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 (for himself, Ms. Lummis, Mr. Whitehouse, Mr. Rubio, and Mr. Hagerty) 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 Representa-
tives 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 2022”.

SEC. 2. SENSE OF CONGRESS.

It is the sense of Congress that—
(1) accelerating technological trends have made sensitive personal data an especially valuable input to activities that adversaries of the United States undertake to threaten both the national security of the United States and the individual privacy that the people of the United States cherish;

(2) it is therefore essential to the safety of the United States and the people of the United States to ensure that the United States Government makes every effort to prevent sensitive personal data from falling into the hands of malign foreign actors; and

(3) because allies of the United States face similar challenges, in implementing this Act, the United States Government should explore the establishment of a shared zone of mutual trust with respect to sensitive personal data.

SEC. 3. 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 Secretary shall, in co-
ordination with the heads of the appropriate Federal
agencies, identify categories of personal data of cov-
ered individuals that could—

“(A) be exploited by foreign governments;

and

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

“(2) LIST REQUIRED.—In identifying categories
of personal data of covered individuals under para-
graph (1), the Secretary, in coordination with the
heads of the appropriate Federal agencies, shall—

“(A) identify an initial list of such cat-
egories not later than one year after the date
of the enactment of the Protecting Americans’
Data From Foreign Surveillance Act of 2022;
“(B) as appropriate thereafter and not less frequently than every 5 years, add categories to, remove categories from, or modify categories on, that list.

“(3) Establishment of threshold.—

“(A) Establishment.—Not later than one year after the date of the enactment of the Protecting Americans’ Data From Foreign Surveillance Act of 2022, the Secretary, in coordination with the heads of the appropriate Federal agencies, shall establish a threshold for determining when the export, reexport, or in-country transfer (in the aggregate) of the personal data of covered individuals by one person to or in a restricted country could harm the national security of the United States.

“(B) Number of covered individuals affected.—The threshold established under subparagraph (A) shall be the export, reexport, or in-country transfer (in the aggregate) by one person to or in a restricted country 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) Category thresholds.—The Secretary, in coordination with the heads of the appropriate Federal agencies, may establish a threshold under subparagraph (A) for each category of personal data identified under paragraph (1).

“(D) Updates.—The Secretary, in coordination with the heads of the appropriate Federal agencies—

“(i) may update the threshold established under subparagraph (A) as appropriate; and

“(ii) shall reevaluate the threshold not less frequently than every 5 years.

“(E) Treatment of persons under common ownership as one person.—For purposes of determining whether a threshold established under subparagraph (A) has been met—

“(i) all exports, reexports, or in-country transfers involving personal data conducted by persons under the ownership or control of the same person shall be aggregated to that person; and
“(ii) that person shall be liable for any export, reexport, or in-country transfer in violation of this section.

“(F) CONSIDERATIONS.—In establishing a threshold under subparagraph (A), the Secretary, in coordination with the heads of the appropriate Federal agencies, shall seek to balance the need to protect personal data from exploitation by foreign governments against the likelihood of—

“(i) impacting legitimate business activities, research 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 Secretary, in coordination with the heads of the appropriate Federal agencies, shall determine, for each category of personal data identified under paragraph (1), the period of time for which encryption technology described in subsection (b)(4)(A)(iii) is required to be able to protect that category of data from decryption to prevent the ex-
exploitation of the data by a foreign government from harming the national security of the United States.

“(5) USE OF INFORMATION; CONSIDERATIONS.—In carrying out this subsection (including with respect to the list required under paragraph (2)), the Secretary, in coordination with the heads of the appropriate Federal agencies, shall—

“(A) use 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 2022, 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 Secretary 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—

“(i) the significant quantity of personal data of covered individuals that has already been stolen or acquired by foreign governments;

“(ii) the harm to United States national security caused by the theft or acquisition of that personal data;
“(iii) the potential for further harm to United States national security if that personal data were combined with additional sources of personal data;

“(iv) the fact that non-sensitive personal data, when analyzed in the aggregate, can reveal sensitive personal data; and

“(v) the commercial availability of inferred and derived data.

“(6) NOTICE AND COMMENT PERIOD.—The Secretary 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 or updating the threshold under paragraph (3); or

“(D) setting forth the period of time for which encryption technology described in sub-
section (b)(4)(A)(iii) 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) MEMBERSHIP.—The committee established pursuant to subparagraph (A) shall include the following members selected by the Secretary:

“(i) Experts on privacy and cybersecurity.

“(ii) Representatives of private sector companies and industry associations.

“(iii) Representatives of civil society groups.

“(C) 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.—

“(A) In General.—In carrying out this subsection, the Secretary may not treat anonymized personal data differently than identifiable personal data if the individuals to which the anonymized personal data relates could reasonably be identified using other sources of data.

“(B) Guidance.—The Under Secretary of Commerce for Standards and Technology shall issue guidance to the public with respect to methods for anonymizing data and how to determine if individuals to which the anonymized personal data relates can be reasonably identified using other sources of data.

