Washington Journal of Law, Technology & Arts

Volume 18 | Issue 3 Article 2

4-24-2023

PARADIGMS FOR FOREIGN TECH-PLATFORMS REGULATION: U.S. OPTIONS AFTER THE TIKTOK SAGA

Zhining Zhang
KoGuan School of Law, Shanghai Jiao Tong University

PARADIGMS FOR FOREIGN TECH-PLATFORMS REGULATION: U.S. OPTIONS AFTER THE TIKTOK SAGA

Cover Page Footnote

L.L.B. Student, KoGuan School of Law, Shanghai Jiao Tong University. With thanks to L. Ben for inspiration, and to the Editors of the Washington Journal of Law, Technology & Arts for their assistance.

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 18, ISSUE 3 — SPRING 2023

PARADIGMS FOR FOREIGN TECH-PLATFORMS REGULATION: U.S. OPTIONS AFTER THE TIKTOK SAGA

Zhining Zhang[1]

ABSTRACT

The heated discussion stirred up by the U.S. regulatory actions against TikTok continues to this day. The nearly predatory popularity of this Chinese application has raised people's awareness that the country is in urgent need of a fully developed policy in order to deal with the surge of robust foreign digital platforms.

This article gives the contour of the latest development of theories regarding the foreign tech-platforms regulation. Three contemporary frameworks are reviewed. The first laissez faire paradigm inherits the values of early neoliberalism to prevent a "Splinternet," but its inaction fails to deal with novel security threats ranging from data privacy to economic competitiveness nowadays. The second case-by-case restrictions paradigm is presently the most mainstream and frequently-discussed scheme. It recognizes the blurriness of the existing non-systemic actions and has been flourished with risk assessment methods proposed by scholars. However, the inconsistency, unpredictability and the complexity of rules constitute its inborn deficiency. The last platform-utilities paradigm is a newly-developed innovative approach, which identifies the similarity between the tech-platforms and traditional utilities platforms of political-economy features, and thus provides legitimacy and viability of the sectoral regulation. Nonetheless, the differences between the internet platforms and the traditional utilities platforms, the shift from the U.S. long standing open attitude, and the risk of second order effects, all require further reflection.

All of the proposals are an inspiration for policymakers to rethink the tension between internet freedom and national security. The article concludes by briefly reviewing the TikTok saga chronologically and analyzing the latest regulation attempt of Executive Orders of different States.

[1] L.L.B. Student, KoGuan School of Law, Shanghai Jiao Tong University. With thanks to L. Ben for inspiration, and to the Editors of the *Washington Journal of Law, Technology & Arts* for their assistance.

TABLE OF CONTENTS

INTRODUCTION

From late 2017 to early 2021, a series of regulatory actions toward the popular Chinese-owned application TikTok by the Trump Administration has sparked a heated debate about the regulation of foreign tech-platforms as national security concerns. This debate continues, and it seems that people haven't reached any definitive conclusion so far.

In fact, the ban of TikTok was not a sudden incident that happened without any signs, but was the culmination of a line of escalating moves under the Sino-U.S. conflicts.[2] With China surging into the field of internet technology, the U.S. technology leadership, which is fundamental to the country's security, prosperity and democratic values, is threatened.[3] Due to its unique interactive nature and network effects, the internet can influence national security in ways that are not traditionally associated with this topic, implicating interests ranging from data privacy, freedom of speech, and economic competitiveness.[4] Apart from the most frequently-quoted risk of the data collection that "threatens to allow the Chinese Communist Party access to Americans' personal and proprietary information" claimed by the president in the executive order,[5] scholars and experts raise great concerns about the financial and economic effects that can be brought by the internet platforms (i.e. the "FinTok" phenomenon).[6] The fact that TikTok and other foreign social media platforms are mainly popular among teenagers and young users[7] further adds to the concerns.[8]

However, the existing presidential actions and the CFIUS process that features strong national security protectionism have been subject to a variety of criticisms. Some allege that the Trump administration's actions blurred together trade and national security issues, and failed to clarify the specific national security dangers as the basis for the CFIUS actions.[9] The executive order was sometimes considered more of a tactical move against a single tech firm than a fully developed policy.[10] Others indicate that shutting down the application is ironic, for such action contributes to the erosion of online freedom and openness which the U.S. has long claimed to defend.[11] There are also scholars who analyze

---

[2] Apratim Vidyarthi & Rachel Hulvey, *Building Digital Walls and Making Speech and Internet Freedom (or Chinese Technology) Pay for It: An Assessment of the US Government's Attempts to Ban TikTok, WeChat, and Other Chinese Technology*, 17 INDIAN J. L. & TECH. 1, 1 (2021).

[3] Eric Schmidt et al., *Asymmetric Competition: A Strategy for China & Technology*, China Strategy Group, 3 (2020), https://perma.cc/TQ4R-CVXG (last visited Jan 23, 2023).

[4] Gary P. Corn et al., *Chinese Technology Platforms Operating In The United States*, HOOVER INSTITUTION, 1 (2021), https://www.hoover.org/research/chinese-technology-platforms-operating-united-states (last visited Jan 22, 2023).

[5] Exec. Order No. 51,297, 85 C.F.R. 1 (2020).

[6] *See* Nikita Aggarwal, D. Bondy Valdovinos Kaye & Christopher K. Odinet, *#Fintok and Financial Regulation*, 54 Ariz. St. L.J. 333 (2023).

[7] H. Tankovska, *TikTok UserRation in the U.S. 2020, by Age Group*, STATISTA (2022), https://www.statista.com/statistics/1095186/tiktok-us-users-age/ (last visited Jan. 26, 2023).

[8] Jake T. Seiler, *TikTok, CFIUS, and the Splinternet*, 29 U. MIAMI INT'L & COMP. L. REV. 36, 155 (2021).

[9] *See* Alicia Faison, *TikTok Might Stop: Why the IEEPA Cannot Regulate Personal Data Privacy and the Need for a Comprehensive Solution Note*, 16 DUKE J. CONST. L. & PUB. POL'Y SIDEBAR 115, 119 (2021); Vidyarthi and Hulvey, *supra* note 1 at 30; Enrique Dans, *A splinternet will take us in the wrong direction*, MEDIUM 37 (2020), https://medium.com/enrique-dans/a-splinternet-will-take-us-in-the-wrong-direction-ef0a0e1f12b9 (last visited Jan 18, 2023).

[10] *See* Justin Sherman, *Building a Better U.S. Approach to TikTok and Beyond*, LAWFARE (Dec. 28, 2020), https://www.lawfareblog.com/improving-tech-policy# [https://perma.cc/5T2X-BYMZ].

[11] Samm Sacks, *Banning TikTok Is a Terrible Idea*, SUPCHINA (July 16, 2020),

the regulatory action from the perspective of the First Amendment and reach the conclusion that the TikTok ban should be struck down as unconstitutional.[12]

In fact, the challenge of regulating foreign tech-platforms has two facets. On one hand, the U.S. government is in urgent need of well-designed policies to protect its core security interests from the rapid spread of Chinese platforms, and to sustain its technological competitiveness against China's growing technology industry. On the other hand, the government has long held a "tech neoliberalism" position in terms of the business policies and the internet regulation, and advocates a "world wide web" with full openness and freedom.[13] Therefore, the sudden shift of the attitude will cause concerns that the U.S. is contributing the formation of a wall-off and splintered battleground, taking the Beijing's strategy that it has long criticized,[14] and it "sets a very bad precedent".[15] In a nutshell, the issue at stake is to seek for a regulatory framework that balances the interests of internet openness and national security well.

This article provides three paradigms envisioned by scholars for r foreign tech-platform regulation. Part I introduces the first laissez faire paradigm. It inherits the values of early neoliberalism, and the belief that it is necessary to protect the "open internet" or a "world wide web.[16] Looking back on the past few decades, the internet platform not only helped spread U.S. values across the world and activates a considerable amount of political movement, but also stimulated economic growth and prosperity. Laissez faire advocates further raise the concern of a "Splinternet", claiming that the arrival of a fragmented and divided internet will greatly hinder freedom of speech and expression as well as the digital economy globally.[17] However, most of the concerns raised by the tech neoliberalists have been challenged as more conceptual than real, and when faced with the actual risks posed by foreign platforms, its inaction fails to deal with novel security threats.[18]

Then, Part II discusses the second case-by-case restrictions paradigm, which is presently the most mainstream and frequently-discussed scheme. Though the advocates of this paradigm also acknowledge the importance of an open world wide web and the dangers of Splinternet, they deem it necessary to take regulatory measures when threats to national security exist. The paradigm indicates a case-by-case analysis for specific risks at hand to apply tailored regulation measures, and is closely related to the present CFIUS process.[19] It recognizes the blurriness of existing non-systemic actions and has caused a flourishing of risk assessment methods proposed by scholars. However, the inconsistency, unpredictability and the complexity of rules constitute its inborn deficiency, and the non-

https://thechinaproject.com/2020/07/16/banning-tiktok-is-a-terrible-idea/ [https://perma.cc/P2Z8-KDFQ].

