FDI AND NATIONAL SECURITY: RISKS FROM A BIG TECH BREAKUP, AND CFIUS'S ROLE TO MITIGATE

BY BENJAMIN CURLEY & THOMAS FEDDO[1]

1 Respectively, MBA Candidate at Columbia Business School, former Vice President at Barclay's Investment Bank; and founder of The Rubicon Advisors, LLC, former U.S. Assistant Secretary of the Treasury, respectively.

CPI ANTITRUST CHRONICLE JUNE 2022

FDI AND NATIONAL SECURITY: RISKS FROM A BIG TECH BREAKUP, AND CFIUS'S ROLE TO MITIGATE

By Benjamin Curley & Thomas Feddo

Breaking up American "Big Tech" companies has in recent years been a topic of much discussion by policymakers and legislators across the political spectrum. Arguments for and against breakup offer various justifications and considerations, but less-discussed potential national security risks lurk within the larger debate — including that breaking up Big Tech could leave American intellectual property, data, technology, and know-how up for grabs by strategic competitors. The interagency U.S. Committee on Foreign Investment in the United States ("CFIUS") was created to protect against this kind of national security risk, but it has its limitations, particularly in terms of resourcing and the inherent opacity of venture capital and private investment. Given these limitations, policymakers who pursue the path of a Big Tech breakup should be aware of this risk and be prepared to address it; CFIUS and other national security authorities will need to be appropriately resourced and staffed.

The call to break up American "Big Tech" is one of the few policy proposals in Washington on which individuals across the political spectrum seem to agree, albeit for different reasons. Arguments for and against breakup often touch on antitrust law as well as geopolitics, and both camps have claims worthy of consideration. There may also be unintended consequences relating to national security, however, of breaking up large American technology companies. These consequences have not garnered a great deal of attention in the larger debate. The aftermath of a Big Tech breakup could push emerging technologies that are vital to national security into adversarial hands, and the interagency U.S. Committee on Foreign Investment in the United States ("CFIUS") will stand in the breach. Regulators and legislators who pursue the path of a Big Tech breakup should be aware of this risk and be prepared to mitigate it, lest they find out that they have walked us down a primrose path.

I. BIG TECH, ANTITRUST, AND GEOPOLITICS

American Big Tech can loosely be defined as the five largest information technology companies in the United States: Apple, Microsoft, Alphabet, Amazon, and Meta. Their combined revenues of over $1.4 trillion in 2021 would be the 14th-largest economy in the world by GDP, just behind Brazil — a country of over 200 million people — and their global reach and influence have raised uncomfortable questions about the survivability of the Westphalian system of nation-state power that has dominated since 1648.[2]

The expansion of the Big Tech companies and the immense power they have accrued has knit together a patchwork quilt of supporters and detractors. Both Senators Elizabeth Warren (MA) and Ted Cruz (TX) agree that Big Tech has too much power and that the government should reign it in. Senator Warren cites the way Big Tech has "bulldozed competition" through mergers and strong-arm tactics and used American's "private information" for profit as justification for breakup.[3] Senator Cruz has raised concerns about Big Tech's accumulation of "market power and monopoly power" and their censorship policies to advocate for greater regulation and potential breakup.[4] But those who oppose breakup are equally bipartisan.

Senators Mark Warner (VA) and Mike Lee (UT), for example, both have criticized Big Tech and called for greater oversight or regulation around censorship, but have tread lightly around the topic of dissolution. Senator Lee said "We are concerned about privacy, data misuse and bias, but that doesn't fall under the antitrust law. Big isn't necessarily bad."[5] Those cautious about breakup often cite antitrust law as focused on the consumer, and argue that Big Tech companies with their innovative methods and economies of scale have created more competition and lowered costs for consumers. Many opposed to breakup also lean on the geopolitical consequences of dissolution. Senator Warner pushed back against breakup in an interview with CNBC saying, "These are all global companies. Frankly, to have them replaced by Alibaba or Baidu or Tencent — Chinese companies may not be the better alternative."[6] At their peak, before the recent tech crackdown from the Chinese Communist Party ("CCP") Government, Alibaba, Baidu, and Tencent were respectively worth $842 billion, $113 billion, and $950 billion, and closing in on their American competitors.

