To amend the Export Control Reform Act of 2018 to require export controls with respect to certain personal data of United States nationals and individuals in the United States, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. Wyden introduced the following bill; which was read twice and referred to the Committee on ____________

A BILL

To amend the Export Control Reform Act of 2018 to require export controls with respect to certain personal data of United States nationals and individuals in the United States, 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 “Protecting Americans’ Data From Foreign Surveillance Act of 2021”.
SEC. 2. REQUIREMENT TO CONTROL THE EXPORT OF CERTAIN PERSONAL DATA OF UNITED STATES NATIONALS AND INDIVIDUALS IN THE UNITED STATES.

(a) In General.—Part I of the Export Control Reform Act of 2018 (50 U.S.C. 4811 et seq.) is amended by inserting after section 1758 the following:

“SEC. 1758A. REQUIREMENT TO CONTROL THE EXPORT OF CERTAIN PERSONAL DATA OF UNITED STATES NATIONALS AND INDIVIDUALS IN THE UNITED STATES.

“(a) Identification of Categories of Personal Data.—

“(1) In General.—The President shall establish and, in coordination with the Secretary and the heads of the appropriate Federal agencies, lead a regular, ongoing interagency process to identify categories of personal data of covered individuals that could—

“(A) be exploited by foreign governments; and

“(B) if exported in a quantity that exceeds the threshold established under paragraph (3), harm the national security of the United States.

“(2) List Required.—The interagency process established under paragraph (1)—
“(A) shall identify an initial list of categories of personal data under paragraph (1) not later than one year after the date of the enactment of the Protecting Americans’ Data From Foreign Surveillance Act of 2021; and

“(B) may, as appropriate thereafter, add categories to, remove categories from, or modify categories on, that list.

“(3) ESTABLISHMENT OF THRESHOLD.—

“(A) IN GENERAL.—Not later than one year after the date of the enactment of the Protecting Americans’ Data From Foreign Surveillance Act of 2021, the interagency process established under paragraph (1) shall establish a threshold for the quantity of personal data of covered individuals the export of which by one person could harm the national security of the United States.

“(B) PARAMETERS.—The threshold established under subparagraph (A) shall be the export by one person during a calendar year of the personal data of not less than 10,000 covered individuals and not more than 1,000,000 covered individuals.
“(C) CONSIDERATIONS.—In establishing the threshold under subparagraph (A), the interagency process shall seek to balance the need to protect personal data from exploitation by foreign governments against the likelihood of—

“(i) impacting legitimate business activities and other activities that do not harm the national security of the United States; or

“(ii) chilling speech protected by the First Amendment to the Constitution of the United States.

“(4) DETERMINATION OF PERIOD FOR PROTECTION.—The interagency process established under paragraph (1) shall determine, for each category of personal data identified under that paragraph, the period of time for which encryption technology described in subsection (b)(4)(C) is required to be able to protect that category of data from decryption to prevent the exploitation of the data by a foreign government from harming the national security of the United States.

“(5) PROCESS.—The interagency process established under paragraph (1) shall—
“(A) be informed by multiple sources of information, including—

“(i) publicly available information;

“(ii) classified information, including relevant information provided by the Director of National Intelligence;

“(iii) information relating to reviews and investigations of transactions by the Committee on Foreign Investment in the United States under section 721 of the Defense Production Act of 1950 (50 U.S.C. 4565);

“(iv) the categories of sensitive personal data described in paragraphs (1)(ii) and (2) of section 800.241(a) of title 31, Code of Federal Regulations, as in effect on the day before the date of the enactment of the Protecting Americans’ Data From Foreign Surveillance Act of 2021, and any categories of sensitive personal data added to such section after such date of enactment;

“(v) information provided by the advisory committee established pursuant to paragraph (7); and
“(vi) the recommendations (which the President shall request) of—

“(I) privacy experts identified by the National Academy of Sciences; and

“(II) experts on the First Amendment to the Constitution of the United States identified by the American Bar Association; and

“(B) take into account the significant quantity of personal data of covered individuals that has already been stolen or acquired by foreign governments, the harm to United States national security caused by the theft of that personal data, and the potential for further harm to United States national security if that personal data were combined with additional sources of personal data.