[12] Cara Groseth, *An Economic Analysis of Banning TikTok: How to Weigh the Competing Interests of National Security and Free Speech in Social Media Platforms*, SSRN J., 28–39 (Dec. 16, 2020), https://www.ssrn.com/abstract=3750779.

[13] *See infra* Parts I.A-B.

[14] Dans, *supra* note 9.

[15] Marimar Jiménez, *Trump rompe definitivamente el sueño de una internet universal*, CINCO DÍAS (2020), https://cincodias.elpais.com/cincodias/2020/08/09/companias/1596960191_078282.html (last visited Jan 19, 2023).

[16] *See infra* Section I.A.

[17] *See infra* Section I.B.

[18] *See infra* Section I.C.

[19] *See infra* Sections II.A-B.

transparency of the CFIUS review also add to the risk of potential abuses of executive power.[20]

The last platform-utilities paradigm is an innovative new approach, which is reviewed in Part III. Advocates of this paradigm identify the similarity between the new tech-platforms and traditional utilities platforms for they share the same political-economy features, and thus envision a sectoral regulation on the tech-platforms.[21] By reviewing the history of restriction on foreign platforms, this paradigm not only illustrates that the sectoral regulation scheme has legitimate precedent and pedigree, but also takes lessons and strategies from common measures of foreign platforms restrictions.[22] Nonetheless, the great differences between the internet platforms and the traditional utilities platforms cast doubts on replicating the regulatory measures for traditional utilities platforms. Also, the shift from the U.S. long standing open attitude and the risk of second order effects due to U.S. identity asymmetry: The U.S. is not only the largest investor but also the largest recipient in FDI, so the strict regulation taken by the U.S. against foreign companies will be used by other countries to justify similar actions against U.S. companies abroad, all require further reflection.[23]

As for Part V, the TikTok saga will be briefly reviewed chronologically and the latest regulation attempt of Executive Orders of different States..[24]

Before turning to Part I, it shall be affirmed that all the strategies are illuminating for future regulatory policies, and what should be expected is not a perfect solution but one that is relatively more viable and less costly. To that end, policymakers must carefully compare the different approaches to figure out the optimal solution best balancing internet openness and national security.

I. THE LAISSEZ FAIRE PARADIGM

Early internet thinkers envisioned a totally free internet with no boundaries, from which tech neoliberalism derives. Under the rhetoric of tech neoliberalism, people call for a laissez faire approach for the sake of the economic and political benefits that an "open internet" can bring about. However, as more and more countries and regions have begun regulating tech-platforms, the atmosphere subtly changed and so did the U.S. government's attitude.

A. Tech Neoliberalism Advocates a World Wide Web

Those who suggest that the government should adopt a laissez faire approach toward foreign tech platforms firmly believe that it is necessary to protect the "open internet" or a "world wide web" for the sake of free flow of information and economic benefits.[25] Thus, any kind of international governance is undesirable. The attitude derives from the

[20] *See infra* Section II.C.
[21] *See infra* Section III.B.
[22] *See infra* Section III.A.
[23] *See infra* Section III.C.
[24] *See infra* Part V.
[25] Seiler, *supra* note 8, at 54.

neoliberalism theory of political economy that has dominated public policy in the U.S. for decades.[26] Neoliberalism endorses the free-market economy and believes that a society's political and economic institutions should be robustly liberal and capitalist.[27] From the perspective of neoliberalism, in the field of foreign investment, minimal state intervention is pursued, the free flow of capital is encouraged, and national security concerns are downplayed.[28]

Indeed, such "tech neoliberalism" is the long-held position of the U.S. From the second term of Clinton's administration to the end of the Obama administration, an "internet freedom" is always what the U.S. government advocated.[29] "Internet freedom", as Jack Goldsmith has summarized, comprises two related principles: The first is the non-regulatory principle, as President Clinton and Vice President Gore put it in 1997, "governments must adopt a non-regulatory, market-oriented approach to electronic commerce".[30] The second is the anti-censorship principle, which calls for freedom of speech and expression on the worldwide web.[31] Across administrations, the U.S. government took great efforts to pursue such internet freedom.[32] In 2006, the George W. Bush administration established the Global Internet Freedom Task Force (GIFT) to promote anti-censorship.[33] During the Obama administration, Secretary of State Hillary Clinton delivered a 2010 speech that expressed the most elaborate and mature idea of internet freedom yet.[34] It cost the government at least $105 million on anti-regulation and anti-censorship projects, including encryption investment and filter-circumvention products.[35] It is arguable that for decades the U.S. government has always faithfully conformed to the "leave us alone" calling proclaimed in the renowned "Declaration of the Independence of Cyberspace" by Barlows.[36]

However, such laissez faire approach is not purely for the noble reasons of championing freedom of speech or individuals' privacy, but for some practical reasons of politics and economy.

One significant benefit brought by a "free internet" or a powerful "world wide web" is undoubtedly political. The free internet provides platforms to spread democracy and

---

[26] *See generally* GARY GERSTLE, THE RISE AND FALL OF THE NEOLIBERAL ORDER: AMERICA AND THE WORLD IN THE FREE MARKET ERA (2022).

[27] Kevin Vallier, *Neoliberalism*, THE STAN. ENCYCLOPEDIA OF PHIL. (Edward N. Zalta & Uri Nodelman eds., Winter 2022), https://plato.stanford.edu/archives/win2022/entries/neoliberalism/ (last visited Jan. 17, 2023).

[28] Ganesh Sitaraman, *The Regulation of Foreign Platforms*, 74 Stan. L. Rev., 1073, 1137 (2022).

[29] Jack Goldsmith, *The Failure of Internet Freedom*, Knight First Amendment Institute 2 (2018), https://perma.cc/3PFP-3QUB.

[30] Office of the Press Secretary of the White House, *A Framework for Global Electronic Commerce: An Executive Summary*, 31 TELECOMMUNICATIONS 35 (1997).

[31] Goldsmith, *supra* note 5, at 2.

[32] *Id.* at 4.

[33] Bureau of Public Affairs Department of State. The Office of Electronic Information, *Global Internet Freedom Task Force*, US Department of state archive (2008), https://2001-2009.state.gov/g/drl/lbr/c26696.htm.

[34] Joshua Keating, *Clinton on Internet freedom*, FOREIGN POLICY (Jan. 21, 2010), https://foreignpolicy.com/2010/01/21/clinton-on-internet-freedom/.

[35] Goldsmith, *supra* note 5, at 4.

[36] John Perry Barlow, *A Declaration of the Independence of Cyberspace,*, (Feb. 8, 1996), https://perma.cc/8GYP-TG23 (last visited Jan 16, 2023).

freedom, allowing U.S. values and discourse to spread across Africa and the Middle East.[37] A great number of political movements have been activated with the aid of the free internet: During the COVID-19 pandemic, 2020 has witnessed numerous heated debates, online activism and large-scale protests happening on the internet, which reflects the strong effect a worldwide web can have on politics.[38] In fact, the political effects of the internet is a long-disputed topic between the U.S. and authoritarian countries; opposite to the actions of the U.S., authoritarian countries are always making efforts to defeat "unwanted" internet activities within their borders and prevent the "import" of U.S. values.[39]

Moreover, the open free internet can bring tremendous economic benefits as well. According to a report published by McKinsey Global Institute, the internet accounts for 3.4 percent of GDP on average across the large economies that make up 70 percent of global GDP.[40] Internet-based products have attracted great investors around the world, and the industry drives much of Foreign Direct Investment that supports more than 7 million jobs in the U.S. with over $200 billion of inward capital flow in recent years.[41] And it is suggested that despite its magnitude and reach, the internet is still very much in its infancy.[42]

In a nutshell, the societal efficiencies and economic growth all serve as incentives for the U.S. government to adopt a neoliberalist approach to internet platforms for quite a long time. However, the rise of TikTok, an internet platform prevalent within the U.S. but owned by a Chinese enterprise, brought a subtle change to the situation. The shift of identity—from the one who provides Googles, Twitter and Facebook that have influenced the rest of the world, to the one who is being greatly influenced by TikTok—created a sense of crisis within the U.S. government. And the subsequent actions taken by the Trump administration seemed to be a significant deviation from the government's long-term laissez faire attitude, raising great concern about the internet's openness.