But breakup advocates have also made justifications on broad geopolitical grounds. In a March 2020 Foreign Affairs article, Ganesh Sitaraman pushed back against views like Senator Warner's, noting that "market concentration in the technology sector . . . means less competition and therefore less innovation, which threatens to leave the United States in a worse position to compete with foreign rivals . . ." and therefore that "breaking up and regulating Big Tech is necessary to protect the United States' democratic freedoms and preserve its ability to compete with and defend against new great-power rivals."[7]

Whether the Big Tech companies violate antitrust laws is up for debate, as is whether fewer, larger, globetrotting tech companies or more of the smaller, nimbler tech companies is better for America's geopolitical interests. What is not up for debate is the research and development

2 Poletti, T., & Owens, J. C. (2022, February 6). *Opinion: $1.4 trillion? Big Tech's pandemic year produces mind-boggling financial results*. MarketWatch. Retrieved from https://www.marketwatch.com/story/1-4-trillion-big-techs-pandemic-year-produces-mind-boggling-financial-results-11644096594.

3 Warren Democrats. (2021). *Break up big tech*. Retrieved from https://2020.elizabethwarren.com/toolkit/break-up-big-tech.

4 *Sen. Cruz: ZERO accountability from Big Tech is dangerous*. Senator Ted Cruz. (2021, April 20). Retrieved from https://www.cruz.senate.gov/newsroom/press-releases/sen-cruz-zero-accountability-from-big-tech-is-dangerous.

5 Yahoo! (2019, September 27). *Big Tech companies look to an unlikely savior: The Republican Party*. Yahoo! Retrieved from https://www.yahoo.com/video/big-tech-companies-look-unlikely-192435789.html.

6 CNBC (2020, July 30). *Sen. Mark Warner opposes Big Tech Breakup – for now*. CNBC. Retrieved from https://www.cnbc.com/2020/07/30/sen-warner-against-big-tech-break-up-for-now-warns-chinese-companies-would-replace-them.html.

7 Sitaraman, G. (2020). *Too Big to Prevail*. Foreign Affairs. Retrieved from https://www.foreignaffairs.com/articles/2020-02-10/too-big-prevail.

("R&D") expenditure and acquisitions undertaken by Big Tech companies. These five companies spent a combined $155 billion on R&D in 2021.[8] [9] [10] [11] [12]By way of comparison, the five top U.S. defense contractors (Boeing, Lockheed Martin, Raytheon Technologies, Northrop Grumman, and General Dynamics) — the companies that traditionally have underpinned the United States and its allies in their military preeminence — spent less than $8 billion on R&D,[13] [14] [15] [16] [17]combined.

As the nature of geopolitical conflict evolves, the areas where Big Tech companies have spent their R&D dollars internally or on acquisitions — such as cloud computing, autonomy, artificial intelligence, and mobile applications — have become more relevant to protecting national security. Policymakers who are breakup advocates may be correct when they accuse Big Tech of acquiring companies to kill competition, and it is up to Congress and regulators to decide a course of action; but one result of Big Tech's acquisitions and capital injections has been that emerging technology and intellectual property have remained under the umbrella of a U.S.-domiciled company.

II. FDI AND NATIONAL SECURITY RISK

An unintended consequence of a government-directed Big Tech breakup could be the opposite: emerging technology and related intellectual property with national security applications being exploited by America's adversaries. As the character of technologies crucial to national security has expanded from traditional fields like aeronautics and munitions to less obvious sub-sectors such as autonomy, agriculture, and dating apps, the risk that these technologies fall into the wrong hands has become more complicated.

National security risk from a foreign acquisition or investment can manifest in a number of ways, including access to sensitive data like genetic or geolocation information or to critical infrastructure like the country's electric grid or SCADA systems; or compromising cybersecurity or supply chain integrity and resiliency in the defense industrial base; or providing proximity to sensitive government installations. And, perhaps most prominent in the context of forcing Big Tech to shed certain businesses, the risk may be transferring technology, know-how, and intellectual property underpinning cutting-edge innovations.

With what is essentially a "Fourth Industrial Revolution" well under way — including the rapidly expanding fields of space, robotics, nanotechnology, quantum computing, and energy, for example — the lines between these innovations' commercial applications and potential military uses are increasingly blurred.

Unlike in the past, when significant innovation came from the military industrial base, today much more tech advancement happens in the private sector. According to Dr. Will Roper, former Assistant Secretary of the Air Force for Acquisition, Technology, and Logistics, today the Defense Department represents about 20 percent of the nation's R&D, which is a "complete 180 flip" from the Cold War when 80 percent of American R&D came from the military industrial base.[18]

Most of the innovative private sector companies that make up the remaining 80 percent of the nation's R&D were created to meet the demands of consumers and companies, and often they are unaware that their technology might have a national security application. The fact

8 Yahoo! (n.d.). *Apple Inc. (AAPL) income statement*. Yahoo! Finance. Retrieved from https://finance.yahoo.com/quote/AAPL/financials/.

