LAW AND POLICY INSIGHT | MAY 2, 2019 | AUTHOR: HDEEL ABDELHADY

Foreign Investment, National Security, and Personal Data: Grindr's Perfect Storm*

Is a dating app a national security asset? Yes, in some cases. Foreign investment in U.S. businesses that collect and maintain U.S. citizens' sensitive personal data is subject to national security reviews, mitigation measures, and, potentially, divestment orders. From social networking to financial services to healthcare to consumer retail, companies across sectors collect, maintain, and have access to the sensitive personal data of U.S. citizens. The implications of the personal data-national security nexus are potentially wide-ranging for foreign investment in U.S. businesses (which can include companies incorporated overseas and engaged in interstate commerce in the United States).

Personal Data as National Security Asset: CFIUS Orders Kunlun to Divest of Grindr

In March news outlets began reporting that the Committee on Foreign Investment in the United States (**CFIUS**) had ordered Chinese company Beijing KunLun Wanwei Technologies (**Kunlun**) to sell Grindr, the dating app wholly owned by Kunlun. Later it was reported that CFIUS has concluded a national security agreement with Kunlun that requires the company to sell Grindr by June 30, 2020. In the meantime, Kunlun is reportedly prohibited from "accessing information" about Grindr's users and transmitting "sensitive information to entities based in China." If Kunlun does not sell Grinder by the June 2020 deadline, the national security agreement with CFIUS is said to require the company to "sign the app over to a trustee."

For those unfamiliar with U.S. national security-based controls of foreign investment, a government-ordered divestment of a dating app on national security grounds may arouse incredulity. But CFIUS' action vis-à-vis Kunlun and Grindr is consistent with its long-standing and recently expanded authority to conduct national security-based reviews of proposed and existing foreign investment in the United States. Importantly, the Grindr divestment order clearly illustrates U.S. government concerns about certain foreign access to U.S. citizens' "sensitive" personal data, particularly the exploitation of such data for foreign espionage operations.

Foreign Investment Risk Review Modernization Act of 2018: Expansion of CFIUS' Authority

Enacted in August 2018 as part of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, (**NDAA**), the Foreign Risk Review Modernization Act of 2018 (**FIRRMA**) broadened and strengthened CFIUS' authority to review foreign investment in the United States on national security grounds. FIRRMA, along with the Export Control Reform Act of 2018 (**ECRA**) and other legislation included in the NDAA, advances intertwined national policies on which there is bipartisan consensus and

support in Congress and the executive branch, including: (1) protecting the United States' technological edge vis-à-vis foreign rivals (principally but not exclusively China) and (2) ensuring that foreign access to and participation in U.S. technology is controlled or blocked as needed to safeguard national security.[2]

CFIUS' Authority to Review Foreign Investment in U.S. Businesses That Transact in Personal Data

FIRRMA enlarges the scope of investments subject to CFIUS' national security review authority to include, among other investments (*i.e.*, "covered transactions"), direct or indirect foreign investment in an unaffiliated U.S. business that "**maintains or collects sensitive personal data of United States citizens that may be exploited in a manner that threatens national security**" where one of the following two criteria are met:

(1) the investment transaction would result in the foreign investor(s) having (i) access to "material nonpublic information;" (ii) membership, observer, or nomination rights as to the U.S. business' board of directors or "equivalent governing body;" or, (iii) "any involvement in substantive decision making," or

(2) the foreign investor is designated by future CFIUS regulations as "foreign person" of concern, because, for example, the foreign investor is "connected to a foreign country or foreign government."[3] FIRRMA's requirement that CFIUS, in promulgating regulations, consider foreign investors' ties to foreign countries or governments clearly applies in the present environment to China and Chinese companies that various U.S. officials have described as being arms of or closely connected to the Chinese government or Chinese Communist Party (*e.g.*, Huawei).

CFIUS' Action Vis-à-Vis Grindr Appears to Be Pursuant to Pre-FIRRMA Authority

While FIRRMA expressly treats the sensitive personal data of U.S. citizens as a national security asset in the case of certain foreign investments, CFIUS' action with respect to Kunlun and Grindr was not taken pursuant to FIRRMA. FIRRMA's provisions that apply to sensitive personal data have not yet taken effect. Nor are investments in U.S. businesses that transact in sensitive personal data included in CFIUS' Pilot Program.[4] Accordingly, in ordering Kunlun to divest itself of Grindr, CFIUS appears to have acted pursuant to pre-FIRRMA authorities that include the power to review, investigate, and take action—such as mandating divestment or the adoption of mitigation measures—as to previously concluded transactions.

Not a Privacy Issue: Links Between Personal Data and Foreign Espionage

FIRRMA's applicability to foreign investment in U.S. businesses that transact in U.S. citizens' personal data is not driven by privacy concerns. Rather, U.S. agencies and officials have identified foreign access to sensitive personal data as a national security threat because personal identifying information (such as health, financial, and other data) can be used as a tool of foreign espionage. Given the nature of U.S. government concerns about certain foreign parties' access to sensitive personal data, the concerns should be taken seriously by foreign investors, relevant U.S. businesses, and other parties in the investment ecosystem (*e.g.*, U.S. co-investors).