But after all, what would happen when the web became not so "worldwide" and was divided into limited communication? The possible resultant "Splinternet" serves as a springboard for further discussion.

B. The Splinternet Concern

The Splinternet is also called "cyber-balkanization" or "internet balkanization", which refers to a characterization of the Internet as splintering and dividing due to various factors.[43] Such splintering or dividing results in country-specific and region-specific

---

[37] Catherine O'Donnell, *New study quantifies use of social media in Arab Spring*, SCIENCEDAILY, (Sept. 16, 2011), https://www.sciencedaily.com/releases/2011/09/110914161733.htm (last visited Jan 17, 2023).
[38] Seiler, *supra* note 7 at 52–53.
[39] Goldsmith, *supra* note 5 at 4.
[40] James Manyika & Charles Roxburgh, *The great transformer: The impact of the Internet on economic growth and prosperity*, MCKINSEY GLOBAL INSTITUTE, 1 (2011).
[41] Seiler, *supra* note 7 at 54.
[42] Manyika and Roxburgh, *supra* note 39 at 6.
[43] Splinternet, WIKIPEDIA (2022), https://en.wikipedia.org/w/index.php?title=Splinternet&oldid=1127029285 (last visited Jan. 19, 2023).

internet as nation states compete for data sovereignty.[44] The governments are capable of imposing their own internet regulations because the delivery of all kinds of digital services online just doesn't happen somewhere in the sky, but in data centers that have to be based on somebody's sovereign territory.[45] Keith Weight has warned that the arrival of a fragmented and divided internet is already upon us, and calls for advocates supporting a free and open internet to stem the tide.[46]

The Splinternet is caused by a variety of factors, including technology, commerce, politics and divergent national interests,[47] among which national security is the most frequently cited. As a matter of fact, China and Russia have long been the biggest internet regulators that adopt measures leading to increasing internet authoritarianism. Iranian and Turkish politicians are pushing "information sovereignty", and Saudi Arabia, Syria and Yemen are joining in as well.[48] Nevertheless, it is not just the Chinese model and other authoritarian followers that threaten the open world web internet.[49] The EU and Brazil have enforced data privacy regulation to restrict international data processing, in accordance with the GDPR and LGPD respectively, and even the US' strong ally India has enacted its own data sovereignty laws.[50] It is clear that the territorial internet regulation is going viral, both in authoritarian and democratic regimes.

As more and more countries attempt to keep foreign nationals off certain web properties,[51] international companies are obliged to comply with a complicated set of conflicting rules in various key markets.[52] This is quite a daunting task for the businesses because they have to be aware of every different set of laws and bend to them accordingly.[53] Digital content available in the U.K. via the BBC's iPlayer is becoming increasingly unavailable to Germans, and South Korea filters and blocks news agencies belonging to North Korea. As Keith Wright puts it, "Never have so many governments, authoritarian and democratic, actively blocked internet access to their own nationals."[54] For U.S. companies, the task is even more demanding because, contrary to companies outside the U.S. that have long been aware of their own national data restriction rules, US tech-companies are usually accustomed to a market in which data moves freely across borders.[55] The rapidly shifting technological landscape has also fundamentally reshaped the process

---

[44] Jeff Kim, *The Splinternet is here and your company needs to be ready*, TNW | PODIUM (2019), https://thenextweb.com/news/the-splinternet-is-here-and-your-company-needs-to-be-ready (last visited Jan. 18, 2023).
[45] L.S., *What is the "splinternet"?*, THE ECONOMIST, https://www.economist.com/the-economist-explains/2016/11/22/what-is-the-splinternet (last visited Jan. 18, 2023).
[46] Keith Wright, *The "splinternet" is already here*, TECHCRUNCH (2019), https://techcrunch.com/2019/03/13/the-splinternet-is-already-here/ (last visited Jan. 18, 2023).
[47] Splinternet, *supra* note 42.
[48] Keith Wright, *supra* note 45.
[49] Kim, *supra* note 43.
[50] *Id*.
[51] Keith Wright, *supra* note 45.
[52] Global Business Policy Council (GBPC), *Competing in an age of digital disorder*, KEARNEY, https://www.kearney.com/web/global-business-policy-council/article/-/insights/competing-in-an-age-of-digital-disorder (last visited Jan 21, 2023).
[53] Seiler, *supra* note 7 at 56.
[54] Keith Wright, *supra* note 45.
[55] Kim, *supra* note 43.

of investing.[56] In recent years, governance and regulatory factors have been the most important considerations investors take into account when choosing markets.[57] Thus, the increasing internet restrictions trend is by no means welcomed by investors. Furthermore, there is also an increasing risk of "islandized" segments of the global digital economy when global supply chains are gradually fragmented.[58]

In the political field, the Splinternet arouses great concerns regarding tremendous censorship and suppression of freedom of speech.[59] For instance, as a typical measure to wall-off sensitive information within the border, the "China's Great Fire Wall" has long been criticized by the U.S. government and American high-tech companies. In 2016, U.S. trade officials accused China's Great Wall of creating an internet barrier and blocking free speech and thought, with former Google CEO Eric Schmidt claiming that "the Chinese Firewall will lead to two distinct Internets."[60] And when the Trump government adopted restrictions directed against TikTok, a number of commentators critiqued that such action was nothing less than the formation of a walled-off and splintered battleground on the internet. Enrique Dans points out that Washington is now copying Beijing's strategy that it has long criticized. Pompeo's phrase "a clean internet free of untrusted Chinese apps" eerily echoes Iranian vice president Ali Agha-Mohammadi's announcement to establish the country's "halal internet" based on "Islamic values that will provide appropriate services."[61] Marimar Jiménez condemned the U.S. government's actions as "set[ting] a very bad precedent."[62] In the neoliberalists' view, the open internet connects people around the world in hyper-personalized but often international subcultures,[63] but the present U.S. regulatory action is destroying it.

The downsides of the Splinternet seem to consist of everything from creating significant hurdles for international businesses to prohibiting freedom of speech and thought.[64] However, does it necessarily mean that a neoliberalist approach should be adopted? Or in other words, does the option of a neoliberalist approach necessarily solve these problems? Opposing ideas have been raised.

C. Criticism of the Laissez Faire Approach

Albeit reasonable, the tech neoliberalism rhetoric has been challenged by a number of scholars for several reasons.

Ganesh Sitaraman reckons that this theory suffers from three main problems. First, the actual internet is not as free or open as the tech neoliberalists think it is. A number of countries have already adopted internet regulations. In fact, TikTok itself demonstrates this for it is not globally available. Second, the possible censorship resulting from total nonregulation may functionally mean less freedom within the U.S., as free speech can be

---

[56] Global Business Policy Council (GBPC), *supra* note 51.
[57] *Id*.
[58] *Id*.
[59] Seiler, *supra* note 8, at 56–57.
[60] Wright, *supra* note 45.
[61] Dans, *supra* note 9.
[62] Jiménez, *supra* note 15.
[63] Joss Fong & Christophe Haubursin, *The Bigger Stakes of the TikTok Debate*, VOX, https://perma.cc/7GSM-EVWS (last visited Jan 16, 2023).
[64] Kim, *supra* note 44.

easily blocked by tech-platforms when there is no regulation at all. Finally, internet governance is not a binary choice between fascism and total nonregulation, and tech neoliberalism exaggerates the effects of proper regulation.[65] Jake Seiler also points out that the problems arising out of the Splinternet are over-exaggerated, and that the utility of TikTok as an amusing platform is actually so minimal that restrictions on it can hardly damage political values.[66] It seems that most of the concerns raised by the tech neoliberalists are more conceptual than real. Focusing on TikTok, it is clear that the actual cybersecurity risks posed by the app are more worrisome, and the U.S. must take action to protect itself.[67] At present, tech neoliberalism is unable to respond to these challenges.