9 Yahoo! (n.d.). *Alphabet Inc. (GOOGL) income statement*. Yahoo! Finance. Retrieved from https://finance.yahoo.com/quote/GOOGL/financials?p=GOOGL.

10 Yahoo! (n.d.). *Amazon.com, inc. (AMZN) income statement*. Yahoo! Finance. Retrieved from https://finance.yahoo.com/quote/AMZN/financials?p=AMZN.

11 Yahoo! (n.d.). *Microsoft Corporation (MSFT) income statement*. Yahoo! Finance. Retrieved from https://finance.yahoo.com/quote/MSFT/financials?p=MSFT.

12 Yahoo! (n.d.). *Meta Platforms, inc. (FB) income statement*. Yahoo! Finance. Retrieved from https://finance.yahoo.com/quote/FB/financials?p=FB.

13 Yahoo! (n.d.). *The Boeing Company (BA) income statement*. Yahoo! Finance. Retrieved from https://finance.yahoo.com/quote/BA/financials?p=BA.

14 Yahoo! (n.d.). *Lockheed Martin Corporation (LMT) income statement*. Yahoo! Finance. Retrieved from https://finance.yahoo.com/quote/LMT/financials?p=LMT.

15 Yahoo! (n.d.). *Raytheon Technologies Corporation (RTX) income statement*. Yahoo! Finance. Retrieved from https://finance.yahoo.com/quote/RTX/financials?p=RTX.

16 Yahoo! (n.d.). *Northrop Grumman Corporation (NOC) income statement*. Yahoo! Finance. Retrieved from https://finance.yahoo.com/quote/NOC/financials?p=NOC.

17 Yahoo! (n.d.). *General Dynamics Corporation (GD) income statement*. Yahoo! Finance. Retrieved from https://finance.yahoo.com/quote/GD/financials?p=GD.

18 "AFA's vASC 2020: Disruptive Agility for A Disruptive World - Dr. Will Roper." *YouTube*, uploaded by Air and Space Forces Association, 19 Oct. 2020, www.youtube.com/watch?v=kl5_LSI04vE.

is, however, these emerging technologies will be vital to the United States and its allies in maintaining their superiority on the battlefield. What's more, many emerging technologies — such as machine learning, autonomous driving, and biotechnology — rely on unique and extensive types of data that also create novel national security vulnerabilities, including with respect to U.S. citizens' personal data.

Many startup companies and their technology have thrived and matured under the umbrella of Big Tech, taking advantage of the funding stream and human capital across the organizations. To the extent these technologies were back on the market as a result of the government's prompting, some would certainly fail, and others would struggle to secure new capital resources. In the context of today's historic great power competition, America's adversaries would be watching and might attempt to step in as white knights — and not with purely capitalist and benign motives.

This kind of national security risk — resulting from a foreign person or entity acquiring or investing in a U.S. business — is what CFIUS is meant to prevent. CFIUS complements other national security authorities — export controls, the mitigation of foreign ownership, control, or influence ("FOCI"), and the "Team Telecom" committee among them — to protect against various national security risks, including the transfer of technology and know-how that has dual-use applications.

III. CONTEXT: A BRIEF CFIUS HISTORY

CFIUS was created through presidential Executive Order ("E.O.") 11,858, issued by President Ford on May 7, 1975. The E.O. assigned to CFIUS the mission of "monitoring the impact of foreign investment in the United States" and, among other things, "review[ing] investments in the United States which . . . might have major implications for United States national interests."[19] CFIUS could not intercede in a transaction — the authorities given to it were largely passive in nature, although it could make policy recommendations.

Because CFIUS initially had little impact on cross-border deals, policymakers grew concerned that the Committee needed more authority, particularly if U.S. national security was implicated by a foreign acquisition. The upshot was that in 1988 Congress passed the "Exon-Florio Amendment," which modified the Defense Production Act (DPA) of 1950. Under the DPA's new "Section 721," the President could "suspend or prohibit any acquisition, merger, or takeover, of a person engaged in interstate commerce in the United States" to ensure that the transaction did "not threaten to impair the national security."[20] Provided that certain findings were made and a report submitted to Congress, the President could block (or order divestment of) a foreign person's "control" of the U.S. company. Deals were voluntarily submitted to CFIUS, and within 30 days the Committee could initiate a second 45-day period to conduct a national security assessment.[21]

Under the "Byrd Amendment" in 1992, Congress made further changes to CFIUS, including explicitly directing the President to consider "the potential effects of the proposed or pending transaction on United States international technological leadership in areas affecting United States national security."[22] CFIUS was now charged to account for the national security impacts of a cross-border transaction as it related to the nation's technological leadership around the globe.

