The requirements of subsection (a) shall not apply to user data that is content produced by a user for the purpose 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)).

(3) ACTIONS BY THE COMMISSION.—Except as otherwise provided, the Commission shall prevent any person from violating section 3 or 4 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, and any person who violates such section shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act.

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

(b) Criminal Penalty.—

(1) OFFENSE.—It shall be unlawful to knowingly cause a technology company to violate a requirement of section 3 or 4.

(2) PENALTY.—Any person who violates paragraph (1) shall be imprisoned for not more than 5 years, fined under title 18, United States Code, or both.

(c) Enforcement by State Attorneys General.—

(1) IN GENERAL.—

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

(i) enjoin that practice;

(ii) enforce compliance with such section;

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

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

(B) NOTICE.—

(i) IN GENERAL.—Before filing an action under subparagraph (A), the attorney general of the State involved shall provide to the Commission—

(I) written notice of that action; and

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

(ii) EXEMPTION.—

(I) IN GENERAL.—Clause (i) shall not apply with respect to the filing of an action by an attorney general of a State under this paragraph if the attorney general of the State determines that it is not feasible to provide the notice described in that clause before the filing of the action.

(II) NOTIFICATION.—In an action described in subclause (I), the attorney general of a State shall provide notice and a copy of the complaint to the Commission at the same time as the attorney general files the action.

(2) INTERVENTION.—

(A) IN GENERAL.—On receiving notice under paragraph (1)(B), the Commission shall have the right to intervene in the action that is the subject of the notice.

(B) EFFECT OF INTERVENTION.—If the Commission intervenes in an action under paragraph (1), it shall have the right—

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

(ii) to file a petition for appeal.

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

(A) conduct investigations;

(B) administer oaths or affirmations; or

(C) compel the attendance of witnesses or the production of documentary and other evidence.

(4) ACTIONS BY THE COMMISSION.—In any case in which an action is instituted by or on behalf of the Commission for violation of section 3 or 4, no State may, during the pendency of that action, institute an action under paragraph (1) against any defendant named in the complaint in the action instituted by or on behalf of the Commission for that violation.

(5) VENUE; SERVICE OF PROCESS.—

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

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

(ii) a State court of competent jurisdiction.

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

(i) is an inhabitant; or

(ii) may be found.

(d) Private Right of Action.—

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

(2) RELIEF.—In a civil action brought under paragraph (1) in which the plaintiff prevails, the court may award such plaintiff up to $1,000 for each day that such plaintiff was affected by a violation of section 3 (up to a maximum of $15,000 per each such violation per plaintiff).

SEC. 6. REQUIREMENT FOR APPROVAL OF COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES OF

CERTAIN TRANSACTIONS.

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

"(9) APPROVAL REQUIRED FOR CERTAIN TRANSACTIONS.—

"(A) IN GENERAL.—A covered transaction described in subparagraph (C) is prohibited unless the Committee—

"(i) reviews the transaction under this subsection; and

"(ii) determines that the transaction does not pose a risk to the national security of the United States.

"(B) MITIGATION.—The Committee, or a lead agency on behalf of the Committee, may negotiate, enter into or impose, and enforce an agreement or condition under subsection (l)(3) with any party to a covered transaction described in subparagraph (C) to mitigate any risk to the national security of the United States that arises as a result of the covered transaction.

"(C) COVERED TRANSACTION DESCRIBED.—A covered transaction described in this subparagraph is a transaction that could result in foreign control of a United States company—

"(i) that collects, sells, buys, or processes user data (as defined in section 2 of the National Security and Personal Data Protection Act of 2019) and whose business consists substantially more of transferring data than manufacturing, delivering, repairing, or servicing physical goods or providing physical services; or

"(ii) that operates a social media platform or website.".