In fact, a laissez faire approach that totally gives up the regulation of foreign tech-platforms is not likely to be the future choice for the U.S. government. Since every industry is subject to various legal restrictions, tech-platform can by no means be an exception. As Sitaraman puts it, "the question, as always, is what set of legal restrictions should apply and when."[68]

II. CFIUS AND THE CASE-BY-CASE RESTRICTIONS PARADIGM

Dating back to November 2019, the Committee on Foreign Investment in the United States (CFIUS) started its investigation into the acquisition of Musial.ly by ByteDance, the parent company of TikTok.[69] In the later-released executive order, President Trump claimed that there was credible evidence that ByteDance's actions "threatened to impair the national security of the United States" and CFIUS was authorized to implement measures it deemed necessary and appropriate to verify compliance with this order.[70] Such case-by-case assessment and the CFIUS process are contemporarily the main regulatory approaches toward foreign tech-platforms. Some refer to this kind of regulation paradigm as "national security technocratic," the advocates of which focus on narrowly tailored rules on a case-by-case basis instead of structural rules.[71]

A. The Committee on Foreign Investment in the United States

1. The Origins and Development of CFIUS

The Committee on Foreign Investment in the United States (CFIUS) is an interagency body established by an executive order of President Ford to assist the President in reviewing the national security issues of foreign direct investment in the U.S. economy.[72] According to the executive order, CFIUS was intended to:

---

[65] Sitaraman, *supra* note 28, at 1084–1087.
[66] Seiler, *supra* note 8, at 57.
[67] *Id.* at 58.
[68] Sitaraman, *supra* note 28, at 1087.
[69] Greg Roumeliotis et al., *Exclusive: U.S. opens national security investigation into TikTok - sources*, YAHOO (NOV. 1, 2019), https://news.yahoo.com/exclusive-u-opens-national-security-152048538.html.
[70] Regarding the Acquisition of Musical.ly by ByteDance Ltd., 85 Fed. Reg. 51297 (Aug. 14, 2020).
[71] Sitaraman, *supra* note 28 at 1087.
[72] Exec. Order No. 11,858, 40 Fed. Reg. 20,263 (May 7, 1975).

> (1) arrange for the preparation of analyses of trends and significant developments in foreign investment in the United States; (2) provide guidance on arrangements with foreign governments for advance consultations on prospective major foreign governmental investment in the United States; (3) review investment in the United States which, in the judgment of the Committee, might have major implications for U.S. national interests; and (4) consider proposals for new legislation or regulations relating to foreign investment as may appear necessary.[73]

Despite the ambitious goal set at its establishment, CFIUS operated in relative obscurity for a long time.[74] Between 1975 and 1980, for instance, the Committee met only ten times and was unable to respond to the political or the economic aspects of foreign direct investment.[75] Later in 1988, the Exon-Florio amendment was approved by Congress and included the Omnibus Trade and Competitiveness Act, which stipulated that the President may exercise the authority to suspend or prohibit any transaction that threatens to impair the national security of the U.S. if it is found that:

> (A) there is credible evidence that leads the President to believe that a foreign person that would acquire an interest in a United States business or its assets as a result of the covered transaction might take action that threatens to impair the national security; and
>
> (B) provisions of law, other than this section and the International Emergency Economic Powers Act, do not, in the judgment of the President, provide adequate and appropriate authority for the President to protect the national security in the matter before the President. [76]

Though CFIUS was not directly mentioned in the Act, President Reagan administered the Exon-Florio provision to CFIUS.[77] Afterwards, the 1992 "Byrd Amendment" further refined the CFIUS process such that two requirements should be met: "(1) the acquirer is controlled by or acting on behalf of a foreign government; and (2) the acquisition results in control of a person engaged in interstate commerce in the United States that could affect the national security of the United States."[78] As CFIUS's functions and processes were polished, the Committee received more and more attention from Congress as well as the general population.[79]

Nevertheless, it was not until the terrorist attack happened on September 11, 2001 that members of Congress greatly altered their view regarding the FDI and national security concerns, and thus greatly changed the status of CFIUS.[80] In 2006, CFIUS's review of the

---

[73] *Id.*
[74] James K. Jackson, CONGRESSIONAL RESEARCH SERV., RL3888, The Committee on Foreign Investment in the United States (CFIUS) at 4, (Feb. 14, 2020).
[75] HOUSE COMM. ON GOV'T OPERATIONS. REP. NO. 96-1216, at 166-184 (1980).
[76] The Defense Production Act, 50 U.S.C. § 4501 (2018).
[77] Exec. Order No. 12,661, 54 Fed. Reg. 779 (Dec. 27, 1988).
[78] Jackson, *supra* note 49, at 9.
[79] Seiler, *supra* note 7, at 38.
[80] *Id*. at 5.

acquisition of six U.S. ports Dubai Ports World caused heated discussion regarding CFIUS and the way it operated, which spurred the Bush Administration to make the most comprehensive reconstruction of CFIUS by signing the Foreign Investment and National Security Act of 2007 (FINSA). FINSA granted CFIUS new statutory authority, added more control of Congress over the Committee, required the Secretary of the Treasury to designate an agency, and stipulated detailed time requirements for the review process.[81]

In the past few years, the national security landscape has greatly shifted for the U.S. as China rose to become its biggest rival and the global governance order has gradually changed, which thus changed the greatest potential risk to national security in the aspect of investment.[82] Chinese technology investment in the U.S. has caused more and more national security concerns, and in response, the Trump administration enacted the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), which expanded the scope and jurisdiction of CFIUS by redefining "covered transactions" and "critical technologies", further specified the reviewing process, and broadened the Committee's mandate.[83]

According to the latest annual report released by CFIUS in 2022, a sharp increase in reviews can be seen during the past decade.[84] In 2021, the number of notices of transactions subject to CFIUS jurisdiction increased to 272, which is the highest number of notices reviewed by the Committee since 2012.[85] The overall number of covered transactions reviewed or assessed by the Committee substantially increased from year to year.[86] It is also worth noting that the CFIUS process has been frequently used recently to review Chinese investment into American hardware and software companies:[87] In 2016, President Obama prevented Chinese company Grand Chip Investment from acquiring the American assets of the semiconductor coating manufacturer company Aixtron. In 2017 and 2018, President Trump blocked two Chinese acquisitions of Lattice Semiconductor and Qualcomm, respectively, where both of which were semiconductor companies. In 2019, Congress initiated a review of Beijing Kunlun Tech's acquisition of the popular LGBTQ dating app Grindr,[88] and shortly thereafter came the sensational investigation and regulation of TikTok and WeChat.

2. The Contemporary Process of CFIUS Review

The contemporary process of CFIUS review can be briefly summarize as follows:[89]

First, the CFIUS process can be started with a voluntary "declaration" or "notice" submitted by the transaction parties, or when a member of the Committee has reason to believe that the transaction is subject to CFIUS jurisdiction in the absence of a voluntary filing. A "declaration" is an abbreviated notification to which the Committee must respond within a 30-day assessment period, during which the Committee can request the parties

[81] Jackson, *supra* note 49, at 10.
[82] *Id.* at 1.
[83] *Id.* at 11-12.
[84] COMM. ON FOREIGN INV. U.S., ANNUAL REP TO CONG. at 8-9 (2021).
[85] *Id*. at 16.
[86] See CFIIUS, Annual Report to Congress at 8-9 (2019).
[87] Vidyarthi & Hulvey, supra note 2 at 29.
[88] *Id.* at 30.
[89] CFIUS, supra note 58 at 9-10.

further submit a written notice or directly initiate a unilateral review.[90]

Second, the Committee is required to complete a "review" of a notified transaction within 45 days. If needed, it may launch an "investigation" that can last up to 45 additional days. Mitigation measures agreed to or imposed by the Committee can be taken to address the national security concerns during this period.

As for the outcome of the "review", if the Committee determines that (1) the transaction does not pose any national security concerns, (2) any national security concerns are adequately addressed by laws other than Section 721 and the International Emergency Economic Powers Act (IEEPA), or that (3) the aforementioned mitigation measures have resolved the security problems, then it will conclude all action with respect to a transaction.

However, if the Committee determines that national security concerns still exist unresolved, it will refer the transaction to the President unless the parties choose to abandon the transaction. The President has to make a decision and publicly announce whether to suspend or prohibit the transaction, including by requiring divestment, within 15 days.

To summarize, the frequent use of CFIUS review in recent years indicates that Congress and the Executive find Committee review an easy and effective method of blocking the sale of companies.[91] It is very likely that it will continue to be the first choice for the U.S. to regulate foreign platforms of national security concern in the short term.

B. The Case-by-Case Restrictions Paradigm

The CFIUS process is closely related to the case-by-case restrictions paradigm, which indicates a case-by-case analysis for specific risks at hand to apply tailored regulation measures.[92] Sitara reckons that this kind of paradigm, or what he calls a "technocratic approach," in many ways is an expansion of the approach that motivates the CFIUS review.[93] Seiler suggests that the CFIUS review and decision toward TikTok is a warranted case-by-case regulatory action.[94] Indeed, the rhetoric behind CFIUS review is similar to the philosophy of the case-by-case paradigm; the tech-platform sectors should be open to foreign investment in principle, and regulation should be imposed on a case-by-case basis when a targeted tech-platform causes security concerns.[95] In that vein, the CFIUS process can be regarded as one specific type of approach under the case-by-case restrictions paradigm.