CFIUS's approval of Dubai Ports World's 2006 acquisition of Peninsular & Oriental Steam Navigation Company, a U.K. firm with U.S. port facilities, instigated even further legislative changes to the Committee's authorities and processes; in 2007 the Foreign Investment and National Security Act ("FINSA") was enacted. FINSA among other things codified CFIUS processes and structure and required that in each transaction the Intelligence Community produce a threat analysis of the foreign investor.[23] CFIUS was also directed to consider whether the acquisition implicated national security because the assets of the U.S. business included "critical technology." The impacts of technology transfer were becoming a growing concern.

In the years after FINSA's enactment, the national security risks from some sources of foreign investment became more stark. Rather than traditional mergers and acquisitions, business transactions increasingly grew in complexity, involved more parties, and included investment vehicles like private equity, venture capital, and SPACs. State-owned or state-directed entities were also more frequently investing in U.S. businesses, raising the risk that national interests rather than financial return might be at play. Finally, China was on the rise, developing into a

19 https://www.archives.gov/federal-register/codification/executive-order/11858.html.

20 Section 5021 of Public Law 100-418 of August 23, 1988 (https://www.congress.gov/100/statute/STATUTE-102/STATUTE-102-Pg1107.pdf).

21 *Id.*

22 Section 837 of Public Law 102-484 of October 23, 1992.

23 Public Law 110-49 of July 26, 2007.

highly consequential "strategic competitor" of the United States. The CCP embraced a philosophy of "civil-military fusion" — what the U.S. State Department has described as China's national strategy to develop military preeminence by "acquiring the intellectual property, key research, and technological advances" of private industry, and scholars and researchers, "systematically reorganizing the Chinese science and technology enterprise to ensure that new innovations simultaneously advance economic and military development."[24]

These factors, plus gaps in CFIUS's jurisdiction identified by policymakers, led to an urgent bipartisan call to overhaul the Committee. In a January 2018 hearing regarding CFIUS reform before the Senate Banking Committee, Senator John Cornyn distilled the challenge:

"It is not just that China poses a threat, though: it's that the kind of threat is unlike anything the U.S. has ever before faced – a powerful economy with coercive, state-driven industrial policies that distort and undermine the free market, married up with an aggressive military modernization and the intent to dominate its own region and potentially beyond.

To close the technology gap with the U.S. and leapfrog ahead of us, China uses both legal and illegal means. One of these tools is investment, which China has weaponized in order to vacuum up U.S. industrial capabilities from American companies that focus on dual-use technologies. China seeks to turn our own technology and know-how against us in an effort to erase our national security advantage."[25]

Senator Cornyn further stated: "China has also been able to exploit minority-position investments in early-stage technology companies in places like Silicon Valley, California, or the "Silicon Hills" in Central Texas to gain access to intellectual property ("IP"), trade secrets, and key personnel."[26]

In August 2018, with overwhelming bipartisan support in both houses of Congress, the Foreign Investment Risk Review Modernization Act ("FIRRMA") became law, initiating the most comprehensive overhaul of CFIUS in its more than 40-year history.[27] The law's preface reiterated congressional motivations, stating in part: "the national security landscape has shifted in recent years, and so has the nature of the investments that pose the greatest potential risk to national security, which warrants an appropriate modernization of the processes and authorities of the Committee on Foreign Investment in the United States . . . ."[28]

FIRRMA made extensive changes to the Committee's processes and jurisdiction. Perhaps most notably, it moved beyond traditional mergers and acquisitions, reaching minority investments that did not convey control over the U.S. business but nonetheless gave the foreign investor access to critical infrastructure, cutting edge technology, or sensitive data, or gave meaningful decision-making authority regarding them.

