ALGORITHMIC COMPETITION, TRADE AND INVESTMENT: THE CFIUS AS PRIVACY REGULATOR

Salil K. Mehra[†]

I. INTRODUCTION

For the past century, theories of regulation have been dominated by the interaction between politics and markets. From eras dominated by capitalism and socialism to ones featuring nationalism and globalism, economists, political scientists and politicians have focused on how to regulate markets to improve social welfare, and their ideas have animated vibrant public debates.[1] Until recent challenges from both the left and the right, the West has been dominated by a globalist liberalism with a presumption in favor of market ordering, plus limited political intervention where necessary—a major expression of this philosophy has been the adoption of policies favoring freedom of international trade and investment.[2]

Algorithmic connectivity and competition has changed the *terms of trade* between politics and markets in a way that upsets current balances between regulation and markets.[3] While algorithms have long existed, concurrent technological advances in data

---

[†] Charles Klein Professor of Law and Government, Temple University, Beasley School of Law, Philadelphia, USA; smehra@temple.edu.

[1] *See generally* FRANCIS FUKUYAMA, THE END OF HISTORY AND THE LAST OF MAN (1992) (arguing that the world had reached a historical moment in which these stark 20th century ideological conflicts were now over and that liberal democracy, market capitalism and globalism had won).

[2] *Cf.* Chantal Thomas, *Law and Neoclassical Economic Development in Theory and Practice: Toward an Institutionalist Critique of Institutionalism*, 96 Cornell L. Rev. 967, 969–70 (2011) (noting the ascendancy of the "Washington Consensus," described as "a blueprint for the implementation of the neoclassical economic policies of the Chicago School: liberalization of trade, privatization of investment, fiscal austerity, and monetary stabilization.").

[3] *See* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 2–4 (2015) (describing, for example, the ways in which algorithms and "Big Data" have made consumers' lives increasingly transparent for big business, financial institutions, and government agencies, but in contrast have made the workings of such organizations more opaque to consumers, shifting the power balance among them).

collection, interconnectivity, and computer processing have generated a new, powerful ability to connect individuals, groups, and firms.[4] These interrelated phenomena have given rise to new forms of algorithmic connectivity and competition that challenge and even supplant the role of traditional markets in matching counterparties.[5] A few notable firms, such as Google, Amazon, and Facebook, have grown powerful by exploiting these developments to become superconnecting platforms.[6] While the economic effects of matching buyers and sellers are already tremendous, superconnectors are also powerfully reshaping how civil society interacts in other areas.[7] In addition to matching buyers and sellers, platforms also match authors with readers and, increasingly, partisans with like-minded comrades.[8] Still other firms, such as Uber, Airbnb, and Match.com, use algorithmic connectivity to link travelers, co-habitants, and seekers of companionship.[9] Part of the power of algorithmic connectivity is reducing the time and transaction costs of traditional markets, while simultaneously increasing the search dimensions beyond price, quantity, and relatively coarse determinants of quality that limit traditional market exchange.[10]

---

[4] *See* DAVID S. EVANS & RICHARD SCHMALENSEE, MATCHMAKERS: THE NEW ECONOMICS OF MULTISIDED PLATFORMS 19–20 (2016) (emphasizing that technological change has "turbocharged" platforms that "connect potential trading partners residing almost anywhere in the world.").

[5] *Id.* at 105 (describing how Uber's algorithm sets its drivers' fares, rather than letting drivers negotiate with passengers, the latter being a form of market-based pricing used for taxi and similar rides in many countries).

[6] *Id.* at 109–18 (explaining these firms' commitment to an "ecosystem" business model designed to take advantage of network effects by robustly engaging multiple sides of the platform).

[7] *See* CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY 179–97 (2016) (describing, prior to the 2016 U.S. presidential election, how Facebook and others firms' behavioral targeting could be used to influence voters).

[8] *See* Elizabeth Dwoskin & Rachel Lerman, *'Stop the Steal' Supporters, Restrained by Facebook, Turn to Parler to Peddle False Election Claims,* WASHINGTON POST (Nov. 13, 2020), https://www.washingtonpost.com/technology/2020/11/10/facebook-parler-election-claims/ [https://perma.cc/NZ5A-5G6F] (describing movements of conservative political adherents to the Parler social media platform).

[9] *See* EVANS & SCHMALENSEE, *supra* note 4, at 143–48 (explaining use of reputational scoring by platforms to match participants).