The advocates of the case-by-case paradigm also acknowledge the importance of an open world wide web and the dangers of Splinternet, just as the tech neoliberalists do. However, they deem it necessary to take regulatory action when foreign internet providers

---

[90] See Id. (finding that CFIUS is authorized to respond in four ways: (1) request that parties file a written notice; (2) inform the parties that the Committee is unable to conclude action with respect to the transaction on the basis of the declaration and that the parties may file a written notice; (3) initiate a unilateral review; or (4) notify the parties that the Committee has concluded all action under Section 721).

[91] *Id.*

[92] *See* Gary P. Corn et al., *Chinese Technology Platforms Operating in the United States*, HOOVER INSTITUTION 6 (2021), https://www.hoover.org/research/chinese-technology-platforms-operating-united-states (last visited Jan 22, 2023); Sitaraman, *supra* note 28 at 1088.

[93] Sitaraman, *supra* note 28 at 1089.

[94] Seiler, *supra* note 8 at 57.

[95] Sitaraman, *supra* note 28 at 1090.

cause risks and threats to the country.[96] They note that the rhetoric of the tech neoliberalists is utopian in that the internet has never been totally free and open. Surveillance of states always exists, and the dangers of internet regulation have been exaggerated by the tech neoliberalists.[97] For instance, the concerns that banning TikTok will let foreign investors completely abandon the U.S. market is not realistic, and the regulation of such an app famous for lip syncing and dancing videos can by no means cause devastating harm to speech freedom and openness.[98] Instead of pointing to an extreme situation when it does not exist, more attention should be paid to the legitimate security concerns posed by TikTok and other foreign digital platforms.[99] As expressed in a Hoover Institution Report, the advocates of this paradigm share a common view that "China's power is growing, that a large part of that power is in the digital sphere, and that China can and will wield that power in ways that adversely affect our national security"[100], and therefore effective regulatory policies are inevitable and necessary.

First and foremost, the case-by-case paradigm emphasizes the importance of specifying the risks and defining the problems of each case in first place. Justin Sherman has criticized that the action towards TikTok taken by the Trump administration lacks such foundation, for "simply asserting 'national security issues' is not enough," and any policy is supposed to "explicitly define the problem" and "clearly articulate the alleged risks at play."[101] Samm Sacks also suggests that the government should "identify the risks created by TikTok and find effective ways to respond to those problems."[102] It is crucial that the government takes action only after explicitly specifying the scope of the cybersecurity concerns at issue.[103] The importance of defining the specific risks and harms on a case-by-case basis lies in the fact that the types of cybersecurity dangers posed by software can vary greatly, and each could be entangled with diverse economic and security issues depending on the specific case.[104] For instance, the cybersecurity risk posed by TikTok differs much from that of Grindr, which is a LGBTQ dating app that has also been blocked by CFIUS from being acquired by a Chinese company. [105] Grindr's extensive collection of intimate data poses risks for blackmail while TikTok's creates concerns more related to censorship and data sharing with the Chinese government.[106] Ignoring such differences will result in ineffective policy design and implementation. As commentators have already pointed out, the Trump administration's actions towards Chinese tech companies often blurred together trade and national security issues, and were unable to clarify the specific national security dangers as the basis for the CFIUS actions.[107] This may lead to a tendency to shut down Chinese digital platforms altogether and will set a dangerous precedent where

[96] *See* Gary P. Corn et al., *supra* note 4 at 1–2; Sitaraman, *supra* note 28 at 1087–88; Seiler, *supra* note 8 at 58–60.
[97] *See* Seiler, *supra* note 7 at 59.
[98] *See* Sacks, *supra* note 10; Seiler, *supra* note 7 at 58–60.
[99] Seiler, *supra* note 7 at 57.
[100] Gary P. Corn et al., *supra* note 3 at 1.
[101] Sherman, *supra* note 9.
[102] Sacks, *supra* note 10.
[103] *Id*.
[104] Sherman, *supra* note 10.
[105] Sacks, *supra* note 11.
[106] Vidyarthi & Hulvey, *supra* note 2, at 16–17.
[107] *See* Faison, *supra* note 9, at 119; Vidyarthi & Hulvey, *supra* note 2, at 30; Dans, *supra* note 9.

the U.S. government may blacklist foreign companies using nothing more than vague concerns about national security as justification.[108]

Further, advocates for the case-by-case restrictions paradigm have provided frameworks for assessing the risks posed by foreign tech-platforms. Sherman offers three dimensions as considerations for the government's executive actions, including (1) explicitly defining the problem, (2) clearly articulating the alleged risks at play, and (3) using cost-benefit calculus to assess whether the supposed risk is likely.[109] Sacks suggests an investigation and regular audits toward foreign tech-platforms to review the type of data being accessed, how that data is being used, and with whom the data is shared.[110]

Among the proposals is the Hoover Institution Report, which is a joint effort of nine distinguished experts—Goldsmith, Sacks, Gary Corn, Jennifer Daskal, Chris Inglis, Paul Rosenzweig, Bruce Schneier, Alex Stamos and Vincent Stewart, gives an elaborative framework for assessing alleged risks in individual cases and aims at inspiring smart policies in response to the regulation challenge of Chinese tech platforms.[111] The report points out that the specific threats and risks, as well as the collateral costs and impacts of each unique technology, varies, and therefore calls for different mitigation measures. It specifies the nature of the risks by foreign technology and categorizes them into three types: "access to data," "influence operations" and "attack vectors," each corresponds with its unique threats of different risky actions that can be conducted by the foreign tech-platforms and its country.[112] To step further, a case-by-case analysis based on necessity and proportionality is introduced, which comprises (1) proper identification of risk, (2) assessment of collateral consequences, and (3) assessment of mitigation measures.[113] In this way, the government can ensure targeted and appropriate responses towards foreign technologies for the sake of the U.S. security and prosperity.

Based on the assessment of case-specific risk, tailored mitigation measures should be undertaken. As advocates of the paradigm have keenly perceived, any regulatory actions taken by the U.S. against Chinese companies will be used to justify similar actions against U.S. companies abroad,[114] and therefore the government should be extremely careful to take narrow, tailored, and effective measures towards the targeted company supported with valid reasons. Otherwise, the second order effects may be more damaging than the original threat.[115] The research group lead by Eric Schmidt and Jared Cohen has proposed a spectrum of mitigations of increasing intensity, including "acceptance of the dependency," "specific concessions negotiated," "specific technical requirements," "proactively enable technology," and consider ban as "a last resort".[116] It is worth noting that other than tailored mitigation measures, advocates of the case-by-case paradigm suggest adopting broad policy responses as well, such as stronger cybersecurity, international engagement, and global cloud computing policies to minimize the threats posed by foreign actors or

[108] Sacks, *supra* note 11.
[109] Sherman, *supra* note 9.
[110] Sacks, *supra* note 10.
[111] Corn et al., *supra* note 3, at 1–2.
[112] *Id.* at 4–6.
[113] *Id.* at 7–9.
[114] Schmidt et al., *supra* note 2, at 10.
[115] *Id.*
[116] *Id.* at 12.

entities.[117]

In a nutshell, the case-by-case restrictions paradigm is the contemporary regulation approach taken by the U.S. government, especially in the form of the CFIUS process. It also constitutes the most mainstream view and raises heated discussion at present. Overall, this paradigm correctly recognizes the lack of clarity of existing government actions and the potential risk of second order effects. The frameworks for assessment proposed by different scholars and experts are undoubtedly inspiring and cast light on the policy-making and CFIUS reviewing process, though this paradigm still faces a few challenges.

C. Challenges to Overcome for the Case-by-Case Paradigm

The case-by-case restrictions paradigm has been challenged by those who support a more aggressive regulatory scheme (i.e., the "platforms-utilities paradigm" to be presented in the following part). This article reviews the various criticisms and classifies them into three categories: the inborn substantial deficiency of the case-by-case paradigm, the shortage compared with a more radical regulation paradigm, and the institutional administrability problem.