From its modest beginning in 1975, the Committee's mission has exclusively been to protect national security — while at the same time maintaining the United States' open-investment climate and refraining from interference in the free market. Some policymakers may view CFIUS as a means to address other issues such as impacts on market share in a key domestic industry, jobs, and economic growth — but doing so would shift to a question of national interest rather than one of national security. Decisions could be subject to more parochial and political motives. In FIRRMA's preamble Congress was unequivocal: CFIUS "should continue to review transactions for the purpose of protecting national security and should not consider issues of national interest absent a national security nexus."[29]

IV. BRIEF CFIUS CASE STUDIES

Public reporting in recent years about CFIUS actions — which are confidential by law — provides instructive context regarding how new technologies and the data economy can impact national security. The examples below illustrate the types of companies

24 U.S. Department of State Web site (https://2017-2021.state.gov/military-civil-fusion/index.html).

25 Testimony of Senator John Cornyn of Texas, before the U.S. Senate Committee on Banking, Housing, and Urban Affairs, *CFIUS Reform: Examining the Essential Elements* (January 18, 2018).

26 *Id.*

27 H.R. 5515 of August 13, 2018 at pp. 538-572. (https://home.treasury.gov/sites/default/files/2018-08/The-Foreign-Investment-Risk-Review-Modernization-Act-of-2018-FIRRMA_0.pdf).

28 *Id.* at Section 1702(b)(4)

29 *Id.* at Section 1702(b)(9)

and technologies under the Big Tech umbrella that could implicate national security if they were available for others to invest in or acquire.

A. Biotech and Health-related Tech

The Big Tech firms in recent years have acquired several companies related to biotech, health monitoring, and medical data. In 2016 Apple acquired Gliimpse, a personal health data platform that allows users to collect and share their health data.[30] In 2019 Amazon acquired a digital health startup called Health Navigator, which builds apps for digitized clinical health information for use in telemedicine.[31] In 2021 Alphabet purchased FitBit, a major manufacturer of wearable health and fitness tracking devices.[32]

These types of companies tend to manage some of the most sensitive data about individuals — their health and medical histories, genetic information, and in the case of health and fitness trackers, geolocation data. CFIUS has demonstrated its interest in protecting this data, both by FIRRMA's regulatory framework and by CFIUS's response to certain transactions. FIRRMA's regulations staked out that both health and geolocation data are considered "sensitive personal data" that could "be exploited in a manner that threatens to harm national security," for example, because it could relate to "sensitive U.S. Government personnel or contractors."[33]

In 2017, the Massachusetts healthcare startup, PatientsLikeMe Inc., received a $100 million investment from iCarbonX, a digital health startup backed by the Chinese company Tencent. PatientsLikeMe offered a means for users to submit patient-reported data and combine it with other patients' data to facilitate research and potentially solve diseases.[34] Media reporting explained that in 2019 PatientsLikeMe was "forced to find a buyer after the U.S. government has ordered its majority owner, a Chinese firm, to divest its stake," and noted similar concerns CFIUS had with a Chinese company's acquisition of gay dating app Grindr — i.e. that "China would use information about American officials' sexual orientation or dating habits *to blackmail or influence them*. . . . PatientsLikeMe potentially presents similar unease, because the company collects data on users who set up profiles so they can ask and answer questions about their conditions." (emphasis added)[35]

B. Autonomous Vehicles ("AVs")

Big Tech has dedicated significant attention and resources to autonomous driving and integrated technologies such as robotics. Amazon in 2020 acquired Zoox, a self-driving vehicle startup focused on building autonomous taxis;[36] and in 2017 it acquired the "urban delivery" robotics startup Dispatch.[37] Apple in 2018 acquired the startup Drive.ai, a maker of artificial intelligence for AVs;[38] in 2013 it had acquired PrimeSense, an Israeli startup that designed sensors and systems that could track objects and their movements in three dimensions.[39] [40] Alphabet has made

30 Farr, C. (2016, September 26). *Apple Acquires Personal Health Data Startup Gliimpse*. Fast Company. Retrieved from https://www.fastcompany.com/3062865/apple-acquires-personal-health-data-startup-gliimpse.

31 *Amazon buys Health Navigator, founded by Chicago ER Doctor David Thompson*. Healthcare Weekly. (2019, November 18). Retrieved from https://healthcareweekly.com/amazon-health-navigator/.

32 *The 53 digital health mergers and acquisitions we covered in 2019*. MobiHealthNews. (2019, December 23). Retrieved from https://www.mobihealthnews.com/news/north-america/53-digital-health-mergers-and-acquisitions-we-covered-2019.

33 84 Fed Reg 50177-8 (https://www.govinfo.gov/content/pkg/FR-2019-09-24/pdf/2019-20099.pdf).

34 Squire Patton Boggs (US) LLP, *CFIUS Filing in Mitigation: iCarbonX and PatientsLikeMe Inc.*, The National Law Review, Volume IX, Number 192. Retrieved from https://www.natlawreview.com/article/cfius-filing-mitigation-icarbonx-and-patientslikeme-inc.

