New York Law Journal

NEW YORK LAW JOURNAL SPECIAL REPORT

An ALM Publication

Cybersecurity

WWW.NYLJ.COM

VOLUME 263—NO. 40

MONDAY, MARCH 2, 2020

SHUTTERSTOCK

Risk of Foreign Access to U.S. Data Spur Government To Act, But Economic Concerns Loom

BY BORIS SEGALIS, KEVIN KING AND JINA JOHN

For the past decade, "big data" was the buzzword for leveraging sophisticated analytics over large data pools to gain deep insights into consumers' shopping behavior. Media stories, such as a retailer determining a woman's pregnancy status by analyzing her hand cream purchases, captivated the imagination and raised concerns about data ethics. With Edward Snowden's revelations, the public's awareness of big data pivoted to concerns about living in a surveillance state. By the time the nation recognized that big data turned from a tool to gain insight into the human mind into the means for attacking it, the largest, coordinated data attack was in the rear view mirror, as we were forced to face the aftermath of foreign interference in the 2016 elections. In that attack, the perpetrators weaponized data to understand their audience, to tailor their messages, and to deliver the messages with impact to precisely targeted audiences.

The 2016 foreign influence campaign shocked the public conscience and forced legislators and regulators to recognize the gaping holes in the country's ability to detect and mitigate threats posed by weaponized data. Since then, the public has grown wary of such cyber risks, suspecting that any foreign-developed apps are intelligence tools, or immediately fearing foreign powers may have intervened in the recent Iowa caucuses when the caucus-reporting app did not function as anticipated. These events have led legislators and regula-

BORIS SEGALIS *is a New York City-based partner at Cooley and vice chair of the firm's cyber/data/privacy practice.* KEVIN KING *is a Washington D.C.-based partner and* JINA JOHN *is a New York City-based associate at the firm.*

tors to begin formalizing their efforts to check foreign access to Americans' data. But the unstructured, diffuse nature of data means that these efforts may result in a false trade-off: the appearance of improved security at the cost of chilling foreign investment in U.S. emerging companies that focus on data-driven products and services, hurting the economy.

In retrospect, trends in commercial contracts and regulatory enforcement of the past decade may have been early signs of recognizing the threat of data weaponization. For example, for years, companies routinely prohibited vendors from providing customer support from certain countries, largely out of intellectual property concerns. On the government side, in 2010, the Federal Trade Commission (FTC) intervened in XY magazine bankruptcy to prevent the sale of personal details of the magazine's customer base—primarily young homosexual men. In bankruptcy, the data was viewed as an asset to be sold for the benefit of the magazine's creditors. Without articulating a rationale, by acting, the FTC arguably demonstrated awareness that sensitive personal data, such as a person's sexual orientation, collected on a large scale, could be weaponized against those individuals. The FTC suggested that divulging this nonpublic information could expose these individuals to harm, since those around them, including their families, may not have been aware of their sexual orientation.

More recently, federal agencies have taken a more direct approach to address the threat of foreign access to U.S. data. In the wake of the Cambridge Analytica scandal, the FTC exercised its Section 5 authority to establish a precedent that U.S. companies should be cautious when sharing personal data with foreign entities, like SCL Group and Cambridge Analytica. But the FTC's ability to leverage its enforcement power is limited because Section 5 does not authorize the Commission to prohibit foreign access to data. Rather, the FTC can only step in where it can allege that data access was deceptive or not properly disclosed to consumers.

Filling this void, the Committee on Foreign Investment in the Unites States (CFIUS) has stepped in to attempt to affirmatively check at least one facet of data access—corporate transactions that provide control over or access to "sensitive personal data."

> As the United States continues to navigate regulating foreign access to American's data, the government should consider lessons **learned from past efforts to limit trade to protect national security.**

CFIUS, a permanent, interagency committee tasked with reviewing foreign acquisitions and investments in U.S. businesses for potential national security risks, has sweeping authority to review, suspend, modify, or prohibit transactions in order to address perceived risks to U.S. national security. In recent years, CFIUS has exercised its broad authority to intervene in transactions that involve the sensitive data of Americans.

CFIUS has acted preemptively to block foreign acquisitions of U.S. companies that collect or store sensitive data. For example, in January 2018, the Committee blocked the proposed acquisition by Alibaba affiliate Ant Financial of MoneyGram, a U.S.-based global money transfer company. Reportedly, CFIUS blocked the deal on concerns that Ant Financial would facilitate the Chinese government's access to Americans' data that MoneyGram processed, including financial data. CFIUS blocked the deal despite Ant Financial's proposals to mitigate these risks. CFIUS similarly tried to block the sale of mobile marketing firm AppLovin to Orient Hontai Capital, reportedly out of concern that the security of user data in the hands of the acquiring company would be compromised.