This article holds the view that the inborn deficiency constitutes the main problem and requires further reflection. First is the inconsistency and unpredictability of case-by-case restrictions. Due to the case-by-case nature, the paradigm inevitably brings the problem of selective law enforcement.[118] To be specific, the tailored mitigation measures may be inconsistent between firms of similar kind, and thus cause alleged or real unfairness.[119] The confidential and non-transparent features of CFIUS also add to the risk of potential abuses of executive power.[120] Moreover, each regulatory action taken on a case-by-case basis may trigger unforeseeable events of various kinds. As is known to all, the sanctions towards TikTok and WeChat happened during a politically sensitive time in the Sino-U.S. trade conflicts, and some believe it was also concerned with China's 2017 domestic law amendment,[121] and even relevant to the fear that Beijing would use TikTok's platform to spread disinformation to influence the 2020 U.S. national election.[122] Such sudden actions brought by certain political incidents is far from predictable for private foreign investors, and thus will bring the downside of deterring foreign investment.[123]

Some scholars have also criticized that the paradigm omits systemic and potential harms. The criticism is based on the argument that when assessing the risks in detail and requiring the risks to be concrete, the systemic threats of broad data collection may be discounted. Similarly, requiring proof of "actual" harms may also ignore the "future"

---

[117] Corn et al., *supra* note 3 at 9–11.
[118] Sherman, *supra* note 9.
[119] Sitaraman, *supra* note 27 at 1091.
[120] Jackson, *supra* note 80 at 32.
[121] The 2017 Cybersecurity Law of the People's Republic of China stipulates that the government and administrative sector have the access to information to the extent necessary for regulatory purposes, but such discretion of acquiring data is not supposed to exist in the context of Chinese companies overseas and is very likely misinterpreted by U.S. commentators.
[122] Samuel List, *Is National Security a Threat to TikTok? How the Foreign Investment Risk Review Modernization Act Threatens Tech Companies Comments*, 46 SETON HALL LEGIS. J. 173, 203 (2022).
[123] *Id.* at 219 (proposing a Foreign Investment Court to establish precedent and thus increase predictability).

possibility of harms.[124] Such criticism is closely related to the comparison between the case-by-case paradigm and a stricter regulation scheme. The advocates of the latter believe that universal regulatory rules towards all the foreign tech-platforms won't cause the aforementioned problems, since collecting data of large quantities will be forbidden for foreign companies in first place, so the case-by-case paradigm clearly "ignored important alternatives to their proposed policies."[125] Nevertheless, this article deems that these are not "problems" of the case-by-case paradigm, but a tradeoff decided by its underlying logic. As mentioned above, the philosophy of this paradigm is that the tech-platform sectors should be open to foreign investment in principle, and only when specific actors cause security concerns should the regulator intervene.[126] It is inevitable that the case-by-case regulation does not target broad data collection or potential actions, and only takes action when actual and concrete risks occur, because it values openness and denies surveillance in the field of foreign technology investment.

In addition, the critics also challenge that the case-by-case paradigm suffers problems of institutional administration. It is argued that the regulation may suffer from weak enforcement, audit and monitor failure, and the difficulties in regulatory capture due to the great cost and the complexity of rules. Cost may not be an unsolvable problem as the government can inject funds to improve the regulation for the sake of crucial national security concerns, just as it did to improve internet openness during the internet neoliberalism period.[127] The complicated and multifactor case-by-case formulas may be an actual problem. However, the claim that "if a narrowly tailored approach is too difficult to implement effectively, then a clear rule—even if somewhat overinclusive—might be superior,"[128] is doubtful as well. Considering the characteristics of tech-platforms, an overinclusive regulatory rule can hardly be "clear" due to the fact that risk varies greatly from one internet service to another, which will be further discussed in Part III.

Indeed, the case-by-case restrictions paradigm suffers from certain problems due to its nature. However, what should be expected is not a perfect solution but one that is relatively more viable and less costly. To that end, policymakers must carefully compare the case-by-case approach and the stricter sectoral regulation approach to figure out the optimal solution balancing the internet openness and national security.

III. THE PLATFORM-UTILITIES PARADIGM

Drawing on the history of the U.S. restrictions on foreign platforms, Ganesh Sitaraman provides an alternative paradigm: the platform-utilities paradigm, which to some extent can overcome the challenges faced with the aforementioned two paradigms. From Sitaraman's perspective, the long-existing regulations on foreign platforms show legitimacy for the U.S. government to regulate TikTok and other similar tech platforms that share the same political-economy features as traditional foreign platforms. Moreover, the common regulatory measures of traditional foreign platforms can be learned and applied

[124] Sitaraman, *supra* note 27 at 1092–1093.
[125] *Id*. at 1091.
[126] *See infra* Part II.A.
[127] Goldsmith, *supra* note 28 at 4.
[128] Sitaraman, *supra* note 27 at 1094.

in the context of tech-platforms.

A. Restrictions on Foreign Platforms With Political-Economy Characteristics

1. The History of the U.S. Restrictions on Foreign Platforms

Contrary to ordinary tradable goods, businesses with political-economy features have long received special restrictions because they are essential to society. These businesses usually include banking, communications, transportation, and other infrastructure industries.[129] These businesses are sectors of the economy featuring non-rivalrousness andnon-excludability, with high sunk cost, high barriers to entry, and increasing returns to scale due to network effects,[130] and thus are often monopolistic in nature. These sectors of the economy are usually referred to as "regulated industries", which Sitaraman refers to simply as "platform."[131]

Historically speaking, a platform is identified by whether it affects a public interest and thus needs special restrictions.[132] To be specific, a public interest exists when a good or service is "used in a manner to make it of public consequence and affect the community at large".[133] In fact, both in the context of economy and politics exist the potential threats to public interest that require expansive regulatory measures. In terms of the economic aspect, restrictions ought to be imposed against discriminatory pricing and special dealing. And in terms of the political context, the possibility of corruption and the threat brought by economic monopolies should also be regulated.[134]

Taking banking and energy as two examples of platforms, it is clear that regulations on foreign platforms have a long history in the U.S. and include a variety of measures.

Since the founding of the U.S., banking laws have always restricted foreign influence to protect the U.S. financial system. Albeit with the urgent need of foreign capital, people still questioned whether capital from abroad was dangerous. Such concerns resulted in the continual development of banking regulations. From the citizenship restrictions suggested by Alexander Hamilton that only the U.S. citizens can vote as a stockholder when choosing the directors of the banks,[135] to Danial Webster's inspiring idea of the separation of ownership and control,[136] as well as specific retail-banking regulations, foreign banking platforms have been always under strict scrutiny of the government.[137]

Also, in the field of energy and power, restrictions have also been long imposed.[138] As early as 1920, the Federal Water Power Act asked the Federal Power Commission to license

---

[129] *Id.* at 1101.
[130] K Sabeel Rahmant, *The New Utilities: Private Power, Social Infrastructure, and the Revival of the Public Utility concept*, 39 CARDOZO LAW REVIEW, 1641 (2018).
[131] Sitaraman, *supra* note 27 at 1104.
[132] *Id.*
[133] Munn v. Illinois, 94 U.S. 113 (1876).
[134] Sitaraman, *supra* note 4 at 1101–1102.
[135] Alexander Hamilton, *Reports on the Public Credit*, Britannica, https://www.britannica.com/topic/Reports-on-the-Public-Credit (last visited Jan 20, 2023).
[136] Senator Daniel Webster, Addressing the Senate on the President's Veto of the Bank Bill, https://perma.cc/8ZND-KNQ5 (last visited Jan 20, 2023).
[137] Sitaraman, *supra* note 27 at 1106–1113.
[138] *Id.* at 1125–1127.

only U.S. citizens, companies and governments.[139] Similarly, the 1970 Geothermal Steam Act also made power production exclusively available to domestic U.S. subjects.[140] Regarding the nuclear industry, the Nuclear Regulatory Commission (NRC) bars application for a license from a foreign applicant unless the parent company is largely owned by U.S. stockholders.[141]

2. Typical Measures of Foreign Platform Restrictions

Analyzing the previous restrictions that the U.S. government has imposed on foreign platforms, several primary strategies can be summarized, which include ex ante approvals, entry limits and reciprocity requirements, and separation of ownership and control.[142]

First and foremost, ex ante approvals are frequently used strategies to prevent the negative influence of foreign platforms, which basically means that firms have to be reviewed and licensed before they enter into the U.S. market. By conducting ex ante approval measures, the government can not only eliminate the potential risk before negative effects actually happen, but also control all the platforms within a certain industry under a set of universal regulations instead of only a particular firm. It is believed that ex ante approvals can overcome the challenges facing the CFIUS process, in that the CFIUS can only take place when a merger occurs and only towards a specific firm. By contrast, ex ante approvals apparently can be applied more widely and timely.[143]

Secondly, reciprocity requirements are also occasionally made by the government to protect the U.S.' interests.[144] In this way, the government can deny the access of a foreign platform if U.S. domestic companies cannot benefit from the market of its home country. Actually, in the context of the tech-platforms, foreign equivalents of TikTok and WeChat have been long banned by the Chinese government, and such kind of asymmetry is unfair and intolerable.[145] Thus, the requirements which ask the home country of the platform's parent company to give reciprocal treatment can be a legitimate reason as well as an effective way to regulate TikTok and other Chinese tech-platforms to defend the U.S.' interests.

