Published on *The National Law Review* https://natlawreview.com

Spotlight On Sensitive Personal Data As Foreign Investment Rules Take Force

Article By:

Austin Mooney

New CFIUS rules—which took effect February 13, 2020—underscore the need for privacy diligence in deals involving foreign investments and signal a larger trend toward heightened regulatory scrutiny of foreign access to sensitive US personal data.

IN DEPTH

The Treasury Department's final rules implementing the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) are now in effect, creating important new regulatory considerations for foreign investments involving US personal data. FIRRMA expanded the authority of the Committee on Foreign Investment in the United States (CFIUS) to review, among other things, certain non-controlling foreign investments involving "sensitive personal data of United States citizens that may be exploited in a manner that threatens national security." The new rules, which took effect February 13, 2020, underscore the need for enhanced CFIUS diligence focusing on data privacy in transactions involving companies, funds, private equity firms and other investors that qualify as "foreign persons" under the new rules. In addition, the rules signal a larger trend away from the historically permissive US approach to foreign data access toward a restrictive framework taking account of national security and other risks posed by foreign access to this information. For a more comprehensive look at the new rules' impact outside of the context of data privacy, see our previous *On the Subject*.

'Sensitive Personal Data'

FIRRMA extended CFIUS jurisdiction to certain non-controlling investments by a foreign person in a US business that "maintains or collects sensitive personal data of United States citizens that may be exploited in a manner that threatens national security." In implementing these provisions, the new rules define "sensitive personal data" as "identifiable" data falling into one of 11 categories:

1. Financial data that might indicate "financial distress or hardship"
2. Credit report information
3. Insurance application data for health, professional liability, mortgage or life insurance

4. Information relating to a person's "physical, mental, or psychological health condition"
5. Private emails or other electronic communications
6. Geolocation data, including data derived from cell towers, WiFi access points and wearable electronic devices
7. Biometric identifiers such as fingerprints and face scans
8. Data used for generating government identification
9. Data concerning security clearance status
10. Data in security clearance application forms
11. Genetic test results

In addition to satisfying one of the above categories, a company only maintains "sensitive personal data" under the rules if it either (a) targets executive branch personnel or contractors, or (b) maintains or intends to maintain this data concerning one million or more US citizens. In other words, a company may maintain one or all of the enumerated categories of personal data but still fall outside of the scope of CFIUS investment review if it does not specifically target government employees or does not meet the one million person threshold.

Notably, the rules single out "genetic test results" as particularly sensitive and exempt from the above limitations. This information will qualify as "sensitive personal data" regardless of the subject or quantity of the data, reflecting a heightened perceived risk to national security stemming from such information. However, "data derived from databases maintained by the U.S. Government and routinely provided to private parties for purposes of research" is not considered "genetic test results" for these purposes.

Sensitive data subject to CFIUS investment review must be "identifiable," defined "data that can be used to distinguish or trace an individual's identity" and includes "aggregated or anonymized data" where "the ability to disaggregate or de-anonymize" is preserved. This is an expansive definition that potentially includes data considered "deidentified" under other regulatory frameworks, such as the Health Insurance Portability and Accountability Act (HIPAA) and the California Consumer Privacy Act (CCPA).

'Threatens National Security'

As noted, the new rules expand CFIUS jurisdiction to "covered investments" in companies holding or processing sensitive personal data where the data "may be exploited in a way that threatens national security." Determining what data might "threaten national security" is not a straightforward analysis; however, one way to predict what CFIUS will assess as threatening national security is by looking at recent actions. In recent years, CFIUS used its existing "control transaction" authority—which covers any transactions where a foreign entity obtains a "controlling" stake in a US company—to divest two companies based on the transfer of sensitive personal data: first, a dating app for LGBT individuals, and second, an online patient forum.

These actions offer some insight into what triggers “national security” concern, though many of the details remain nonpublic. Health information, for example, appears to be a particular concern for CFIUS. HIPAA-covered entities such as hospitals and health insurers, as well as their business associates, would likely merit CFIUS review if subject to covered foreign investments. In addition, as the divestment of the online patient forum makes clear, health-related data can trigger national security concerns even if not generated within the context of traditional HIPAA-covered healthcare services. Accordingly, health tech companies offering products such as wearables, exercise apps and health tracking programs could all fall within the scope of CFIUS review if targeted for covered foreign investments.

Ultimately, it is the role of CFIUS and its component agencies, in particular the Office of the Director of National Intelligence, to assess national security risk for the purpose of recommending action to the President, who has the final authority to block, impose conditions or divest completed transactions reviewed by CFIUS. These national security assessments often involve classified information unavailable to the public. As a result, even seemingly benign personal data could be determined by CFIUS to pose a national security risk by CFIUS, leading to the risk of post-closing investigations and divestment. For this reason, in many circumstances, the recommended approach for companies and their foreign investors is to submit covered transactions to voluntary CFIUS review before closing. Under the new rules, voluntary submissions must be reviewed within 45 days, after which a full investigation can extend up to an additional 90 days while CFIUS makes its determination. These voluntary reviews offer clarity to investments that could otherwise be clouded by the threat of an investigation. In addition to offering voluntary review, FIRRMA provides for mandatory CFIUS review in certain high-risk scenarios, including certain cases where the investor in a company with sensitive personal data is a foreign government.

Shifting the US Approach to Foreign Data Access

In addition to the immediate takeaways for foreign investors and companies soliciting foreign investments, the new CFIUS rules highlight a growing trend in US data privacy that impacts all industries and further underscores the need for privacy diligence. Unlike the European Union, the United States has not historically placed restrictions on the transfer of personal data overseas. The new CFIUS rules, however, are the latest evidence of a gradual shift toward skepticism of foreign data access. In addition to CFIUS’ enhanced review of foreign investments, foreign intelligence-gathering activities involving data transfers are also being aggressively countered by the US government, as illustrated by recent indictments of Chinese intelligence officials for orchestrating the major data breach of a credit bureau. Similarly, foreign-operated technology services are increasingly treated with heightened scrutiny. Last fall, for example, a viral image-editing application based in Russia triggered Congressional investigations and public scrutiny over its transfer of data overseas. As federal privacy legislation continues to (slowly) work its way through Congress, it is possible these concerns may be addressed in a future federal privacy law.

National Law Review, Volumess X, Number 49