PROMINENT DIVESTITURE ORDERS DEMONSTRATE CFIUS'S FOCUS ON ACCESS TO SENSITIVE PERSONAL DATA AS A NATIONAL SECURITY CONCERN

Date: 7 May 2019

U.S. International Trade Alert

By: Steven F. Hill, Jeffrey Orenstein, Lana A. Yaghi, Erica L. Bakies, Michael J. O'Neil, Stacy J. Ettinger

Two major actions by the Committee on Foreign Investment in the United States ("CFIUS") have recently come to light that underscore the significant risks of investments in U.S. businesses that have large volumes of sensitive personal information of U.S. citizens. According to media reports, CFIUS, the multi-agency federal entity that has jurisdiction to review foreign acquisitions of and investments in U.S. businesses for national security threats, has required two separate Chinese investors to divest of their shareholding in U.S. social media companies, based on data privacy concerns. In particular, Beijing Kunlun Tech Co. Ltd. ("Kunlun"), a Chinese gaming company, is being required to divest its 100% ownership of Grindr, LLC, an LGBTQ dating app, which Kunlun had acquired in two separate transactions in 2016 and 2018 for $93 million and $150 million, respectively.[1] Shortly thereafter, it was reported that CFIUS has pressured iCarbonX, a Chinese genome company, to divest of its majority ownership in PatientsLikeMe, a U.S. company that provides a platform for patients with the same diseases to connect with one another and track and share their own experiences.[2]

While access to sensitive personal data has historically not been considered a matter of national security, CFIUS has increasingly focused on this area in light of multiple high-profile data privacy breaches, including some that U.S. authorities believe have originated in China. Last August, Congress formalized data privacy as part of CFIUS's review jurisdiction in the Foreign Investment Risk Review Modernization Act of 2018 ("FIRRMA") by instructing the Committee to examine investments in U.S. businesses that maintain or collect "sensitive personal data of United States citizens that may be exploited in a manner that threatens national security."[3] As part of its authority to review foreign acquisitions and investments, CFIUS can require transactions be restructured, modified, or even blocked to mitigate a national security threat. CFIUS can also reach back to completed transactions that were not cleared by a review prior to closing, analyze them for national security concerns, and order divestiture of shares or business assets by a foreign owner, if the circumstances warrant.

It is widely understood that CFIUS had significant concerns over the vulnerability of the large volumes of personal and sensitive data held by these companies. According to Grindr's website, the app collects location and distance information; messages, including photos, location, audio, and video sent via messages; and user-provided profile information, including name, relationship status, height, weight, HIV status, and date last tested for the HIV virus, among other information.[4] PatientsLikeMe likewise collects both "Restricted Data," which are data that could reasonably be used to identify a particular user, and "Shared Data," which is information that the user shares on the platform.[5] Examples of Restricted Data include the user's name, email, mailing address, date of birth, and various genome analyses. Shared Data includes biographic and demographic information, condition/disease information, treatment information, symptom information, laboratory test results and biomarkers, the status of individual genes or variants, among other information such as family histories.

CFIUS's concern with access to this type of sensitive, confidential personal and medical data stems from its

potential abuse by a foreign power to surveil, influence, or even blackmail or threaten individuals. For example, misuse of Grindr geo-location and HIV status information could expose the app's users to surveillance and potentially arrest and imprisonment in certain jurisdictions with anti-LGBTQ laws or practices. Additionally, some users may be U.S. government or military personnel and release of such information could expose them to manipulation or exploitation.

These divestiture orders also indicate CFIUS's increased focus on completed transactions that were not previously reviewed and the risks of closing on a transaction without voluntarily notifying CFIUS and seeking clearance. CFIUS recently established a dedicated office to identify transactions subject to its jurisdiction that were not notified to the Committee and for which information is reasonably available. The Grindr and PatientsLikeMe acquisitions by foreign investors were not notified to CFIUS. The divestiture orders indicate that there are likely a number of non-notified investments from the past several years that could be vulnerable for a post-transaction review based on CFIUS's expanded jurisdiction. They also indicate that even small acquisitions and investments with seemingly limited risk could have an enhanced risk profile as a result of an increase in the growth and exposure of a company.

Finally, the risk with the Grindr and PatientsLikeMe transactions was no doubt heightened due to the presence of Chinese investors. Although CFIUS officially states that no specific country is singled out for enhanced review, in reality due to concerns by U.S. policymakers over data privacy, intellectual property protections, and an organized effort to develop technologies and industries in key strategic areas, CFIUS applies much greater scrutiny to deals with Chinese acquirers and investors. As a result, CFIUS is taking a more aggressive approach toward China deals regardless of the industry sector that they involve.

For more information regarding this topic or any other related issues, the international trade practice group of K&L Gates is available to assist.

Notes

[1] Carl O'Donnell, Liana B. Baker, and Echo Wang, *Exclusive: Told U.S. security at risk, Chinese firm seeks to sell Grindr dating app*, Reuters (Mar. 27, 2019), https://www.reuters.com/article/us-grindr-m-a-exclusive/exclusive-us-pushes-chinese-owner-of-grindr-to-divest-the-dating-app-sources-idUSKCN1R809L; David E. Sanger, *Grindr Is Owned by a Chinese Firm, and the U.S. Is Trying to Force It to Sell*, The New York Times (Mar. 28, 2019), https://www.nytimes.com/2019/03/28/us/politics/grindr-china-national-security.html.

[2] Christina Farr and Ari Levy, *The Trump administration is forcing this health start-up that took Chinese money into a fire sale*, CNBC (Apr. 4, 2019), https://www.cnbc.com/2019/04/04/cfius-forces-patientslikeme-into-fire-sale-booting-chinese-investor.html.

[3] 50 U.S.C. § 4565(a)(4)(B)(iii)(III).

[4] *Grindr Privacy and Cookie Policy*, Grindr, https://www.grindr.com/privacy-policy/#collect_EN (last visited May 2, 2019).

[5] *Welcome to the privacy policy*, PatientsLikeMe, https://www.patientslikeme.com/about/privacy (last visited May 2, 2019).

KEY CONTACTS

STEVEN F. HILL
PARTNER

WASHINGTON DC
+1.202.778.9384
STEVEN.HILL@KLGATES.COM

JEFFREY ORENSTEIN
PARTNER

WASHINGTON DC
+1.202.778.9465
JEFFREY.ORENSTEIN@KLGATES.COM