[10] *See* Ryan Calo, *Privacy and Markets: A Love Story,* 91 NOTRE DAME L. REV. 649, 650 (2016) (arguing that pre-Internet privacy norms promoted marketing

But at the same time, the development of algorithmic connectivity changes the relationship between international investment, domestic governance, and individual privacy. [11] Transactions in consumer data are key to consumer targeting and tailoring, which in turn are critical to algorithmic connectivity.[12] This tension is increasingly expressed in the scrutiny paid to cross-border M&A investment involving algorithmic connectivity and consumer data transactions, particularly that of the CFIUS ("Committee on Foreign Investment in the United States"). Recently, United States national security reviews forced divestiture by Chinese acquirers of Grindr (an online service for LGBTQ community members) and health data startup PatientsLikeMe, and also blocked a Chinese firm's acquisition of the MoneyGram payment service.[13] This short Article, prepared in connection with a symposium focusing in part on mergers and acquisition policy, argues that the recent burst of CFIUS action arises from the inherent limits of consumer sovereignty and contractarian approaches in dealing with consumer data privacy—especially across the borders of nations with very different approaches to using the acquired data.

II. CHINA, AND THE CFIUS, WAKES

The CFIUS: An Origin Story

Despite its recent emergence as a focus of mergers and acquisitions lawyers involved in United States-China investment, the CFIUS is not a recent invention. Established in 1975 via an executive

---

functioning by hiding "salient but distorting information such as personal or political commitments" that are increasingly being used to "cancel" economic actors).

[11] *See* PASQUALE, *supra* note 3, at 189–94 (arguing for steps to regulate the interaction between these interests).

[12] *See* O'NEILL, *supra* note 7, at 173 (warning that "oceans of behavioral data, in coming years, will feed straight into artificial intelligence systems," which will target individual consumers, "[a]nd these will remain, to human eyes, black boxes").

[13] Nevena Simidjiyska, *CFIUS Flexes New Muscles Where Consumer Data and Critical Technology are Involved*, CORPORATE COMPLIANCE INSIGHTS (Apr. 24, 2019), https://www.corporatecomplianceinsights.com/cfius-flexes-new-muscles-where-customer-data-and-critical-technology-are-involved/ [https://perma.cc/3PJQ-FJ7K].

order by President Gerald Ford, the CFIUS is a committee with representation from multiple executive branch departments, chaired by the Secretary of the Treasury and tasked with reviewing certain transactions involving foreign investment in the United States to determine their national security implications.[14]

That said, the CFIUS did not always have the power and the relevance that it has today. In fact, its history shows a certain level of ad hoc amendment that has characterized its development. In response to concerns about the Japanese firm Fujitsu's proposed acquisition of Fairchild Semiconductor, the 1988 Exon-Florio Amendment gave the president the power to review and block foreign investments that might harm national security; President Reagan then delegated the review process to the CFIUS.[15] Subsequently, in 2007, concern over the potential management of six major United States seaports by a U.A.E.-based firm led Congress to formalize and strengthen the CFIUS review process.[16]

Recent CFIUS actions regarding Chinese firm investment in the United States have triggered fears of a "new Cold War," at least in the economic sphere.[17] Similar to the Japanese and U.A.E. investment inspired actions, the past decade has seen significant

---

[14] *See generally* Exec. Order No. 11858, 3 C.F.R. (1975).

[15] *See* Omnibus Trade and Competitiveness Act of 1988 (Exon-Florio Amendment), Pub. L. No. 100–418, 102 Stat. 1107, 1425–26 (amended 2006, 2018) (giving the president the power to block foreign investments when "there is credible evidence that leads the President to believe that the foreign interest exercising control might take action that threatens to impair the national security").

[16] *See* Foreign Investment and National Security Act of 2007, Pub. L. No. 110–49, 121 Stat. 246 (formalizing the CFIUS's membership, establishing a 45-day pre-transaction review period, requiring a report to Congress and authorizing the CFIUS to require mitigation steps, such as agreed pre-transaction divestitures).

[17] *See* Jack Nicas, Mike Isaac & Ana Swanson, *TikTok Said to Be Under National Security Review*, N.Y. TIMES (Nov. 1, 2019), https://www.nytimes.com/2019/11/01/technology/tiktok-national-security-review.html [https://perma.cc/3BNQ-SNP4] (describing the CFIUS review of TikTok's parent firm's U.S. investment and describing it as "what some analysts refer to as a new Cold War"); *see also* Dan Primack, *"New Cold War" Fears Hit Silicon Valley*, AXIOS (May 24, 2019), https://www.axios.com/us-china-trade-new-cold-war-9ab805a4-bd8e-4d99-9b91-0e3495a945ba.html [https://perma.cc/JSY8-E44N] (describing the perception among some tech firms that "Chinese companies are no longer viewed as viable acquirers due to concerns that the deals could be blocked by CFIUS").

changes to the CFIUS and its application that have been driven by concern about rising Chinese investment in the United States. In particular, inbound investment into the United States from Chinese sources rose from less than $5 billion annually on the eve of the Global Financial Crisis to over seven times as much one decade later; the number of deals has increased similarly.[18] The Treasury Department issues annual reports concerning the CFIUS's activity, and the public version of the most recent report details a significant rise in overall CFIUS action (see Figure 1).