“(9) Sense of Congress on Identification of Categories of Personal Data.—It is the sense of Congress that, in identifying categories of personal data of covered individuals under paragraph (1), the Secretary should, to the extent reasonably possible and in coordination with the Secretary of the Treasury, harmonize those categories with the categories of sensitive personal data described in paragraph (5)(A)(iv).
“(b) Commerce Controls.—

“(1) Controls required.—Beginning 18 months after the date of the enactment of the Protecting Americans’ Data From Foreign Surveillance Act of 2022, the Secretary shall impose appropriate controls under the Export Administration Regulations on the export or reexport to, or in-country transfer in, all countries (other than countries on the list required by paragraph (2)(D)) of covered personal data in a manner that exceeds the applicable threshold established under subsection (a)(3), including through interim controls (such as by informing a person that a license is required for export, reexport, or in-country transfer of covered personal data), 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 manner that exceeds the applicable 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 Secretary, in coordination with the heads of the ap-
propriate Federal agencies, shall take into ac-

count—

“(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 trans-
ferred, 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 per-
sonal data is not exploited for intel-
ligence purposes by foreign govern-
ments to the detriment of the national
security of the United States; and

“(III) prevent the reexport of the
covered personal data to a third coun-
try for which a license would be re-
quired 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 national of that country to disclose the covered personal data; and

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

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

“(i) In general.—The Secretary shall—

“(I) 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 in a manner 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 2022, 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 manner that exceeds the applicable 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 applicable 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 2022, the Secretary shall, in con-
sultation with the heads of the appropriate Federal agencies and based on the considerations described in subparagraph (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 any 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 Representatatives 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, consistent with the provisions of section 1756 and in coordination with the heads of the appropriate Federal agencies—

“(i) review applications for a license or other authorization for the export or re-export to, or in-country transfer in, a re-
stricted country of covered personal data
in a manner that exceeds the applicable
threshold established under subsection
(a)(3); and
“(ii) establish procedures for con-
ducting the review of such applications.
“(B) DISCLOSURES RELATING TO COL-
laborative arrangements.—In the case of
an application for a license or other authoriza-
tion for an export, reexport, or in-country
transfer described in subparagraph (A)(i) sub-
mitted by or on behalf of a joint venture, joint
development agreement, or similar collaborative
arrangement, the Secretary may require the ap-
plicant to identify, in addition to any foreign
person participating in the arrangement, any
foreign person with significant ownership inter-
est in a foreign person participating in the ar-
angement.
“(4) EXCEPTIONS.—
“(A) IN GENERAL.—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:

“(i) The export, reexport, or in-country transfer by an individual of covered personal data that specifically pertains to that individual.

“(ii) The export, reexport, or in-country transfer of the personal data of one or more individuals by a person performing a service for those individuals if the service could not possibly be performed (as defined by the Secretary in regulations) without the export, reexport, or in-country transfer of that personal data.

“(iii) 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 to a restricted country or (except as provided in subparagraph (B)) a national of a restricted country; and
“(II) the encryption technology
used to protect the data against
decryption is certified by the National
Institute of Standards and Tech-
ology as capable of protecting data
for the period of time determined
under subsection (a)(4) to be suffi-
cient to prevent the exploitation of the
data by a foreign government from
harming the national security of the
United States.

“(iv) The export, reexport, or in-coun-
try transfer of personal data that is or-
dered by an appropriate court of the
United States.

“(B) Exception for certain nationals
of restricted countries.—Subparagraph
(A)(iii)(I) does not apply with respect to an in-
dividual who is a national of a restricted coun-
try if the individual is also a citizen of the
United States or a noncitizen described in sub-
section (k)(5)(C).

“(c) Requirements for identification of cat-
egories and determination of appropriate con-
trols.—In identifying categories of personal data under
subsection (a)(1) and imposing appropriate controls under subsection (b), the Secretary, in coordination with the heads of the appropriate Federal agencies, as appropriate—

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

“(A) 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;

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

“(C) 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.—In addition to any person that commits an unlawful act described
in subsection (a) of section 1760, an officer or employee of an organization has committed an unlawful act subject to penalties under that section if the officer or employee 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 and subsequently did export, reexport, or in-country transfer such data.

“(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 being di-
rected to do so by 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) with respect to a person for a violation
of this section, the court shall consider—

“(A) how many covered individuals had
their covered personal data exported, reex-
ported, or in-country transferred in violation of
this section;

“(B) any harm that resulted from the vio-
lation; and

“(C) the intent of the person in commit-
ting the violation.

“(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 sub-
mit 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.—

“(1) IN GENERAL.—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 information specified in paragraph (2), with respect to each application—

“(A) for a license for the export or reexport to, or in-country transfer in, a restricted country of covered personal data in a manner that exceeds the applicable threshold established under subsection (a)(3); and

“(B) with respect to which the Secretary made a decision in the preceding 90-day period.
“(2) INFORMATION SPECIFIED.—The information specified in this paragraph with respect to an application described in paragraph (1) is the following:

“(A) The name of the applicant.
“(B) The date of the application.
“(C) The name of the foreign party to which the applicant sought to export, reexport, or transfer the data.
“(D) The categories of covered personal data the applicant sought to export, reexport, or transfer.
“(E) The number of covered individuals whose information the applicant sought to export, reexport, or transfer.
“(F) Whether the application was approved or denied.