Finally, separation of ownership and control is another controversial but commonly used strategy. Citizenship rules are usual provisions that require that the directors be U.S. citizens, or foreign ownership without U.S. citizenship is isolated from the decision-making process.[146] As Andrew Verstein observes, the "national security corporate governance", which indicates that government representatives take the control of the boardrooms of private entrepreneurs and to deny illegal or risky plans for public purposes,

---

[139] Cong. Rsch. Serv., The Federal Power Act (FPA) and Electricity Markets (2017), https://perma.cc/UHY3-FWC2.
[140] Geothermal Steam Act of 1970, Pub. L. No. 91-581 (1970) (current version at 30 U.S.C. §§ 1001-1027). .
[141] *Foreign Ownership, Control, or Domination (FOCD) of Commercial Nuclear Power Plants*, U.S.NRC, https://www.nrc.gov/reactors/focd.html (last updated Feb. 9, 2023).
[142] Sitaraman, *supra* note 28, at 1127.
[143] *Id.* at 1128.
[144] *See, e.g.*, Reciprocal Tariff Act, ch. 474, 48 Stat. 943 (1934) (current version at 19 U.S.C. § 1351).
[145] Tim Wu, *A TikTok Ban Is Overdue*, THE NEW YORK TIMES, https://perma.cc/ZN7P-B2K9 (last visited Jan 20, 2023).
[146] Sitaraman, *supra* note 28 at 1130.

is quite widespread and of great importance.[147] Nevertheless, this strategy faces a few challenges. To be specific, the citizen rules are against the principles of corporate law; also, it is not ensured that the U.S. citizens as directors will not be manipulated by foreign investors, and administration problems also exist for it is difficult to specify the percentage of permissible foreign investment.[148]

All the aforementioned strategies used for regulating traditional platforms can be illuminating in the context of foreign tech platforms regulations. On the one hand, the history of imposing various restrictions on platforms back the legitimacy of regulating foreign tech platforms. On the other hand, these strategies can also selectively be adopted in the regulation of foreign tech-platforms.

B. The Platform-Utilities Paradigm

1. The Shared Characteristics of Tech Platforms and Traditional Platforms

Despite the varied features of different types of platforms, one of the most important characteristics shared by all platforms and distinguishes them from other products is the strong political-economy dynamics.[149] Power and energy, communications, transportation, and banking all raise national security concerns regarding sovereignty, democracy, economics, and public interest.[150] And it is exactly these characteristics that raise national security concerns regarding personal data and privacy, which makes governmental regulation legitimate and inevitable.

The political-economy features of tech platforms is rather obvious, especially with giant platforms of great influence. As discussed in Part I, the booming tech platforms nowadays substantially impact economic development as well as freedom of speech and expression. When defining the "platforms," Lina Khan raised five relevant factors to be considered: (1) "the extent to which the entity serves as a central exchange or marketplace for the transaction;" (2) "the extent to which the entity is essential for downstream productive uses;" (3) "the extent to which the entity derives value from network effects;" (4) "the extent to which the entity serves as infrastructure for customizable applications by independent parties;" and (5) "the size, scope, scale, and interconnection of the company."[151] By weighing these factors, Khan indicates that Google, Amazon and other online providers all constitute dominant digital platforms that can result in conflicts of interest, thwart competition and stifle innovation, and thus need the structural separation regulation.[152]

In the case of TikTok, users are mainly teenagers or children, and various personal data have been collected for precise advertising, which in addition amplifies its platform-utilities feature. Also, it is rather clear that from the supply chain perspective and considering the five factors mentioned above, the tech platforms by no means belong to the same category of ordinary tradable goods. In fact, the tech platforms are special ones

---

[147] Andrew Verstein, *The Corporate Governance of National Security*, 95 WASH. U. L. REV., 775, 777–778 (2018).
[148] Sitaraman, *supra* note 28 at 1131–1133.
[149] *Id.* at 1101.
[150] *Id.* at 1139.
[151] Lina M. Khan, *The Separation of Platforms and Commerce*, 119 COLUMBIA LAW REVIEW, 119 (2019).
[152] *Id.* at 973.

that feature political-economy characteristics but appear in different traditional platforms sectors: for instance, Alipay in banking and TikTok in communications.[153]

To sum up, the shared political-economy dynamics of current tech platforms and traditional platforms indicates reconsideration of the regulation modes. Those who advocate laissez faire approach or the case-by-case approach may neglect the fact that these approaches mainly target ordinary tradable goods instead of platforms with special political-economy characteristics. Indeed, "categorizing tech-platforms as platforms" reveals the inappropriateness of applying the general rules of ordinary tradable products to tech-platforms, and therefore "suggests an alternative path forward."[154]

2. Applicable Regulatory Measures of the Platform-Utilities Paradigm

Regarding specific measures of the platform-utilities paradigm, Sitaraman envisions the applicable sectorial rules as "sector before firms" and "structural separation." The paradigm also calls for international cooperation to improve interconnection, and resorts to public investment and options to supplement private investment.[155]

To begin with, platform-utilities regulation begins with sectoral rules towards separated subjects of different categories, so that the administration can be conducted easily, predictably, and consistently.

The first rule is "sector before firms," setting sectoral regulation standards in sharp contrast with the case-by-case process of CFIUS.[156] As a matter of fact, the potential risk varies from sector to sector, but may not vary as much within a sector. Thus, a universal regulation rules across each sector is desirable. And compared with the case-by-case approach, such as a presidential executive order, regulations based on the sectoral rules are not only easier to administer for the government, but also more predictable for the platform's investors. Combined with the aforementioned traditional ex ante measures, the clarity of definite and universal rules for the whole sector would create a level competing atmosphere and prevent the abuse of administrative power.[157]

The second rule is "structural separation," which indicates regulations are separated under different criteria. Structural separations of regulations can be conducted easily and clearly, albeit in an over-inclusive way. Geographic separation, governance separation, and activity separation are three common practices.[158] It is worth noting that in the tech platforms context, special internal separations have been identified. Specifically, it is suggested that ByteDance can adopt RBAC (role-based access control) to alleviate geopolitical concerns, which means setting up an internal firewall so that its Chinese personnel cannot access data in the U.S., and each department has its own database.[159]

What's more, international standards and shared regulatory criteria should be set to improve interconnection between countries. In fact, as a report by The Economist puts it, "What is needed, they said, is more international co-operation—but not of the old kind."[160]

---

[153] Sitaraman, *supra* note 27, at 1082.
[154] *Id.* at 1105.
[155] *Id.* at 1140–46.
[156] Seiler, *supra* note 7, at 11.
[157] Sitaraman, *supra* note 27 at 1140–1142.
[158] *Id.* at 1141–1143
[159] Kevin Xu, *Can ByteDance Build Trust?*, https://perma.cc/WC36-YFCL (last visited Jan 20, 2023).
[160] L.S., *supra* note 45.

Whether it is a constellation of "multi-stakeholder" organizations[161] or a UN open internet (OI) system,[162] intensifying worldwide co-operation in the context of the internet has been frequently raised as a solution to isolation effects due to regulation. It is believed that by sharing the regulatory standards with its allies, foreign investors will find it easy to fulfill compliance obligations under U.S. regulations.[163]

Finally, to deal with the possible damage to foreign investment due to regulation, which Sitaraman regards as inevitable, public investment and public provision can complement and thus reduce reliance on foreign investment in the tech platforms. Since the U.S. has historically adopted these two practices, their feasibility is also ensured.[164]

C. Reviews on the Platform-Utilities Paradigm

The platform-utilities paradigm is relatively new scheme. It boldly raises the idea that the U.S. government can impose special regulations on the whole foreign tech platform sector due to its unique features of political-economy. Reviewing the history of restrictions on foreign platforms reveals this paradigm is legitimate with precedent and pedigree, and that it takes lessons and strategies from common measures of foreign platforms restrictions. The platform-utilities paradigm updates existing regulatory paradigms developed to regulate ordinary tradable goods and provides us with a new perspective on the public interests at play with special platforms. However, the paradigm still faces several challenges.