Figure 1.[19]

Year	Number of Notices	Number of Investigations	Notices Withdrawn and Transactions Abandoned in Light of CFIUS-Related National Security Concerns
2014	147	51	2
2015	143	66	3
2016	172	79	3
2017	237	172	24
2018	229	159	17

While the absolute numbers of transactions blocked are small, the percentage change in a few short years is dramatic. Moreover, these numbers may understate the CFIUS's actual impact. Notably, deal participants report changing their behavior due to the perception of an increasingly active CFIUS; that is, the numbers of transactions abandoned may be rising despite increasing caution regarding the

[18] *See* Monan Zhang, *Investment Protectionism in the Name of National Security*, CHINA-US FOCUS (Sept. 6, 2017), https://www.chinausfocus.com/finance-economy/investment-protectionism-in-the-name-of-national-security [https://perma.cc/TW2U-9E7G] (citing Thomson Reuters data detailing the acceleration of China's purchase of United States companies over ten years).
[19] U.S. Dep't of Treasury, CFIUS Annual Report to Congress, ¶ Table I-1 Covered Transactions, Withdrawals, and Presidential Decisions, 2010–2018, https://home.treasury.gov/system/files/206/CFIUS-Summary-Data-2014-2018.pdf [https://perma.cc/S7PF-RQAF].

investments that make up the underlying deal mix that is being reviewed.[20]

The perception that recently stiffened CFIUS review policies have disproportionately affected Chinese firms and investors has some factual support—early in the Trump Administration, a number of high-profile proposed acquisitions of United States firms by Chinese buyers were blocked.[21] In particular, several of these transactions were high-profile investments that attracted significant attention in the business press. Among these blocked transactions were potential acquisitions of the Grindr LGBTQ community app, the MoneyGram money transfer service, and the health data startup PatientsLikeMe.[22] The targets of each of these investments were U.S. firms with substantial access to sensitive consumer data.[23] But because the objects of these investments did not fit a traditional notion of national security-related infrastructure, such as ports,

---

[20] *See* Primack, *supra* note 17 (reporting the considerable impact that CFIUS activity has had on the deals between Silicon Valley investors and firms).

[21] *See China's Ant Financial is Obliged to Abandon an American Acquisition*, ECONOMIST (Jan. 6, 2018), https://www-economist-com.proxy.library.upenn.edu/business/2018/01/06/chinas-ant-financial-is-obliged-to-abandon-an-american-acquisition [https://perma.cc/HA83-U83L] (providing an overview of several prominent Chinese attempted purchases of U.S. businesses that were stopped by the Trump Administration).

[22] *See* Harry L. Clark et al., *Grindr And PatientsLikeMe Outcomes Show Non-Cleared Transactions' Exposure to CFIUS Scrutiny, Especially When PII Is Involved*, MONDAQ (May 8, 2019), https://www.mondaq.com/unitedstates/inward-foreign-investment/804096/grindr-and-patientslikeme-outcomes-show-non-cleared-transactions39-exposure-to-cfius-scrutiny-especially-when-pii-is-involved [https://perma.cc/QKZ3-NL8D] (suggesting that U.S. blocking of Chinese investments in Grindr, MoneyGram and PatientsLikeMe can be explained by the desire to protect Americans' privacy interest in their personally identifiable information).

[23] *See* Simidjiyska, *supra* note 13 (stating that "[t]he Grindr and PatientsLikeMe decisions strongly suggest that the [CFIUS] overseers are very concerned about Chinese investment, particularly where sensitive personal data is involved" even though these potential transactions predated the FIRRMA of 2018's effective date); Louise Lucas, Don Weinland & Shawn Donnan, *Data Take Centre Stage as Ant Financial Fails in MoneyGram Bid,* FIN. TIMES (Jan. 3, 2018), https://www.ft.com/content/fd22dd9c-f06d-11e7-b220-857e26d1aca4 [https://perma.cc/G88G-VGZB] (quoting an anonymous banker "with knowledge of the MoneyGram deal say[ing] its demise was a 'strong precedent for anything involving personal data,' extending national security concerns to a much broader number of sectors").

aviation or defense-related electronics, their rejection by the CFIUS was seen as unprecedented to observers.[24] In retrospect, CFIUS opposition to these Chinese investments reveals a shifting understanding of what constitutes national security.

