The Protecting Americans' Data From Foreign Surveillance Act

In spite of the clear national security threat posed by foreign governments acquiring personal data about Americans, there are currently no legal restrictions preventing the sale of Americans' personal data to foreign companies and foreign governments.

China's successful efforts to hack Americans' personal data are well known. However, this is not the only way China can obtain large amounts of personal data from the United States. Vast troves of personal information about Americans, including records of cell phone locations, credit card purchases, and web browsing, are available for purchase on the open market to both foreign and domestic buyers. The top U.S counter-intelligence official has said China is "one of the leading collectors of bulk personal data around the globe, using both illegal and legal means."

Congress took a major step in 2018, by directing the Committee on Foreign Investment in the United States (CFIUS) to prevent the sale to foreign firms of American companies holding large amounts of sensitive data about Americans. However, these restrictions only apply to the sale of the company, not the sale of data. The Protecting Americans' Data From Foreign Surveillance Act addresses this critical national security gap, by adding large volumes of Americans' personal data to the list of items controlled under existing export control laws. This bill:

- Directs the Secretary of Commerce to lead an interagency process to identify categories of personal data that, if exported by third parties, could harm U.S. national security.
- Directs the Secretary of Commerce to compile a list of countries to which exports of Americans' personal data would not harm national security, and to require licenses for exports of the identified categories of personal data to other countries in bulk, based on:
    - the adequacy and enforcement of data protection, surveillance, and export control laws in the foreign country.
    - the circumstances under which the government of the foreign country can compel, coerce, or pay a person in that country to disclose personal data.
    - whether that government has conducted hostile foreign intelligence operations against the United States.
- Exempts from the new export controls any data encrypted with NIST-approved algorithms, if the key protecting the data is not exported.
- Ensures that the export rules do not apply to journalism and other speech protected by the First Amendment.
- Applies export control penalties to senior executives who knew or should have known that employees below them were directed to illegally export Americans' personal data.
- Creates a private right of action for individuals who have been physically harmed or arrested or detained in a foreign country as a result of the illegal export of personal data.
- Requires the Commerce Department to publish quarterly reports on personal data exports.