“(g) NEWS MEDIA PROTECTIONS.—A person that is engaged in journalism is not subject to restrictions imposed under this section to the extent that those restrictions directly infringe on the journalism practices of that person.

“(h) CITIZENSHIP DETERMINATIONS BY PERSONS PROVIDING SERVICES TO END-USERS NOT REQUIRED.—This section does not require a person that provides prod-
ucts or services to an individual to determine the citizenship or immigration status of the individual, but once the person becomes aware that the individual is a covered individual, the person shall treat covered personal data of that individual as is required by this section.

“(i) Fees.—

“(1) IN GENERAL.—Notwithstanding section 1756(c), the Secretary may, to the extent provided in advance in appropriations Acts, assess and collect a fee, in an amount determined by the Secretary in regulations, with respect to each application for a license submitted under subsection (b).

“(2) DEPOSIT AND AVAILABILITY OF FEES.—
Notwithstanding section 3302 of title 31, United States Code, fees collected under paragraph (1) shall—

“(A) be credited as offsetting collections to the account providing appropriations for activities carried out under this section;

“(B) be available, to the extent and in the amounts provided in advance in appropriations Acts, to the Secretary solely for use in carrying out activities under this section; and

“(C) remain available until expended.
“(j) Regulations.—The Secretary may prescribe such regulations as are necessary to carry out this section.

“(k) Authorization of Appropriations.—There are authorized to be appropriated to the Secretary and to the head of each of the appropriate Federal agencies participating in carrying out this section such sums as may be necessary to carry out this section, including to hire additional employees with expertise in privacy.

“(l) Definitions.—In this section:

“(1) Appropriate Congressional Committees.—The term ‘appropriate congressional committees’ 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 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 Secretary considers appropriate.

“(3) COVERED INDIVIDUAL.—The term ‘covered individual’, with respect to personal data, means an individual who, at the time the data is acquired—

“(A) is located in the United States; or
“(B) 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 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, if the shipment or transmission is intentional, without regard to whether the shipment or transmission was intended to go out of the United States; or

“(ii) the release or transfer of the data to any noncitizen (other than a noncitizen described in subparagraph (C)), if the release or transfer is intentional, with-
out regard to whether the release or transfer was intended to be to a noncitizen.

“(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 discoverable by and 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 who is authorized to be employed in the United States.

“(D) Transmissions through restricted countries.—

“(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 2022, and except as provided in clause (iii), the term ‘export’ includes the transmission of data through a restricted coun-
try, without regard to whether the person originating the transmission had knowledge of or control over the path of the transmission.

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

“(I) the data is encrypted as described in subsection (b)(4)(A)(iii); 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 restricted country.

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

“(6) IN-COUNTRY TRANSFER; REEXPORT.—The terms ‘in-country transfer’ and ‘reexport’, with re-
spect to personal data, shall have the meanings
given those terms in regulations prescribed by the
Secretary.

“(7) \text{LAWFULLY ADMITTED FOR PERMANENT}
RESIDENCE; NATIONAL.—The terms ‘lawfully admit-
ted 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)).

“(8) \text{NONCITIZEN.}.—The term ‘nonecitizen’
means an individual who is not a citizen or national
of the United States.

“(9) \text{RESTRICTED COUNTRY.}.—The term ‘re-
stricted country’ means a country for which a license
or other authorization is required under subsection
(b) for the export or reexport to, or in-country
transfer in, that country of covered personal data in
a manner that exceeds the applicable threshold es-
tablished under subsection (a)(3)).”.

(b) \text{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, notwithstanding section 203(b) of the International Emergency Economic Powers Act (50 U.S.C. 1702(b)), the export of personal data of United States citizens and other covered individuals (as defined in section 1758A(l)) 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(l)) in a quantity and a manner that could harm the national security of the United States.”.

(c) Limitation on Authority to Make Exceptions to Licensing Requirements.—Section 1754 of the Export Control Reform Act of 2018 (50 U.S.C. 4813) is amended—

(1) in subsection (a)(14), by inserting “and subject to subsection (g)” after “as warranted”; and
(2) by adding at the end the following:

“(g) LIMITATION ON AUTHORITY TO MAKE EXCEPTIONS TO LICENSING REQUIREMENTS.—The Secretary may create under subsection (a)(14) exceptions to licensing requirements under section 1758A only for the export, reexport, or in-country transfer of covered personal data (as defined in subsection (l) of that section) by a Federal department or agency.”.

(d) RELATIONSHIP TO INTERNATIONAL EMERGENCY ECONOMIC POWERS ACT.—Section 1754(b) of the Export Control Reform Act of 2018 (50 U.S.C. 4813(b)) is amended by inserting “(other than section 1758A)” after “this part”.