A CFIUS Reboot

Reflecting a changing conception of national security concerns, Congress recently passed legislation aimed at bringing the CFIUS's process and substance up to date; that legislation was notably passed during the uptick in serious review of China-related transactions.[25] The Foreign Investment Risk Review Modernization Act of 2018 ("FIRRMA") changed CFIUS review in several ways, formalizing the process, clarifying certain safe harbor countries and defining industries and types of transactions that are likely to attract strong concern.[26]

Procedurally, the FIRRMA transforms the CFIUS process into a formal notification regime, similar in some ways to the Hart-Scott-Rodino process for antitrust clearance.[27] Previously, the CFIUS had a voluntary filing regime whereby a foreign investor could *choose* whether to notify the CFIUS of its transaction before closing.[28] That said, prior to the FIRRMA, the CFIUS could review a transaction even in the absence of notification.[29] The FIRRMA makes formal notification mandatory; a foreign investor must submit

---

[24] *See* Morrison & Foerster, *CFIUS Means Business, Uniwinding Non-Notified Transactions and Penalizing Non-Compliance with Mitigation Agreements,* JD SUPRA (Apr. 16, 2019), https://www.jdsupra.com/legalnews/cfius-means-business-unwinding-non-86555/ [https://perma.cc/Z8WH-W7JN] (listing the Grindr and PatientsLikeMe acquisitions, in particular, among several unprecedented CFIUS developments).

[25] *See e.g.*, Foreign Investment Risk Review Modernization Act of 2018, Pub. L. No. 115–232, §1701–93, 132 Stat. 1636, 2174 (2018) [hereinafter *FIRRMA*] (aiming to change CFIUS processes to reflect the modern economic environment).

[26] *Id.*

[27] The Hart-Scott-Rodino Act is codified in 15 U.S.C. § 18a(a) (2016). Like the FIRRMA, it sets forth a positive duty for investors to notify the government of a covered transaction, as well as a time schedule for the review process.

[28] F.T.C. & U.S. DEP'T OF JUST., ANNUAL REPORT TO CONGRESS FISCAL YEAR 2004 (2004).

[29] *See* Morrison & Foerster, *supra* note 24 (pointing out that the CFIUS had "unwind[ed] non-notified transactions").

a declaration to the CFIUS at least 45 days before closing on any transaction in which the foreign investor would acquire control of a company that develops "critical technologies"—or by which the foreign investor could gain "material non-public access" to those technologies." [30] Significantly, it also authorizes the Treasury Department to create and maintain lists of "excepted investors" from specific "excepted foreign states," such as United States treaty allies, that would potentially be exempt from the CFIUS process.[31]

The FIRRMA's changes to the substantive scope of CFIUS review will likely create increased tension with Chinese investors—though the source of that tension lies not simply in anti-China sentiment, but in the changing nature of what is considered *sensitive* in terms of national security. The key FIRRMA changes involve both the degree of control triggering concern, as well as the specific industries and technologies at issue. First, before FIRRMA, the CFIUS could only block transactions that would result in foreign *control* of a United States business.[32] Under the prior understanding, "control" in practice meant the ability to sell the company, enter or

---

[30] *Id*.

[31] Notably, the Department of the Treasury has issued somewhat contradictory language regarding the strength of any potential safe harbor. *See* U.S. DEP'T OF TREASURY, FREQUENTLY ASKED QUESTIONS ON FINAL CFIUS REGULATIONS IMPLEMENTING FIRRMA (Jan. 13, 2020), https://home.treasury.gov/system/files/206/Final-FIRRMA-Regulations-FAQs.pdf [https://perma.cc/6AGH-YVHY] (noting that while identifying Australia, Canada, and the United Kingdom as the "initial excepted foreign states," Treasury has also stated that "[n]ot necessarily" "will every foreign person based in an 'excepted foreign state' . . . qualify as an 'excepted investor,'" and even if so qualified, the "CFIUS retains the authority to review a transaction that could result in foreign control of any U.S. business, regardless of whether the foreign person is an 'excepted investor'"); *see also supra* note 28, at 5 (providing CFIUS with review authority over transactions).