Key Takeaways: Foreign Investment in the United States and Personal Data

Foreign investors, U.S. businesses that transact in U.S. citizens' personal data, and U.S. and foreign entities in the investment ecosystem (*e.g.*, private equity firms, investment banks) should note the following key points:

(1) Certain foreign access to personally identifying information of U.S. citizens is a national security issue from the perspective of U.S. law and U.S. officials and agencies. This is true in cases in which personal data is accessed by illicit means (*e.g.,* malign cyber operations) or by lawful means, such as by investment and other commercial transactions.

(2) While FIRRMA's provisions expanding CFIUS' authority to intervene in foreign investment involving U.S. citizens' sensitive personal data have not yet taken effect, CFIUS has acted pursuant to pre-FIRRMA legal authorities to retroactively review, investigate, and order foreign investors to dispose of their holdings. CFIUS' action vis-à-vis Kunlun and Grindr is one example.

(3) CFIUS' authority to look back at previously concluded transactions predates FIRRMA. Parties to proposed, pending, or concluded foreign investments in U.S. businesses that transact in the sensitive personal data of U.S. citizens should assess the potential for CFIUS action and determine if notifications or filings to CFIUS should be made, as appropriate (or as required in cases of investments proposed or pending on or after November 10, 2018 and subject to the CFIUS Pilot Program's mandatory declarations and notice requirements).

(4) "Sensitive personal data," while not defined by FIRRMA, should be viewed broadly and in U.S. national security context for purposes of assessing whether a foreign investment might come within CFIUS' purview. Relatedly, it should not be assumed that personal data collected, compiled, and maintained in contexts seemingly unrelated to national security (*e.g.*, consumer retail) is irrelevant to national security from the perspective of CFIUS and the officials and agencies that inform CFIUS priorities.

(5) Parties directly and indirectly involved in foreign investment transactions should understand that CFIUS alone does not determine national security concerns pertinent to foreign investment. The intelligence community, the Department of Justice, and other authorities are central to the identification of national security risks and the development of counter-measures. Thus, to understand the expanding foreign investment and national security landscape, it is insufficient to focus only news reports of CFIUS' actions, CFIUS' annual reports to Congress (the public portions), or rulemaking or guidance issued by or concerning CFIUS (through the Treasury Department). Parties needing to understand the national security-foreign investment landscape should broaden the scope of their information gathering to capture the various streams and sources relevant information, as well as broad context.■

MASSPOINT PUBLICATIONS

TECHNOLOGY & NATIONAL SECURITY

- China's Rare Earth Exports: End Use and End User Controls Coming? , June 2, 2019.
- Tech War: U.S. Whole-of-Government Approach to China is a Force Multiplier, May 2, 2019.
- Huawei, Questions About Ownership, and the Foreign Agents Registration Act, April 24, 2019.
- Protect Our Universities Act Restricts Foreign Student Participation in "Sensitive" Academic Research, May 15, 2019.
- What Academia Should Know About the DOJ's China Initiative , Jan. 29, 2019.
- Infographic: U.S.-China Trade and Policy Issues, Jan. 10, 2019.
- Critical Minerals, National Security & Supply Chains: American Bar Association-MassPoint PLLC (Audio), Jan. 16, 2019.
- Brain Drain: Emerging Technologies Export Controls Could Spur Tech Inversions, NOV. 29, 2018.
- Brain Drain: Emerging Technologies Export Controls Could Spur Tech Inversions , Nov. 29, 2018.
- BIS Rulemaking on Emerging Technologies Export Controls-Analysis , Nov. 27, 2018.
- Tech Wars: Restrictions on Foreign Access to U.S. Technology, Oct. 26, 2018.

Author Contact, More Information

Hdeel Abdelhady is Principal at MassPoint Legal and Strategy Advisory PLLC and covers foreign investment and national security in law practice and in her law school course on the Regulation of Foreign Access to U.S. Technology. To learn more about this piece and MassPoint's related services, write to habdelhady@masspointpllc.com.

Notes

[*] This publication is an abbreviated version of a detailed briefing provided to clients and friends of MassPoint. Please write to habdelhady@masspointpllc.com for additional information.

[2] FIRRMA and ECRA together advance national security objectives around technology. As explained in an earlier MassPoint update, ECRA declares that the "national security of the United States requires that the United States maintain its leadership in the science, technology, engineering, and manufacturing sectors, including in foundational technology that is essential to innovation." With FIRRMA, ECRA "lays the groundwork for strengthened controls of transfers of U.S.-origin technologies—whether by exports or commercial or other transactions—deemed essential to U.S. national security, which includes maintaining both U.S. military and industrial and innovation superiority vis-à-vis other nations (such as China)." MassPoint PLLC, BIS Rulemaking on Emerging Technologies Export Controls- Analysis, Nov. 25, 2018.

In addition, the NDAA included provisions that exclude foreign companies, such as Huawei and ZTE, from federal government and private telecommunications supply chains. *See* Hdeel Abdelhady, Tech Wars: National Security-Based Restrictions on Foreign Access to U.S. Technology, Oct. 19, 2019.

[3] 50 U.S.C. § 4565.

[4] FIRRMA authorized CFIUS to institute, at its discretion, pilot programs to implement FIRRMA's provisions. CFIUS has established a pilot program applicable to certain non-controlling foreign investment in "critical technologies" related to specific industries (*e.g.,* semiconductors). Foreign investment in U.S. businesses that transact in U.S. citizens' sensitive personal data are not targeted (primarily) by the CFIUS pilot program now in effect (as of November 10, 2018).