“(6) NOTICE AND COMMENT PERIOD.—The President shall provide for a public notice and comment period after the publication in the Federal Register of a proposed rule, and before the publication of a final rule—
“(A) identifying the initial list of categories of personal data under subparagraph (A) of paragraph (2);

“(B) adding categories to, removing categories from, or modifying categories on, that list under subparagraph (B) of that paragraph;

“(C) establishing the threshold under paragraph (3); or

“(D) setting forth the period of time for which encryption technology described in subsection (b)(4)(C) is required under paragraph (4) to be able to protect such a category of data from decryption.

“(7) ADVISORY COMMITTEE.—

“(A) IN GENERAL.—The Secretary shall establish an advisory committee to advise the Secretary with respect to privacy and sensitive personal data.

“(B) APPLICABILITY OF FEDERAL ADVISORY COMMITTEE ACT.—Subsections (a)(1), (a)(3), and (b) of section 10 and sections 11, 13, and 14 of the Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the advisory committee established pursuant to subparagraph (A).
“(8) Treatment of anonymized personal data.—The interagency process established under paragraph (1) may not treat anonymized personal data differently than identifiable personal data if the persons to which the anonymized personal data relates could reasonably be identified using other sources of data.

“(b) Commerce Controls.—

“(1) In general.—Beginning 18 months after the date of the enactment of the Protecting Americans’ Data From Foreign Surveillance Act of 2021, the Secretary shall impose appropriate controls under the Export Administration Regulations on the export, reexport, or in-country transfer of covered personal data in a quantity that exceeds the threshold established under subsection (a)(3), including through interim controls (such as by informing a person that a license is required for export), as appropriate, or by publishing additional regulations.

“(2) Levels of control.—

“(A) In general.—Except as provided in subparagraph (C) or (D), the Secretary shall—

“(i) require a license or other authorization for the export, reexport, or in-country transfer of covered personal data in a
quantity that exceeds the threshold established under subsection (a)(3);

“(ii) determine whether that export, reexport, or in-country transfer is likely to harm the national security of the United States—

“(I) after consideration of the matters described in subparagraph (B); and

“(II) in coordination with the heads of the appropriate Federal agencies; and

“(iii) if the Secretary determines under clause (ii) that the export, reexport, or in-country transfer is likely to harm the national security of the United States, deny the application for the license or other authorization for the export, reexport, or in-country transfer.

“(B) Considerations.—In determining under clause (ii) of subparagraph (A) whether an export, reexport, or in-country transfer of covered personal data described in clause (i) of that subparagraph is likely to harm the national security of the United States, the Sec-
retary, in coordination with the heads of the appropriate Federal agencies, shall take into account—

“(i) the adequacy and enforcement of data protection, surveillance, and export control laws in the foreign country to which the covered personal data would be exported or reexported, or in which the covered personal data would be transferred, in order to determine whether such laws, and the enforcement of such laws, are sufficient to—

“(I) protect the covered personal data from accidental loss, theft, and unauthorized or unlawful processing;

“(II) ensure that the covered personal data is not exploited for intelligence purposes by foreign governments to the detriment of the national security of the United States; and

“(III) prevent the reexport of the covered personal data to a third country for which a license would be required for such data to be exported directly from the United States;
“(ii) the circumstances under which
the government of the foreign country can
compel, coerce, or pay a person in or na-
tional of that country to disclose the cov-
ered personal data; and

“(iii) whether that government has
conducted hostile foreign intelligence oper-
ations, including information operations,
against the United States.