[32] *See* U.S. DEP'T OF TREASURY, *supra* note 31, at 2 (stating that FIRRMA updated and strengthened CFIUS processes). *See also* Joseph V. Moreno et al., *CFIUS Unbound: Foreign Investor Deals Continue to Draw Intense National Security Scrutiny*, NAT'L L. REV. (Aug. 1, 2019), https://www.natlawreview.com/article/cfius-unbound-foreign-investor-deals-continue-to-draw-intense-national-security [https://perma.cc/8HPU-4PPT] (noting that "Prior to FIRRMA, a "covered transaction" subject to CFIUS review was limited to mergers, acquisitions, or takeovers by or with a foreign person that could result in foreign "control" of any person engaged in interstate commerce in the United States, and that could threaten the national security of the United States").

leave contracts, close production facilities, and the like.[33] The FIRRMA expands that jurisdiction to permit review of transactions which give a foreign investor even just a noncontrolling stake in certain industries, recognizing that even sub-majority ownership can confer access and influence.[34]

Additionally, the FIRRMA broadens the range of industries that attract review. CFIUS review expands to cover foreign investment in U.S. companies involved with critical technologies and, crucially, the sensitive personal data of U.S. citizens. The FIRRMA also includes a new focus on "material nonpublic technical information."[35] Moreover, the FIRRMA authorizes the Department of the Treasury to identify *pilot* industries of particular concern. Alongside traditional national security-related concerns such as aerospace and oceangoing vessel production, the initial named industries included computers, semiconductors, wireless communications, and electronic storage.[36]

The FIRRMA and its implementing regulations, by standardizing the CFIUS process, create increased certainty for foreign investors and their US counterparties regarding the CFIUS process. However, that increased certainty will not necessarily diffuse trade tensions, particularly with China. In particular, the focus industries that the Department of the Treasury has identified pursuant to its FIRRMA authority include a number of areas that are also priority industries under the "Made in China 2025" industrial policy pursued by China's central government; these areas include such key industries as electrical equipment, materials science, biopharmaceuticals, and most importantly for this Article,

---

[33] *Id.*
[34] *Id.*
[35] *Id. See also* Jeffrey Richardson, *CFIUS Review Authority Expands*, JD SUPRA (Feb. 12, 2020), https://www.jdsupra.com/legalnews/cfius-review-authority-expands-62714/ [https://perma.cc/5LUX-PRJP].
[36] *See Treasury Releases Interim Regulations for FIRRMA Pilot Program,* U.S. DEP'T OF TREASURY (Oct. 10, 2018), https://home.treasury.gov/news/press-releases/sm506 [https://perma.cc/Y9V4-9ML5] (introducing the new regulations' scope, purpose, and basic contents); *see also CFIUS Laws and Guidance*, U.S. DEP'T. OF TREASURY (Feb. 13, 2020), https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-legislation [https://perma.cc/K7DF-TETW] (releasing final CFIUS regulations).

information and communications technology.[37] However, any attempt to deal with this tension runs into an ambiguity that serves as a kind of roadblock: the United States' own current lack of concrete policies outlining its citizens' fundamental interests regarding information technology, including data privacy.

III. CURRENT U.S. LAW: DATA PRIVACY LIKE NO ONE'S WATCHING

What is generating the CFIUS' tension with Chinese investment in U.S. information technology is a two-part question that goes beyond foreign investment: to what extent does United States citizens' data privacy matter, and what legal steps should be taken to address that concern? Both parts of that question are the subject of intense current discussion, and both parts are critical to why the CFIUS has become increasingly active.

Data Privacy—What, Why and How Much?

Whether U.S. citizens should enjoy data privacy, and if so, how much, is a leading question of the early twenty-first century. Much as the development of portable, snapshot-capable film cameras catalyzed Samuel Warren and Louis Brandeis' 1890 landmark article *The Right to Privacy*,[38] the increasing ability of firms and

[37] *See generally China to Invest Big in "Made in China 2025 Strategy*," XINHUA NEWS AGENCY (Oct. 12, 2012), http://english.www.gov.cn/state_council/ministries/2017/10/12/content_281475904600274.htm [https://perma.cc/LS7R-SVLQ] (introducing China's "Made in China 2025 Strategy"); *see also* Martijn Rasser, *The United States Needs a Strategy for Artificial Intelligence*, FOREIGN POL'Y (Dec. 24, 2019), https://foreignpolicy.com/2019/12/24/national-artificial-intelligence-strategy-united-states-fall-behind-china/ [https://perma.cc/X7AS-KRVY] (contrasting relatively laissez-faire United States policy concerning its "technological edge" with the "Made in China 2025 initiative—a wide-ranking industrial policy intended to vault China into the select club of global technology powers"); James McBride & Andrew Chatzky, *Is 'Made in China 2025' a Threat to Global Trade?,* COUNCIL ON FOREIGN REL. (May 13, 2019) https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade [https://perma.cc/9BHR-7DBC] (listing 12 targeted sectors thought to be critical and technologically advanced).

