November 10, 2021

Bipartisan Legislative Proposal Would Expand CFIUS's Jurisdiction

Attorneys
Ama A. Adams
Brendan C. Hanifin
Emerson Siegle

Last week, Senators Marco Rubio (R, FL) and Raphael Warnock (D, GA) introduced bipartisan legislation titled the "Protecting Sensitive Personal Data Act" (the "Act"). The Act would authorize the Committee on Foreign Investment in the United States ("CFIUS" or the "Committee") to expand the scope of transactions subject to a mandatory, pre-closing CFIUS filing requirement to include qualifying investments in "sensitive personal data" companies. This change would significantly increase the number of transaction subject to mandatory CFIUS notification, with cost and timing implications for foreign investors and U.S. businesses across a range of industries.

Background

CFIUS is an interagency committee of the U.S. government with authority to review certain foreign investments in U.S. businesses. CFIUS received authority to review foreign transactions following passage of the Exon-Florio Amendment, which amended Section 721 of the Defense Production Act of 1950 ("DPA") and granted the President authority to block foreign investments in the United States when "the transaction threatens to impair … national security."[1]

The Foreign Investment Risk Review Modernization Act ("FIRRMA") of 2018 dramatically expanded the scope of CFIUS's jurisdiction to include non-passive, non-controlling investments in "TID U.S. businesses" (*i.e.*, a U.S. business that deals in critical technology, services critical infrastructure, or collects or collects or maintains sensitive personal data, each as defined in the CFIUS regulations).[2] In addition, FIRRMA introduced, for the first time, a mandatory filing requirement, applicable to (x) qualifying investments in critical technology companies; and (y) investments that result in acquisition of a substantial interest in a TID U.S. business by a foreign government-affiliated investor. Failure to comply with a mandatory filing obligation (*i.e.*, to file with CFIUS at least 60 days prior to closing) can result in a significant financial penalty, up to the value of the entire transaction, in addition to traditional CFIUS mitigating measures.[3]

Currently, qualifying investments in sensitive personal data companies are not subject to a mandatory filing requirement, with the exception of a limited subset of investments by sovereign investors (although the parties to such transactions have the option to voluntarily seek CFIUS clearance of the transaction either before or after closing).

The Act

The Act would amend the DPA to permit CFIUS to develop rules mandating filings for qualifying investments in sensitive personal data companies (similar to CFIUS's current, mandatory jurisdiction over qualifying investments in critical technology companies).

Like FIRRMA, introduction of the Act appears to have been primarily motivated by national security concerns related to China. An accompanying press release states that the Act "would expand CFIUS' authority to issue regulations that require mandatory declarations to foreign investments in U.S. companies that handle sensitive personal data," to address

[1] 50 U.S.C. § 2170.
[2] A non-passive, non-controlling investment is one that affords a foreign investor board member or observer rights; access to material nonpublic technical information in the possession of the TID U.S. business; or involvement in substantive decision-making of the TID U.S. business regarding critical technology, critical infrastructure, or sensitive personal data.
[3] For additional background on the changes to the CFIUS regulations pursuant to FIRRMA, please see our prior alert covering the proposed rules, the proposed real estate rules, and the final rules.

concerns that "adversaries, like the People's Republic of China . . . stockpile Americans' healthcare data, creating both privacy and national security risks."[4]

Prospective Considerations

If enacted in its current form, the Act would require CFIUS to engage in rulemaking to implement changes to the current CFIUS regulations. Under the most expansive interpretation of the Act, CFIUS could require a mandatory filing for any covered investment in a TID U.S. business that collects or maintains "sensitive personal data," representing an enormous expansion of the Committee's existing mandatory jurisdiction. Alternatively, CFIUS could adopt a more tailored approach, including by:

- Targeting Specific Categories of Data: "Sensitive personal data" is defined broadly in the CFIUS regulations to include various categories of identifiable data, including certain financial data, consumer report information, biometric enrollment data, insurance-related information, non-electronic communications, geolocation data (*e.g.*, collected via mobile applications), health-related data, and genetic information, among others.[5] CFIUS could tailor the mandatory filing requirements to particular categories of data that are of greatest concern to the U.S. government, such as health-related data and genetic information.

- Targeting Specific Data Thresholds: With the exception of companies that collect genetic information or target or tailor solutions to government personnel, companies generally must collect sensitive personal data of at least one million U.S. persons to qualify as TID U.S. businesses. CFIUS could limit the mandatory filing requirements to TID U.S. businesses that collect even higher volumes of sensitive personal data (or, alternatively, specify different volume thresholds for different categories of sensitive personal data, similar to the current treatment of genetic information).

- Targeting Specific Countries: The regulations implementing FIRRMA introduced a "white list" concept, exempting from CFIUS jurisdiction—or a mandatory filing requirement—certain (very limited) categories of investments by Australian, Canadian, and UK investors. In implementing the Act, CFIUS conceivably could limit its scope by expanding on this approach and delineate a list of jurisdictions that are either within—or exempt from—the expanded mandatory filing requirement.

More generally, if the Act becomes law, CFIUS will need to balance (1) the need to effectuate the Act's purpose and increase scrutiny of qualifying transactions involving sensitive personal data companies; against (2) the regulatory burden of an expanded mandatory filing requirement, which foreseeably could result in an exponential increase in CFIUS filings. This, in turn, could strain CFIUS's existing resources, resulting in longer review times, fewer outright approvals of transactions notified by abbreviated declarations, and additional requests for full-form joint voluntary notices (with associated filing fees).

While the passage of the Act, and the potential timing of such passage, is currently unclear, if the Act—which, like FIRRMA, is a bipartisan proposal—gains traction, it could presage a significant increase in CFIUS scrutiny of foreign investment in U.S. businesses going forward.

---

[4] Press Release, Rubio, Warnock Introduce Bill to Protect Americans' Sensitive Personal Data (Nov. 2, 2021), https://www.rubio.senate.gov/public/index.cfm/2021/11/english-espa-ol-rubio-warnock-introduce-bill-to-protect-americans-sensitive-personal-data.

[5] With continued innovation in artificial intelligence and machine learning, as well as increased reliance on e-commerce, the volume of U.S. businesses that qualify as sensitive personal data companies is growing at breakneck pace.