“(C) LICENSE REQUIREMENT AND PRE-
SUMPTION OF DENIAL FOR CERTAIN COUN-
TRIES.—

“(i) IN GENERAL.—The Secretary
shall—

“(I) require a license or other au-
thorization for the export or reexport
to, or in-country transfer in, a coun-
try on the list required by clause (ii)
of covered personal data in a quantity
that exceeds the threshold established
under subsection (a)(3); and

“(II) deny an application for
such a license or other authorization
unless the person seeking the license
or authorization demonstrates to the
satisfaction of the Secretary that the export, reexport, or in-country transfer will not harm the national security of the United States.

“(ii) List Required.—

“(I) In General.—Not later than one year after the date of the enactment of the Protecting Americans’ Data From Foreign Surveillance Act of 2021, the Secretary shall, in consultation with the heads of the appropriate Federal agencies and based on the considerations described in subparagraph (B), establish a list of each country with respect to which the Secretary determines that the export or reexport to, or in-country transfer in, the country of covered personal data in a quantity that exceeds the threshold established under subsection (a)(3) will be likely to harm the national security of the United States.

“(II) Modifications to List.—

The Secretary, in consultation with
the heads of the appropriate Federal agencies—

“(aa) may add a country to or remove a country from the list required by subclause (I) at any time; and

“(bb) shall review that list not less frequently than every 5 years.

“(D) NO LICENSE REQUIREMENT FOR CERTAIN COUNTRIES.—

“(i) IN GENERAL.—The Secretary may not require a license or other authorization for the export or reexport to, or in-country transfer in, a country on the list required by clause (ii) of covered personal data, without regard to the threshold established under subsection (a)(3).

“(ii) LIST REQUIRED.—

“(I) IN GENERAL.—Not later than one year after the date of the enactment of the Protecting Americans’ Data From Foreign Surveillance Act of 2021, the Secretary shall, in consultation with the heads of the appro-
priate Federal agencies and based on the considerations described in sub-
paragraph (B) and subject to clause (iii), establish a list of each country with respect to which the Secretary determines that the export or reexport to, or in-country transfer in, the country of covered personal data (without regard to the threshold established under subsection (a)(3)) will not harm the national security of the United States.

“(II) MODIFICATIONS TO LIST.— The Secretary, in consultation with the heads of the appropriate Federal agencies—

“(aa) may add a country to or remove a country from the list required by subclause (I) at any time; and

“(bb) shall review that list not less frequently than every 5 years.

“(iii) CONGRESSIONAL REVIEW.—
“(I) IN GENERAL.—The list required by clause (ii) and any updates to that list adding or removing countries shall take effect, for purposes of clause (i), on the date that is 180 days after the Secretary submits to the appropriate congressional committees a proposal for the list or update unless there is enacted into law, before that date, a joint resolution of disapproval pursuant to subclause (II).

“(II) JOINT RESOLUTION OF DISAPPROVAL.—

“(aa) JOINT RESOLUTION OF DISAPPROVAL DEFINED.—In this clause, the term ‘joint resolution of disapproval’ means a joint resolution the matter after the resolving clause of which is as follows: ‘That Congress does not approve of the proposal of the Secretary with respect to the list required by section 1758A(b)(2)(D)(ii) submitted to...
Congress on ______., with the blank space being filled with the appropriate date.

“(bb) Procedures.—The procedures set forth in paragraphs (4)(C), (5), (6), and (7) of section 2523(d) of title 18, United States Code, apply with respect to a joint resolution of disapproval under this clause to the same extent and in the same manner as such procedures apply to a joint resolution of disapproval under such section 2523(d), except that paragraph (6) of such section shall be applied and administered by substituting ‘the Committee on Banking, Housing, and Urban Affairs’ for ‘the Committee on the Judiciary’ each place it appears.

“(III) Rules of House of Representatives and Senate.—This clause is enacted by Congress—
“(aa) as an exercise of the rulemaking power of the Senate and the House of Representatives, respectively, and as such is deemed a part of the rules of each House, respectively, and supersedes other rules only to the extent that it is inconsistent with such rules; and

“(bb) with full recognition of the constitutional right of either House to change the rules (so far as relating to the procedure of that House) at any time, in the same manner, and to the same extent as in the case of any other rule of that House.