[38] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

governments to capture, store and process all manner of individuals' information has driven a movement to bolster data privacy. Much as with better cameras, better and more portable computing power has driven shifts in how people live that has come with both benefits, such as increased productivity and convenience, as well as costs in terms of personal privacy.

That said, whether data privacy should be protected is still not a matter of consensus. As the COVID-19 crisis has revealed, some doubt that privacy needs protecting.[39] However, well before the pandemic, Facebook founder Mark Zuckerberg argued that privacy was no longer a "social norm," and so did not need protecting.[40] Similarly, about a decade ago, Google Chief Executive Eric Schmidt had gone on record to question the need for data privacy, stating that "if you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place."[41]

While the antagonistic view of major tech titans may have slowed the growth of interest in citizens' data privacy in the United States, it did not stop it. Survey data comparing citizens' concerns at the start of the twenty-first century and again in 2010 showed that individuals had become increasingly concerned with companies tracking their behavior online and then making the acquired data an object of commerce.[42] Technological change has forced regulators such as the FTC to become involved in protecting citizens'

---

[39] *See* Roy Cellan-Jones, *Coronavirus: Privacy in a Pandemic*, BBC (Apr. 4, 2020), https://www.bbc.com/news/technology-52135916 [https://perma.cc/ZCR2-FQ6X] (quoting a Tweet concerning privacy concerns regarding COVID-19 tracking via smartphone, the former Portuguese Minister for Europe stating: "I am more and more convinced the greatest battle of our time is against the 'religion of privacy.' It literally could get us all killed."); @MacaesBruno, TWITTER (Mar. 31, 2020, 9:12 PM), https://twitter.com/MacaesBruno/status/1245157022816968704.

[40] Bobbie Johnson, *Privacy No Longer a Social Norm, Says Facebook Founder*, GUARDIAN (Jan. 10, 2020), https://www.theguardian.com/technology/2010/jan/11/facebook-privacy [https://perma.cc/4PEY-QR4B].

[41] Helen A.S. Popkin, *Privacy is Dead on Facebook. Get Over It*, NBC NEWS (Jan. 13, 2010), http://www.nbcnews.com/id/34825225/ns/technology_and_science-tech_and_gadgets/t/privacy-dead-facebook-get-over-it/#.XoeJW257mF0 [https://perma.cc/VBB2-UKNP].

[42] *See* Annie I. Anton et al*., How Internet Users Privacy Concerns Have Evolved Since 2002*, 8 IEEE SEC & PRIV. MAG., 21 (2010) (reporting changes over time in systematic survey responses regarding consumer concerns).

longstanding interest in their privacy, and lawyers, academic commentators and policymakers have become increasingly active, at least in specific sectors such as health and financial information privacy.[43]

Despite citizens' interest in their privacy in a technologically shifting world, the United States continues to lack any general national privacy legislation – in contrast to the European Union's General Data Protection Regulation (GDPR).[44] Does this mean that Americans value their privacy less than Europeans? Not necessarily, of course; the reality is that comparative difficulties in working through the political process could also explain the lack of a United States analogue to the GDPR.[45] Whatever the reason, the lack of general data privacy law in the U.S. leaves the protection of consumer information online largely to private ordering.

Foreign Investment in Data and the CFIUS as Placeholder

Without general privacy regulation, United States consumers' online data is largely governed by private contracting, supplemented with reputational enforcement.[46] Doubts have arisen concerning the

---

[43] *See* DANIEL J. SOLOVE, *A Brief History of Information Privacy Law*, *reprinted in* PROSKAUER ON PRIVACY: A GUIDE TO PRIVACY AND DATA SECURITY LAW IN THE INFORMATION AGE 37–53 (Kristen J. Mathews, Proskauer Rose LLP eds., 2d ed. 2016) (outlining history of information privacy, including new targeted sectoral regulation such as the Health Insurance Portability and Accountability Act (HIPAA) and the Fair and Accurate Credit Transactions Act of 2003 (FACTA) enacted after the growth of the consumer-facing Internet).