35 Christina Farr, A. L. (2019, April 4). *The trump administration is forcing this health start-up that took Chinese money into a fire sale.* CNBC. Retrieved from https://www.cnbc.com/2019/04/04/cfius-forces-patientslikeme-into-fire-sale-booting-chinese-investor.html.

36 NBCUniversal News Group. (2020, June 26). *Why did Amazon just buy autonomous driving start-up Zoox?* NBCNews.com. Retrieved from https://www.nbcnews.com/business/autos/amazon-closes-1-2b-deal-autonomous-driving-start-zoox-n1232295.

37 Harris, M. (2019, February 7). *Amazon quietly acquired Robotics Company Dispatch to build scout*. TechCrunch. Retrieved from https://techcrunch.com/2019/02/07/meet-the-tiny-startup-that-helped-build-amazons-scout-robot/.

38 Chaturvedi, A. (2019, June 27). *Apple's acquisition of Drive.AI to boost its Autonomous Vehicle program*. Geospatial World. Retrieved from https://www.geospatialworld.net/blogs/apple-acquisition-drive-ai/.

39 MIT Technology Review. (n.d.). *Primesense*. MIT Technology Review. Retrieved from http://www2.technologyreview.com/tr50/primesense/.

40 Tobe, F. (2021, July 7). *Apple, Amazon, and now google: An exciting time for robotics*. IEEE Spectrum. Retrieved from https://spectrum.ieee.org/apple-amazon-and-now-google-an-exciting-time-for-robotics.

extensive investments in the autonomous vehicle sector, primarily through its self-driving vehicle subsidiary Waymo,[41] and has been very active in the robotics sector, snapping up companies several years ago and then revitalizing its robotics efforts in recent years.[42]

Several national security risks underlie AV industry technology, ranging from technology transfer of cutting-edge integrated technologies like robotics, LiDAR mapping, and artificial intelligence, all of which could be utilized in developing sophisticated military AVs or other military equipment.[43] AVs rely "on software, computing, and connectivity, [and] could be a new vector for cybersecurity risks."[44] There could also be risks from external manipulation of systems, surveillance, espionage, and the compromise of massive data troves collected by operating these complex systems.[45]

CFIUS has frequently intervened in foreign investments in AV companies. In early 2021, the Committee requested that TuSimple Holdings Inc., an autonomous trucking company, file regarding its acquisition by a Cayman company that was held in part by a Chinese technology company.[46] In the end, the deal parties entered into a National Security Agreement with CFIUS promising "to keep U.S.-developed core technology out of China," remove two board members with connections to a Chinese technology company, abide by an equity standstill provision, and "limit access to certain data and adopt a technology control plan, appoint a security officer and a security director, and establish a board-level government security committee to be chaired by the security director. . . . Protecting U.S.-developed technology from China was a key issue."[47]

Similarly, in 2019 the Committee intervened in Japanese venture firm SoftBank's $2.25 billion investment in General Motor's majority-owned AV company Cruise.[48] "CFIUS approved the investment based on fresh assurances that Cruise's technology would be completely off limits to SoftBank, whose investments in Chinese mobility firms have rattled U.S. authorities."[49] And in 2018 CFIUS intervened in the investment by DD Global Holdings Limited into the startup Canoo Technologies, which was building "a new multipurpose electric vehicle aimed at last-mile deliveries and other small businesses."[50] One of the U.S. company's key investors led a "massive investment firm in China and is the son-in-law of Jia Qinglin who was the fourth-most senior leader in China before retiring in 2013."[51] The Committee imposed a national security agreement that required, among other things, limitations on DD Global's governance rights, data protections and restrictions, restrictions on voting rights, and a reduction of equity stake to less than 10 percent.[52]

CFIUS has also been active in the field of robotics according to public reporting,[53] Including in 2020 when it halted an investment into a joint venture between Chinese entities and the robotic exoskeleton company Ekso Bionics Holdings, Inc.[54] [55] Ultimately, CFIUS required the termination of the joint venture to prevent technology transfer.[56]

41 Feiner, Lauren. (2021, June 16). *Alphabet's self-driving car company Waymo announces $2.5 billion investment round*. CNBC. Retrieved from https://www.cnbc.com/2021/06/16/alphabets-waymo-raises-2point5-billion-in-new-investment-round.html.

42 Metz, C., Dawson, B., & Felling, M. (2019, March 26). *Inside Google's rebooted Robotics Program*. The New York Times. Retrieved from https://www.nytimes.com/2019/03/26/technology/google-robotics-lab.html.