“(3) REVIEW OF LICENSE APPLICATIONS.—

“(A) IN GENERAL.—The Secretary shall establish—

“(i) an interagency process, in which the appropriate Federal agencies participate, to conduct review of applications for a license or other authorization for the export, reexport, or in-country transfer of
covered personal data in a quantity that exceeds the threshold established under subsection (a)(3); and

“(ii) procedures for conducting the review of such applications.

“(B) DISCLOSURES RELATING TO COLLABORATIVE ARRANGEMENTS.—In the case of an application for a license or other authorization for an export, reexport, or in-country transfer described in subparagraph (A)(i) submitted by or on behalf of a joint venture, joint development agreement, or similar collaborative arrangement, the Secretary may require the applicant to identify, in addition to any foreign person participating in the arrangement, any foreign person with significant ownership interest in a foreign person participating in the arrangement.

“(4) EXCEPTIONS.—The Secretary shall not impose under paragraph (1) a requirement for a license or other authorization with respect to the export, reexport, or in-country transfer of covered personal data pursuant to any of the following transactions:
“(A) The export, reexport, or in-country transfer by an individual of the personal data of the individual.

“(B) The export, reexport, or in-country transfer of the personal data of an individual by a person performing a service for the individual if the export, reexport, or in-country transfer of the personal data is strictly necessary to perform that service.

“(C) The export, reexport, or in-country transfer of personal data that is encrypted if—

“(i) the encryption key or other information necessary to decrypt the data is not exported, reexported, or transferred; and

“(ii) the encryption technology used to protect the data against decryption is certified by the National Institute of Standards and Technology as capable of protecting data for the period of time determined under subsection (a)(4) to be sufficient to prevent the exploitation of the data by a foreign government from harming the national security of the United States.
“(D) The export, reexport, or in-country transfer of personal data that is ordered by an appropriate court of the United States.

“(e) Requirements for Identification of Categories and Determination of Appropriate Controls.—In identifying categories of personal data under subsection (a)(1) and imposing appropriate controls under subsection (b), the interagency process established under subsection (a)(1) or the Secretary, as appropriate—

“(1) may not regulate or restrict the publication or sharing of—

“(A) a photograph or audio or video recording in which no individual appearing had a reasonable expectation of privacy;

“(B) personal data that is a matter of public record, such as a court record or other government record that is generally available to the public, including information about an individual made public by that individual or by the news media;

“(C) information about a matter of public interest; or

“(D) consistent with the goal of protecting the national security of the United States, any other information the publication of which is
protected by the First Amendment to the Constitution of the United States; and

“(2) shall consult with the appropriate congressional committees.

“(d) Penalties.—

“(1) Liable persons.—

“(A) In general.—A person violates this section if the person—

“(i) exports, reexports, or in-country transfers covered personal data in violation of this section;

“(ii) directs or causes another person to export, reexport, or in-country transfer covered personal data in violation of this section; or

“(iii) is an officer or employee of an organization and knew or should have known that another employee of the organization who reports, directly or indirectly, to the officer or employee was directed to export, reexport, or in-country transfer covered personal data in violation of this section.

“(B) Exceptions and clarifications.—
“(i) INTERMEDIARIES NOT LIABLE.—

An intermediate consignee (as defined in section 772.1 of the Export Administration Regulations (or any successor regulation)) or other intermediary is not liable for the export, reexport, or in-country transfer of covered personal data in violation of this section when acting as an intermediate consignee or other intermediary for another person.

“(ii) SPECIAL RULE FOR CERTAIN APPLICATIONS.—In a case in which an application installed on an electronic device transmits or causes the transmission of covered personal data without the knowledge of the owner or user of the device who installed the application, the developer of the application, and not the owner or user of the device, is liable for any violation of this section.