[44] *See generally* DIRK AUER & GEOFFREY A. MANNE, IS EUROPEAN COMPETITION LAW PROTECTIONIST? (Int'l Ctr. for L. & Econ. eds., 2019), https://laweconcenter.org/wp-content/uploads/2019/04/Is-European-Competition-Law-Protectionist-Issue-Brief.pdf [https://perma.cc/W9U6-NRS7] (pointing out this divergence in privacy policy, while noting that California did enact a state-level general privacy law in 2018).

[45] *See* Müge Fazlioglu, *Tracking the Politics of US Privacy Legislation*, IAPP (Dec. 13, 2019), https://iapp.org/news/a/tracking-the-politics-of-federal-us-privacy-legislation/ [https://perma.cc/4ME8-XK23] (suggesting that the U.S.' inability to adopt national privacy protection as the EU has with the GDPR reflects not only a lack of interest in protecting privacy, but further exposes the drawbacks of the U.S. political process and its veto points, including in Congress).

[46] *See* Thomas B. Norton, *The Non-Contractual Nature of Privacy Policies and a New Critique of the Notice and Choice Privacy Protection Model*, 27 FORDHAM

viability of a consumer sovereignty-based market solution to privacy issues—it has become increasingly questionable whether consumers can truly contract for their online privacy given asymmetries of information and market power.[47]

Moreover, the contractarian rationale has failed in actual application to protect consumers over the course of these transactions. Specifically, while first-generation privacy scholarship predicted that contract law would play a role in enforcing breaches of privacy policies, courts have often concluded that privacy policies are "general statements of policy rather than enforceable contracts."[48] Additionally, network effects may prevent consumer choice from being a shield against privacy harms.[49] In concrete terms, when one has only weak competitive alternatives due to the choices of others (e.g., join Facebook versus an alternative social networking service that lacks one's friends and family), one's choices will not necessarily resemble the Economics 101 product of voluntary actions in an efficient market. Finally, behavioral economics has revealed some weaknesses in the consumer-sovereignty/contractarian approach to transactions in consumer data.[50] For example, studies of bounded attention demonstrate that if users are distracted for even a couple of seconds after being given a privacy policy, they significantly lower their risk perceptions and become more amenable to consent; moreover, consistent with other findings from behavioral law and economics, consumers cannot easily value long-term risks associated with the disclosure of personal information.[51]

This United States' privacy regulation gap has drawn concern from commentators and policymakers. Some worry about the increasing power of data-rich monopolistic platforms to implement a

---

INTELL. PROP. MEDIA & ENT. L. J. 181, 187 (2016) (explaining why, without legal requirement, "nearly all companies [in the United States] have a privacy policy").

[47] *See* John Mark Newman, *Antitrust in Zero-Price Markets: Foundations,* 164 U. PA. L. REV. 149 (2015) (describing these arguments and critiquing them).

[48] Norton, *supra* note 46, at 190.

[49] *See id.* at 202–203 (concluding that the trend in case law renders privacy policy breaches effectively "categorically immune" from consumers' privately brought breach of contract claims).

[50] *See* Yoan Hermstrüwer, *Contracting Around Privacy: The (Behavioral) Law and Economics of Consent and Big Data*, 8 J. INTELL. PROP., INFO. TECH. & ELECTRONIC COM. L. 9, 16 (2017) (stating that consumers, even when partially protected, may create market inefficiencies that erode their privacy rights).

[51] *Id.* at 18–22.

"market-driven coup from above" via "surveillance capitalism."[52] Others question whether the United States' approach positions the nation well in a global race to develop critical artificial intelligence capabilities.[53] Finally, more practical concerns about cybersecurity and the vulnerability of networked infrastructure—as highlighted by the 2017 NotPetya attacks—have raised alarm concerning unprotected data.[54]

The lack of general legal protections for data privacy goes beyond foreign investment transactions. However, the recent draft implementing regulations of the FIRRMA specifically make transactions giving access to U.S. citizens' "sensitive personal data" a focus of CFIUS review.[55] Viewed through the lens of the general ambiguity concerning the current use of personal data, CFIUS review can be seen as a placeholder or *pause button*. Lacking a consensus about how to regulate and protect data privacy, the CFIUS is arguably trying to minimize the data privacy harm to avoid having to *unscramble the eggs* later. Because current privacy protections are based on difficult-to-enforce consumer contracts, acquisition of United States consumer data by Chinese firms, and especially Chinese government-related or -controlled firms, potentially involves harms that are not addressable via the current underdetermined approach.[56] The CFIUS' activity concerning data privacy responds to general legal and policy inaction.

---

[52] SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 513 (2019).