43 *National security implications of leadership in autonomous vehicles*. National Security Implications of Leadership in Autonomous Vehicles | Center for Strategic and International Studies. (2022, April 27). Retrieved from https://www.csis.org/analysis/national-security-implications-leadership-autonomous-vehicles.

44 *National security implications of leadership in autonomous vehicles*. National Security Implications of Leadership in Autonomous Vehicles | Center for Strategic and International Studies. (2022, April 27). Retrieved from https://www.csis.org/analysis/national-security-implications-leadership-autonomous-vehicles.

45 *National security implications of leadership in autonomous vehicles*. National Security Implications of Leadership in Autonomous Vehicles | Center for Strategic and International Studies. (2022, April 27). Retrieved from https://www.csis.org/analysis/national-security-implications-leadership-autonomous-vehicles.

46 Squire Patton Boggs (US) LLP, *The Trade Practitioner; CFIUS Investigation: Sina Corporation and TuSimple Holdings Inc.*, (2021, August 18). Retrieved from https://www.tradepractitioner.com/2021/08/cfius-sina-corporation-tusimple-holdings-inc/.

47 Adler, A. (February 22, 2022). US takes limited oversight of TuSimple as foreign investment probe ends. Freightwaves, Inc. Retrieved at https://www.freightwaves.com/news/us-takes-limited-oversight-of-tusimple-as-foreign-investment-probe-ends.

48 Alper, A., & Roumeliotis, G. (2019, July 6). *Exclusive-U.S. panel OKAYS Softbank's $2.25 BLN investment in GM-linked self-driving firm*. Reuters. Retrieved from https://www.reuters.com/article/cfius-softbank-gm-idUKL2N24700B.

49 *Id.*

50 https://www.theverge.com/2020/12/17/22179588/canoo-delivery-vehicle-nasdaq-spac-merger-listing-public.

51 *Id.*

52 Discussion of CFIUS mitigation of Canoo Transaction. *R/Canoo*. reddit. (n.d.). Retrieved from https://www.reddit.com/r/canoo/.

53 *See, e.g.*, SoftBank's acquisition of Boston Dynamics from Alphabet (https://www.ft.com/content/81f10306-b38c-11e7-a398-73d59db9e399).

54 https://www.globaltradelawblog.com/2020/05/29/biotech-ekso-case/.

55 https://www.globenewswire.com/news-release/2020/05/20/2036681/0/en/Ekso-Bionics-Announces-CFIUS-Determination-Regarding-China-Joint-Venture.html.

56 *Id.*

V. CFIUS: LEANING IN

As this essay sets forth, a number of arguments have been made for and against Big Tech. These examples of CFIUS transactions illustrate another consideration, one that implicates national security. CFIUS is designed to mitigate these risks, and FIRRMA gave it the authorities to face evolving threats — including jurisdiction over certain minority investments[57] and certain types of real estate transactions,[58] mandatory filings for certain types of technology-related investments, and substantial monetary penalties for failing to file or from circumventing CFIUS national security agreements.[59] FIRRMA also ensured the government has the resources — such as a dedicated funding stream for the first five years, the ability to rapidly hire new staff, and a filing fee regime to provide other funding support. But government bureaucracies do not have unlimited staff and resources.

The number of transactions submitted to the Committee steadily increased in the leadup to FIRRMA. In 2009, 65 notices were filed. By 2017 and 2018, the number of deals reviewed had swelled nearly four-fold to 237 and 249, respectively. Since FIRRMA's enactment, the Committee's caseload has reached all-time highs, with 324 total transactions reviewed in 2019 and 313 in 2020.

Definitive data on the annual number of mergers, acquisitions, and investments with any involvement of foreign capital is not easily discernible, but we know that foreign direct investment in the United States increased by $187.2 billion to a total stock of $4.63 trillion in 2020; and that there were over 17,000 venture deals in the United States in 2021, which does not include traditional private equity.[60] [61] From these numbers, we can reasonably conclude that CFIUS is only looking at a small fraction of the FDI transactions that are executed annually in the United States.[62]

This transaction magnitude, as well as limited transparency in parts of the investment ecosystem, versus the size and capacity of CFIUS, means that cases posing national security risk will inevitably slip through the cracks. There are also likely instances where a filing is mandatory because it involves critical technology but the parties nonetheless refrain from submitting it to CFIUS. Investments that aren't filed with the Committee, whether or not mandatory, but which pose national security risk are referred to as "non-notified" transactions. FIRRMA required that the Committee establish a process to identify this type of transaction and the risk that it might involve.[63]