First, the digital tech platform differs greatly from traditional platforms. Digital platforms are systems that facilitate interactions and transactions between multiple groups. A platform's economic value and activity is driven by the parties using the platform, rather than just the company that builds and mediates the platform.[165] To that end, the sole reason that platforms "have some shared political-economy dynamics"[166] may not be sufficient for replicating the regulatory measures for traditional utilities platforms. As tech platforms rely on network effects to gain momentum and scale, regulatory measures for traditional utilities platforms such as entry restrictions and structural separation may greatly hinder the development of the industry. Public investment from U.S. domestic markets is not able to gather enough production factors, including but not limited to cross-border capital, data, and technology. Also, universal regulatory rules across the whole sector may be difficult to establish, given that the inherent risks drastically vary from one platform to another.[167] The traditional trade reciprocity requirements are very likely to be ineffective as well, as China's domestic markets are larger than the U.S. market and may not be willing to offer reciprocity.[168]

Also, restrictions on the whole sector do not parallel the U.S.'s long standing position, and may therefore deter foreign investment. The U.S.' policy approach to international investment generally aimed to establish an open and rules-based system consistent across

---

[161] *Id.*
[162] Keith Wright, *supra* note 46.
[163] Sitaraman, *supra* note 2, at 1145.
[164] *Id.* at 1145–1146.
[165] Eric Schmidt et al., *supra* note 3, at 10.
[166] Sitaraman, *supra* note 28, at 1080.
[167] *See supra* Part II.B.
[168] Eric Schmidt et al., *supra* note 3 at 10.

countries and in line with U.S. interests. [169] As a matter of fact, the country has acted as an open internet protector for decades,[170] and sudden restrictions on the whole tech platforms sector would probably concern investors worldwide. It is worth noting that a sectoral regulation not only acts on investors from rival countries, but potential investors all around the world. So strict and unpleasant restrictive requirements such as the separation of ownership and control may greatly damage overall investment enthusiasm. Furthermore, the domestic public investment by the U.S. government suggested by advocates of the paradigm[171] cannot make up for the loss considering the high percentage the foreign investment takes in U.S. technology markets.[172]

A step further, as the largest global foreign direct investor as well as the largest recipient of foreign direct investment,[173] The U.S. has an identity asymmetry and thus should try to avoid the second order effects that actions taken by the U.S. against foreign companies will be used to justify similar actions against U.S. companies abroad, which may be more damaging to U.S. interests than the original threat.[174]

Apart from the problems caused by the inappropriateness of transplanting traditional regulatory measures to new tech platforms regulation, other side-effects of traditional sectoral regulation, such as suppression of technology regulation and monopolies of domestic companies, exist as well.

IV. THE TIKTOK SAGA AND THE LATEST ATTEMPTS BY NORTH CAROLINA

A. Brief Overview of the TikTok Saga

As early as November 2017, TikTok's parent company ByteDance acquired the U.S.-based Musical.ly and completed its subsequent merger with TikTok successfully. However, two years after the acquisition, when TikTok became the U.S.' most downloaded application and tangled up with a variety of national security concerns, CFIUS launched its investigation into the acquisition. While the CFIUS process was advancing, the Trump Administration also started to take other action. On July 22, 2020, the House voted to bar federal employees from downloading TikTok on government-issued devices. President Trump then announced his intention to ban TikTok, expressing that he could use an executive order or emergency economic powers, and also prepared to require ByteDance to divest its ownership in TikTok.

Though only vague explanations were given by the president at first, the administration further relied on the CFIUS result as justification to announce that TikTok would be banned if it was not sold to U.S. buyers by September 15, 2020, and President officially signed the "Executive Order on Addressing the Threat Posed by TikTok" and "Order Regarding the Acquisition of Musical.ly by ByteDance Ltd." Potential buyers including Microsoft,

[169] Jackson, *supra* note 80, at 39.
[170] *See infra* Part I.A.
[171] Sitaraman, *supra* note 27, at 1145–1146.
[172] See Manyika and Roxburgh, *supra* note 39, at 1; Seiler, *supra* note 7, at 54.
[173] Jackson, *supra* note 80, at 39.
[174] Eric Schmidt et al., *supra* note 2, at 10.

Walmart and Oracle emerged, among which Oracle's proposal stood out, though Microsoft claimed that it "would have made significant changes to ensure the service met the highest standards for security, privacy, online safety, and combatting disinformation."[175] On September 20, 2020, President Trump approved the transaction between TikTok and Oracle, and at the same time put off the ban until September 27.

Meanwhile, TikTok brought suit against the Trump administration over the forthcoming ban set by the executive order on August 24, 2020, and claimed that the administration did not give it a fair chance to defend against allegations it was a national security risk. In its notice of appeal, TikTok alleged that the executive order violated the International Emergency Economic Powers Act (IEEPA) and the due process protections of the Fifth Amendment. The suit suspended the ban temporarily while the court determined whether the nationwide ban was warranted.

After President Biden took office, he reversed Trump's previous strategies. In February 2021, the Biden Administration paused the TikTok litigation. Later in July, he revoked a series of Trump's executive orders and simultaneously asked the Secretary of Commerce to reconsider the problem in a new Executive Order.[176] It is believed that the new order grants the Secretary of Commerce broad discretion to develop a new framework for regulating foreign tech platforms, which provides the chance to form new policies using the lessons of the three aforementioned paradigms.

B. Latest Attempt: Independent Ban by Executive Order of Different States

Since the end of 2022, a number of States have successively launched executive orders to ban the use of foreign applications in state government technology, which seems to be the latest trend in foreign tech platform regulation.

To be specific, the State of Virginia launched Executive Order #24 in December 2022 to ban the use of TikTok, WeChat, and any other ByteDance or Tencent applications on state government devices and wireless networks.[177] The State of North Carolina and the State of Alaska banned TikTok and WeChat in early January 2023.[178] The latest is Executive Order #184 of the State of Wisconsin, which came on January 13, 2023, banning a list of nine products with Chinese ties.[179] The reasons and the scope of the bans slightly vary from State to State, and seemingly constitute geographic-separated rules but with united spirit. It is not clear yet whether the rest of the States will take similar action, and whether a universal policy will be better than the present rules set by each States independently.

---

[175] Eric Savitz, *Oracle Won the TikTok Bid After Beating Out Microsoft and Walmart*, BARRON'S (2020), https://www.barrons.com/articles/oracle-wins-tiktok-bid-beating-out-microsoft-and-walmart-what-to-know-51600043161 (last visited Jan 27, 2023).

[176] Makena Kelly, *Biden revokes and replaces Trump orders banning TikTok and WeChat*, THE VERGE (2021), https://www.theverge.com/2021/6/9/22525953/biden-tiktok-wechat-trump-bans-revoked-alipay (last visited Jan 27, 2023).

[177] Va. Exec. Order No. 24 (Dec. 16, 2022).

[178] N.C. Exec. Order No. 276 (Jan. 12, 2023); James Brooks, *Alaska follows other states, bans social media app TikTok from state-owned electronics*, ALASKA BEACON (2023), https://alaskabeacon.com/2023/01/06/alaska-follows-other-states-bans-social-media-app-tiktok-from-state-owned-electronics/ (last visited Apr 5, 2023)..

[179] Wis. Exec. Order No. 184 (Jan. 13, 2023).

CONCLUSION

Faced with the uprising of foreign tech platforms, the U.S. is challenged in multiple aspects. While the prevailing foreign applications are favored by the next generation of Americans, the massive data collection poses risk of widespread privacy infringement. While the U.S. always declares itself a champion a totally free internet, the government feels obliged to take regulatory actions in the digital world. While the U.S. asks for non-restrictive entry or operative regulation as its tech giants, such as Google, Facebook, and Microsoft, have frequently invested abroad, it seems to set double standards when the foreign TikTok "invades" its territory. As technology competition gets tougher, more "TikToks" will emerge, and the country is in urgent need for a well-developed regulation policy. The laissez faire approach, the case-by-case restrictive approach, and the platform-utilities approach all serve as inspiration for a future viable policy. This article has not, and does not intend to, choose a "best plan." Instead, this article aims to objectively review all the advantages and drawbacks of each theory and thus provides the policymaker with an all-around view to reflect on the factors to be considered at hand. Presently, the crucial problem is how to strike a balance between national security and internet freedom. Whether by further refining the CFIUS and case-by-case reviewing process, or launching sectoral policies based on geographic separation or other criteria alike, the purpose is always the same: to find a scheme that not only well protects the nation's core interests but also withstands the legitimacy examination from home and abroad.