[53] *See, e.g.,* KAI-FU LEE, AI SUPERPOWERS: CHINA, SILICON VALLEY, AND THE NEW WORLD ORDER 102 (2018) (arguing that "China's techno-utilitarian approach gives it a certain advantage" and that the US needs a similar public-private synergy concerning data and AI in order to compete in the development of AI technologies).

[54] *See generally* ANDY GREENBERG, SANDWORM: A NEW ERA OF CYBERWAR AND THE HUNT FOR THE KREMLIN'S MOST DANGEROUS HACKERS (2019) (describing the rise of international cybersecurity concerns in light of a series of critical attacks).

[55] *See* U.S. DEP'T OF TREASURY, *supra* note 31, at 5 (describing 2020 final Treasury Department regulations implementing FIRRMA).

[56] Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN REL. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection [https://perma.cc/55E3-FS2Q] (explaining how the "United States lacks a single, comprehensive federal law that regulates the collection and use of personal information" and that what patchwork provisions exist are of uncertain power).

IV. CONCLUSION: BEYOND DATA PRIVACY TO INFORMATION AND NARRATIVE CONTROL

While data privacy is part of the national security dilemma, it may be more a start than an endpoint. Concerns about the foreign control of new information and communications technology may go beyond issues of blackmail, as may have been the case with the CFIUS' intervention in the acquisitions of Grindr and MoneyGram. As a result, the CFIUS may face pressure to act vis-à-vis new gaps in dealing with consumers and information platforms.

For example, at the start of 2020, a transaction under CFIUS scrutiny exemplified this shift: the Chinese firm ByteDance's acquisition of the United States-based social media app Musical.ly, which brought with it the basis for the wildly popular TikTok video sharing platform.[57] The concern with TikTok, particularly popular with users 16 to 24, may not simply be that it has access to their sensitive private information; it may also be the possibility that the platform could be used to spread disinformation or manipulate voters.[58] In August 2020, President Trump issued an executive order that would prohibit U.S. individuals and firms from engaging in any transactions with TikTok.[59] While the order cited TikTok's capturing "Americans' personal and proprietary information,"[60] voices in the media have observed that Trump's public concern with TikTok appeared to follow its use by a social media campaign that tampered with attendance at one of his pre-election rallies.[61]

---

[57] *See* David R. Hanke, *TikTok National Security Problem: Don't Ignore the Lessons of 2016*, HILL (Jan. 28, 2020), https://thehill.com/opinion/cybersecurity/480251-the-tiktok-national-security-problem-dont-ignore-the-lessons-of-2016 [https://perma.cc/HJH8-WFTZ] (comparing potential of ByteDance, which also manages a Chinese state-owned joint venture, to use TikTok to influence young voters to the alleged use by Russian intelligence of Twitter and Facebook to affect the 2016 US national election).

[58] *Id.*

[59] Exec. Order No. 13873 (Aug. 6, 2020), https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/ [https://perma.cc/4W3Y-U8R4].

[60] *Id.*

[61] *Id*. *See also* Dave Lee, *TikTok to Sue Trump Administration over Ban*, FIN. TIMES (Aug. 22, 2020), https://www.ft.com/content/78da8b5a-7a83-4692-afbb-628e29025511 [https://perma.cc/E88M-K98E] (noting that "in June [2020], a

Given concerns about the manipulation of the 2016 United States national election, the review of the TikTok-related investment may be warranted.[62] But this represents a different concern than consumer data privacy—instead, the worry is about the manipulation of information and the control of political narratives. The intersection of so-called *fake news* and the political process is a problem that goes beyond an interagency committee like the CFIUS and arguably involves questions about epistemology and the nature of democratic governance. The CFIUS alone cannot answer such questions; but it surely can be pressed into action while the United States government, media, and civil society engage with this question and other yet-unknown data- and information-related questions that will arise. Is this, as it has been accused of being, protectionism? Not in the way we have previously understood that word, as in the service of national mercantile gain. Instead, it is, at least in part, an attempt to shield noneconomic values such as privacy, liberty and even less obvious ones that are difficult to define and measure, but vital nonetheless. "You don't know what you've got 'til it's gone.'"[63]

campaign that spread on TikTok was credited with inflating the expected turn out of a Trump re-election rally in Tulsa, Oklahoma").

[62] *See generally* LEE, *supra* note 53 (stating that Tik-Tok could potentially be used for espionage).

[63] Joni Mitchell, *Big Yellow Taxi* (1970), https://jonimitchell.com/music/song.cfm?id=13 [https://perma.cc/BZ3P-KXSW].