The Protecting Americans' Data From Foreign Surveillance Act

Section by Section (of the newly added 18 U.S.C. 1758A):

a) Identification of Categories of Personal Data of United States Persons

Requires the establishment of an ongoing interagency process to identify categories of personal data of United States persons that, if exported, could be exploited by foreign governments to the detriment of the national security of the United States. The initial list shall be compiled within one year of enactment.

The interagency process shall also establish a threshold, between 10,000 and 1,000,000 people. The export controls created by this bill will then restrict exports of personal data above this annual threshold.

In compiling the list of categories, the interagency process shall consider publicly available information, classified information from the intelligence community, the Committee on Foreign Investment in the United States (CFIUS), the categories of personal data specified under 31 CFR 800.241, input from an advisory committee established by the Commerce Dept., the recommendations of independent privacy experts and First Amendment experts, and a public notice and comment period.

In identifying the categories of sensitive data, the interagency shall consider the personal data of Americans that has already been acquired or stolen by foreign governments and the harm that could be caused if this data were combined with new exported data.

The interagency process shall 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

Requires the Secretary of Commerce to impose export control regulations on the export, reexport, or in-country transfer of the categories of personal data identified by the interagency process above the threshold established by the interagency process.

Requires the Secretary of Commerce to identify a list of countries for which exports will be presumptively banned, unless the potential exporter can demonstrate that the export, reexport or in-country transfer will not harm the national security of the United States.

Requires the Secretary of Commerce to identify a list of countries for which no export license will be required because exports, reexports and in-country transfers will not harm the national security of the United States. Countries can only be added or removed from this list after notifying Congress and giving Congress 180 days to object via a joint resolution of disapproval.

Exports, reexports and in-country transfers to countries not on these two lists will require a license.

When determining which countries will be on the presumptive denial and the no license required lists, and in other cases, to determine whether or not to approve a license, the Secretary of Commerce will consider the following things:

1. the adequacy and enforcement of data protection, surveillance, and export control laws in foreign countries in order to determine whether such laws are sufficient to:
    a. protect personal data from accidental loss, theft, and unauthorized or unlawful processing;
    b. ensure that personal data is not exploited for intelligence purposes by foreign governments to the detriment of the national security of the United States; and
    c. prevent the reexport of personal data to third countries for which a license would be required for such data to be exported directly from the United States;
2. the circumstances under which the government of a foreign country can compel, coerce, or pay a person in or national of that country to disclose personal data; and
3. whether a foreign government has conducted hostile foreign intelligence operations, including information operations, against the United States.

These export control restrictions will not apply to exports by an individual of their own data, exports on behalf of an individual by someone performing a service for them, exports of encrypted data if the key is also not exported, or the disclosure of data required by a court in the United States.

c) **Requirements for Identification of Categories and Determination of Appropriate Controls**

Requires that the interagency process, when identifying the categories of personal data, and the Secretary of Commerce, when imposing the export controls must consult with Congress and may not regulate or restrict the publication or sharing of:

- a photograph or audio or video recording in which no individual appearing had a reasonable expectation of privacy;
- 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;
- information about a matter of public interest; or
- 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

d) Penalties

Under the Export Control Reform Act of 2018 (50 U.S.C. §§ 4801-4852) criminal penalties can include up to 20 years of imprisonment and up to $1 million in fines per violation, or both. Administrative monetary penalties can reach up to $300,000 per violation or twice the value of the transaction, whichever is greater.

In addition to criminal and civil liability for those who export personal data in violation of the law, this section also extends that liability to their supervisor or anyone else who directed them to export personal data in violation of the law. In the case of an employee who was directed by a supervisor to illegally export data, liability extends to everyone above that supervisor in the chain of command who knew, or should have known that the employee was directed to export personal data in violation of the law.

Also clarifies that intermediaries, such as email providers, are not liable for illegal exports of data by users of their services.

For the purpose of calculating the term of imprisonment, the court shall consider how many United States persons had their personal data illegally exported and any harm that resulted from it.

The bill also creates a private right of action, enabling individuals to sue if the illegal export, reexport or in-country transfer of personal data resulted in physical harm to the individual or their detention or arrest in a foreign country. Courts may award actual damages, punitive damages, or attorney's fees.

e) Reports to Congress

Requires the Secretary of Commerce report to Congress every year on implementation of the law.

f) Disclosure of Certain License Information

Requires the Secretary of Commerce to publish on a publicly accessible website of the Department of Commerce, including in a machine-readable format, information about each application for a license of export of personal data.

g) News Media Protections

Exempts persons engaged in journalism from the export control restrictions created by this bill.

h) Citizenship Determination

Clarifies that companies have no obligation to proactively ask their customers about their citizenship, but that once a company learns that a customer's data is protected by these export control regulations, the company shall treat that data accordingly.

i) Authorization of Appropriations

Appropriates funds as necessary to the Secretary of Commerce to carry out the requirements of the bill and to hire additional employees with expertise in privacy.

j) Definitions

Defines various terms used in the bill. The term export is defined, so that it includes:

- 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
- the release or transfer of the data to non-US citizens in the United States, except those on the list below.
- Starting five years after enactment of this bill, the unintended transmission of personal data through a restricted country, if that data is not encrypted.

Exempts from the definition of export:

- any activities protected by the speech or debate clause of the Constitution.
- the publication of personal data on the internet in a manner that makes the data accessible to any member of the general public.

Permits disclosing data, without an export license, to the following categories of non-US citizens:

- Permanent residents (green card holders)
- Individuals who DHS has granted an employment authorization document (Form I–766).
- DACA recipients.
- Individuals present in the United States with a valid, unexpired E–3, H–1B, H–1B1, H–1B2, J–1, L–1,O–1A, or TN–1 visa.