Congress made clear in FIRRMA that appropriately resourcing the Committee so that it could face these challenges was an imperative, stating that CFIUS "plays a critical role in protecting the national security of the United States, and, therefore, it is essential that the member agencies of the Committee are adequately resourced and able to hire appropriately qualified individuals in a timely manner . . . ."[64] Divestment of businesses from a Big Tech company would necessitate even greater CFIUS vigilance and resources to identify and monitor subsequent acquisitions or investments. In fact, sufficient resourcing to find high-risk transactions will be essential for CFIUS to effectively execute its mission.

To ensure CFIUS implemented FIRRMA in the right way, Congress allocated the necessary funding in concert with the resourcing statement quoted above, authorizing funding of $20 million annually for five fiscal years (2019 to 2023).[65] The Treasury Department, which is the Chair of the Committee, received $40 million in its budget in 2020 and 2021 for CFIUS.[66] Part of Treasury's funding in 2019 and 2020 was

57 Section 1703 of H.R. 5515 of August 13, 2018.

58 *Id.*

59 Section 1706 of H.R. 5515 of August 13, 2018.

60 *Direct Investment by Country and Industry, 2020.* Direct Investment by Country and Industry, 2020 | U.S. Bureau of Economic Analysis (BEA). (n.d.). Retrieved from https://www.bea.gov/news/2021/direct-investment-country-and-industry-2020.

61 Ceppos, R. (2022, January 13). *U.S. venture capital activity soars to new highs in 2021 as deal value exceeds $300 billion and fundraising tops $100 billion.* NVCA. Retrieved from https://nvca.org/pressreleases/u-s-venture-capital-soars-to-new-highs-in-2021/#:~:text=The%20top%2Dline%20figures%20for,2020's%20previous%20deal%20value%20high.

62 It should also be noted that as the number of cases CFIUS must review outpaces the resources as its disposal, the time to review each deal will likely increase. This has financial implications for each deal and over time, if not resolved, could disincentivize benign capital investments in certain areas of U.S. industry that the U.S. desires.

63 Section 1710 of H.R. 5515 of August 13, 2018.

64 *Id.* at Section 1702.

65 *Id.* at Section 1723.

66 Dow Jones & Company. (2021, January 31). *Government 'SWAT team' is reviewing past startup deals tied to Chinese investors.* The Wall Street Journal. Retrieved from https://www.wsj.com/articles/government-swat-team-is-reviewing-past-startup-deals-tied-to-chinese-investors-11612094401.

dedicated to the development of a "new enforcement arm of roughly two dozen people tasked with rooting out old investment deals that involve sensitive technologies and could pose a threat to national security . . . The team has its sights on venture-capital investments, even small-dollar deals, where the money can be traced back to China . . . Recent hires to its enforcement team include professionals from venture-capital firms, investment banks and technology backgrounds, according to people involved in the effort."[67]

If regulators were to break up a Big Tech firm, the resulting new companies and their assets could provide prime targets for acquisition by foreign Big Tech or industry-leading foreign firms; and the U.S. technology and intellectual property — developed and cultivated through economies of scale and specialized human capital and know-how — could materially augment the foreign firms' technology and know-how, and might advantage a strategic competitor. In that event, CFIUS will need to be prepared.

VI. CONCLUSION

American antitrust laws designed to protect the consumer are not focused on national security considerations, nor should they be. Regulators and policymakers will decide whether and how to address Big Tech companies and their various impacts on the American consumer, including whether to break them up. But even as such decisions will not be made on national security grounds, it is vital that policymakers and regulators are aware of and understand the potential national security consequences so that the nation is prepared. A breakup of Big Tech could leave American intellectual property, data, technology, and know-how up for grabs. In this event, CFIUS and other national security authorities will need to be appropriately resourced and staffed, and be ready to step in.

For CFIUS to be prepared, Congress must remain committed to funding it and fully empowering its "non-notified" enforcement functions that allow CFIUS to seek out risky deals that may hide under the radar, and it should exercise continuing oversight of CFIUS's enforcement activities more generally.

67 *Id.*

CPI COMPETITION POLICY™ INTERNATIONAL

CPI Subscriptions

CPI reaches more than 35,000 readers in over 150 countries every day. Our online library houses over 23,000 papers, articles and interviews.

Visit competitionpolicyinternational.com today to see our available plans and join CPI's global community of antitrust experts.