Notably, CFIUS can also act after the fact, by forcing divestiture. In 2019, for example, CFIUS compelled iCarbonX to divest its majority stake in PatientsLikeMe, an online community for patients seeking treatments for common health conditions, reportedly to prevent foreign access to the company's database of patient information. That same year, CFIUS ordered Kunlun Tech to divest its ownership of Grindr, a popular LGBT+ dating app. Commentators suggested that CFIUS acted out of data privacy concerns, especially risks to U.S. officials or government contractors who could face discrimination or compromise. In these instances, CFIUS took action over concerns about foreign access to large swaths of sensitive personal information, such as health information, financial information, and sexual orientation, through those platforms.

This year, CFIUS's review authority expanded to cover foreign investments in U.S. companies that afford foreign persons control over or access to "sensitive personal data." The expanded authority comes from the Foreign Investment Risk Review Modernization

Act of 2018 (FIRRMA), which Congress passed in 2018 as a response to concerns with the high level of Chinese investment in U.S. technology companies. In response to FIRRMA, CFIUS recently issued final regulations that give the Committee authority to review direct or indirect foreign investments in US businesses that maintain or collect, directly or indirectly, "sensitive personal data" of U.S. citizens, where the foreign investor may acquire control or other governance rights in the target business, or acquire access to the sensitive personal data maintained by the U.S. business. The regulation defines "sensitive personal data" to include location data, biometric data, certain consumer report data, health data, and certain financial data.

The regulations effectively codify the position that foreign access to personal data may pose a national security risk. CFIUS has now put companies that collect or maintain sensitive personal data on notice that foreign investments may raise national security concerns that require CFIUS review. The expansive definition of sensitive personal data means that a broad swath of U.S. emerging companies that are active in capital markets and routinely attract foreign investment may be subject to CFIUS's review. This possibility could delay or block investment, create uncertainty, and further the chilling effect on foreign investment, as evidenced by the 90 percent decline in Chinese direct investment in the United States from 2016 to 2018. See Uptin Saiidi, "China's Foreign Direct Investment Into the US Dropped Precipitously in 2018, Data Show," CNBC, Jan. 15, 2019.

Furthermore, where a foreign government is involved at a certain threshold in the investment transaction in a U.S. business that maintains sensitive personal data, the regulations mandate submitting a pre-closing filing to CFIUS. Failure to submit a required filing can subject the parties to penalties up to the amount of the transaction. Even where a covered transaction does not trigger a mandatory filing, CFIUS has the power to require the parties to adopt mitigation measures to address perceived national security issues.

While the efforts by Congress, the FTC and CFIUS demonstrate the government's interest in establishing controls on foreign access to U.S. data, the vastness and diversity of global data flows and data access mechanisms may make regulators feel like they are using a toy telescope to study the universe. The record of existing efforts on controlling cross-border data flows are not encouraging. For example, commentators estimate that under 10% of flows of personal data flows from Europe to the United States are captured by the EU's efforts to control outflows of personal data to the United States through legal mechanisms, such as Standard Contractual Clauses, Binding Corporate Rules, and U.S.-EU Privacy Shield. The vast majority of the data reportedly flows freely across the Atlantic.

Even though the increased regulation comes in response to the 2016 influence campaign, the powers afforded the FTC and CFIUS would not have prevented or stopped that campaign. The FTC's applicable authority limits the Commission's power to prevent data misuse. Instead, the FTC only can penalize ongoing or past conduct that the agency alleges to be misleading or deceptive. CFIUS can only impose its restriction in connection with foreign investments (i.e., mergers, acquisitions, takeovers, investments, or conversions of contingent equity interests), not any other transfer of data, such as those that occur in the course of dealings with foreign service providers or in connection with other commercial transactions.

CFIUS's authority is in some respects a blunt instrument, the application of which is a matter of regulatory discretion. The mere possibility of enforcement will undoubtedly deter foreign investment into data-driven companies. In an age where there's an app for everything, from booking travel to grocery shopping to buying insurance to finding the best selfie angle, there may be an outsized impact on emerging companies.

As the United States continues to navigate regulating foreign access to American's data, the government should consider lessons learned from past efforts to limit trade to protect national security. For example, in 1999, fearing foreign access to U.S. satellite technology, the U.S. imposed export controls limiting foreign sales of U.S. commercial satellites. The result: The U.S. market in global satellite manufacturing shrunk in half from 1999 to 2013, and industry groups estimate that U.S. manufacturers lost $21 billion in satellite manufacturing revenue from between 1999 and 2009 alone. See Stephen Clark, "Obama Signs Law Easing Satellite Export Controls," Spaceflight Now (Jan. 3, 2013). This history suggests that efforts to stem foreign access to sensitive personal data should be narrowly tailored to facilitate security and limit economic impact.