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 governments. This threat was highlighted last year by the Wall Street Journal, which demonstrated that U.S. troops overseas could be tracked using location data sold by data brokers.

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.

In April 2021, Director of National Intelligence Avril Haines warned of the threat: "There's a concern about foreign adversaries getting commercially-acquired information as well, and [I] am absolutely committed to trying to do everything we can to reduce that possibility."

The Committee on Foreign Investment in the United States (CFIUS) has the power to prevent the sale to foreign firms of American companies holding large amounts of sensitive data about Americans, which it has used in several cases. However, CFIUS can only stop 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, in consultation with other key agencies, to identify categories of personal data that, if exported, could harm U.S. national security.
- Directs the Secretary of Commerce to compile a list of low-risk countries for which exports will be unrestricted and to require licenses for bulk exports of the identified categories of personal data to other countries. Exports to high-risk countries will be presumptively denied. The risk status of countries will be determined based on:
    - the adequacy and enforcement of the country's privacy and export control laws.
    - the circumstances under which the foreign government can compel, coerce, or pay a person in that country to disclose personal data.
    - whether that foreign government has conducted hostile foreign intelligence operations against the United States.
- Exempts from the new export rules data encrypted with NIST-approved technology.
- Ensures the export rules do not apply to journalism & other 1st Amend. protected speech.
- 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.
- Permits the Commerce Dept to charge fees for data export licenses to offset agency costs.
- Requires the Commerce Dept to publish quarterly reports on personal data exports.