“(2) CRIMINAL PENALTIES.—In determining an appropriate term of imprisonment under section 1760(b)(2) for a violation of this section, the court shall consider—
“(A) how many covered individuals had their covered personal data exported, reexported, or in-country transferred in violation of this section; and

“(B) any harm that resulted from the violation.

“(3) Private right of action.—

“(A) In general.—An individual may bring a civil action in an appropriate district court of the United States if, as a result of an export, reexport, or in-country transfer of covered personal data in violation of this section, the individual is—

“(i) physically harmed; or

“(ii) detained or imprisoned in a foreign country.

“(B) Relief.—A court may award a prevailing plaintiff in a civil action under subparagraph (A) appropriate relief, including actual damages, punitive damages, or attorney’s fees.

“(e) Report to Congress.—

“(1) In general.—Not less frequently than annually, the Secretary, in coordination with the heads of the appropriate Federal agencies, shall submit to the appropriate congressional committees a
report on the results of actions taken pursuant to this section.

“(2) INCLUSIONS.—Each report required by paragraph (1) shall include a description of the determinations made under subsection (b)(2)(A)(ii) during the preceding year.

“(3) FORM.—Each report required by paragraph (1) shall be submitted in unclassified form but may include a classified annex.

“(f) DISCLOSURE OF CERTAIN LICENSE INFORMATION.—Not less frequently than every 90 days, the Secretary shall publish on a publicly accessible website of the Department of Commerce, including in a machine-readable format, the following information, with respect to each application for a license for the export, reexport, or in-country transfer of covered personal data in a quantity that exceeds the threshold established under subsection (a)(3):

“(1) The name of the applicant.

“(2) The date of the application.

“(3) The name of the foreign party to which the applicant sought to export, reexport, or transfer the data.

“(4) The categories of covered personal data the applicant sought to export, reexport, or transfer.
“(5) The number of covered individuals whose
information the applicant sought to export, reexport,
or transfer.

“(6) Whether the application was approved or
denied.

“(g) News Media Protections.—A person that is
engaged in journalism is not subject to restrictions im-
posed under this section to the extent that those restric-
tions directly infringe on the journalism practices of that
person.

“(h) Citizenship Determinations Not Re-
quired.—This section does not require a person to deter-
mine the citizenship or immigration status of the cus-
tomers of the person, but once the person becomes aware
that data belongs to a covered individual, the person shall
treat that data as is required by this section.

“(i) Authorization of Appropriations.—There
are authorized to be appropriated to the Secretary such
sums as may be necessary to carry out this section, includ-
ing to hire additional employees with expertise in privacy.

“(j) Definitions.—In this section:

“(1) Appropriate Congressional Com-
mittees.—The term ‘appropriate congressional com-
mittees’ means—
“(A) the Committee on Banking, Housing, and Urban Affairs, the Committee on Foreign Relations, the Committee on Finance, and the Select Committee on Intelligence of the Senate; and

“(B) the Committee on Foreign Affairs, the Committee on Financial Services, the Committee on Ways and Means, and the Permanent Select Committee on Intelligence of the House of Representatives.

“(2) APPROPRIATE FEDERAL AGENCIES.—The term ‘appropriate Federal agencies’ means the following:

“(A) The Department of Defense.
“(B) The Department of State.
“(C) The Department of Justice.
“(D) The Department of the Treasury.
“(E) The Office of the Director of National Intelligence.
“(F) The Cybersecurity and Infrastructure Security Agency.
“(I) The Federal Communications Commission.

“(J) The Department of Health and Human Services.

“(K) Such other Federal agencies as the President or the Secretary of Commerce considers appropriate.

“(3) COVERED INDIVIDUAL.—The term ‘covered individual’ means an individual—

“(A) who is located in the United States;

or

“(B) who is—

“(i) located outside the United States or whose location cannot be determined;

and

“(ii) a citizen of the United States or a noncitizen lawfully admitted for permanent residence.

“(4) COVERED PERSONAL DATA.—The term ‘covered personal data’ means the categories of personal data of covered individuals identified pursuant to the interagency process under subsection (a).

“(5) EXPORT.—
“(A) IN GENERAL.—The term ‘export’, with respect to covered personal data, includes—

“(i) subject to subparagraph (D), the shipment or transmission of the data out of the United States, including the sending or taking of the data out of the United States, in any manner; or

“(ii) the release or transfer of the data to any noncitizen (other than a noncitizen described in subparagraph (C)).

“(B) EXCEPTIONS.—The term ‘export’ does not include—

“(i) the publication of covered personal data on the internet in a manner that makes the data accessible to any member of the general public; or

“(ii) any activity protected by the speech or debate clause of the Constitution of the United States.

“(C) NONCITIZENS DESCRIBED.—A noncitizen described in this subparagraph is a noncitizen—

“(i) who is lawfully admitted for permanent residence;
“(ii) to whom the Secretary of Homeland Security has issued an employment authorization document (Form I–766);

“(iii) who has been granted deferred action pursuant to the memorandum of the Department of Homeland Security entitled ‘Exercising Prosecutorial Discretion with Respect to Individuals Who Came to the United States as Children’ issued on June 15, 2012; or

“(iv) who is present in the United States pursuant to a valid, unexpired E–3, H–1B, H–1B1, H–1B2, J–1, L–1, O–1A, or TN–1 visa.

“(D) UNINTENTIONAL TRANSMISSIONS.—

“(i) IN GENERAL.—On and after the date that is 5 years after the date of the enactment of the Protecting Americans’ Data From Foreign Surveillance Act of 2021, and except as provided in clause (iii), the term ‘export’ includes the transmission of data through a country described in clause (ii), without regard to whether the person originating the trans-
mission had knowledge of or control over the path of the transmission.

“(ii) COUNTRIES DESCRIBED.—A country is described in this clause if a license would be required for the export or reexport to, or in-country transfer in, that country of covered personal data in a quantity that exceeds the threshold established under subsection (a)(3).

“(iii) EXCEPTIONS.—Clause (i) does not apply with respect to a transmission of data through a country described in clause (ii) if—

“(I) the data is encrypted as described in subsection (b)(4)(C); or

“(II) the person that originated the transmission received a representation from the party delivering the data for the person stating that the data will not transit through a country described in clause (ii).

“(iv) FALSE REPRESENTATIONS.—If a party delivering covered personal data as described in clause (iii)(II) transmits the data through a country described in clause
(ii) despite making the representation described in clause (iii)(II), that party shall be liable for violating this section.

“(6) Lawfully admitted for permanent residence; national.—The terms ‘lawfully admitted for permanent residence’ and ‘national’ have the meanings given those terms in section 101(a) of the Immigration and Nationality Act (8 U.S.C. 1101(a)).

“(7) Noncitizen.—The term ‘noncitizen’ means an individual who is not a citizen or national of the United States.”.

(b) Statement of Policy.—Section 1752 of the Export Control Reform Act of 2018 (50 U.S.C. 4811) is amended—

(1) in paragraph (1)—

(A) in subparagraph (A), by striking “; and” and inserting a semicolon;

(B) in subparagraph (B), by striking the period at the end and inserting “; and”; and

(C) by adding at the end the following:

“(C) to restrict the export of personal data of United States citizens and other covered individuals (as defined in section 1758A(e)) in a
quantity and a manner that could harm the national security of the United States.”; and

(2) in paragraph (2), by adding at the end the following:

“(H) To prevent the exploitation of personal data of United States citizens and other covered individuals (as defined in section 1758A(e)) in a quantity and a manner that could harm the national security of the United States.”.

(c) Conforming Amendment.—Section 1742(13)(A) of the Export Control Reform Act of 2018 (50 U.S.C. 4801(13)(A)) is amended, in the matter preceding clause (i), by inserting “(except section 1758A)” after “part I”.