Hastings Communications and Entertainment Law Journal

Volume 44
Number 2 *Spring 2022*

Article 3

Spring 2022

Digital Wild West: Foreign Social Media Bans, Data Privacy, and Free Speech

Tiange (Tim) Chen

Digital Wild West: Foreign Social Media Bans, Data Privacy, and Free Speech

TIANGE (TIM) CHEN*

* Tiange (Tim) Chen is an Associate of Robinson & Cole LLP, where he practices corporate and securities law at the firm's New York Office. Tim received his J.D. degree with honors from The George Washington University Law School where he was a recipient of the Pamela Spanogle International Commercial Arbitration Competition Award and Pro Bono Service Award. Before law school, he worked as a business development assistant at a major international law firm's China Practice. He would like to thank Professor Dawn C. Nunziato for her valuable inputs and guidance for the paper.

TABLE OF CONTENTS

I. INTRODUCTION 165
II. MAJOR NATIONAL SECURITY REGIMES & RECENT CHANGES 166
A. Access to Technologies 167
B. Access to Data 170
C. Executive Order 13873 172
D. *TikTok* and *WeChat* Litigations 173
III. *WECHAT*, THE FIRST AMENDMENT AND NATIONAL SECURITY 175
A. *WeChat I* 176
B. *WeChat II* 177
C. Broader Implications 178
1. Cyber Exploitation 179
2. Economic Security 182
IV. *TIKTOK*, IEEPA AND EXECUTIVE AUTHORITY 183
A. *TikTok* 183
B. *Marland* 184
C. Broader Implications 184
V. AFTERMATH 185
VI. A TUMULTUOUS PAST AND A TROUBLED FUTURE 186
A. Patchwork of government regulators and policies 188
B. Contradictory Towards First Amendment Value 189
C. Losing Credibility 190
D. Moving Beyond The Past 192

I. INTRODUCTION

In June 2020, a group of Korean pop music ("K-Pop") fans mobilized on TikTok, a popular social media platform for sharing short videos, and pranked former President Donald Trump's campaign by reserving tickets en masse for his rally in Tulsa, Oklahoma without showing up.[1] A week later, only 6,000 people showed up in the 19,000-seat stadium used by the campaign.[2] Two months later in August, Trump issued an executive order, directing the Commerce Department to ban TikTok in the United States ("TikTok Ban").[3]

While federal officials cited national security risks as the reason for issuing the order,[4] few gave credence to the justifications. Some suggested that the former President wanted to force TikTok's Chinese parent to sell the popular platform to an American company;[5] others cited it as another example of his political war against China;[6] a few of TikTok stars even suggested that the ban was a revenge for their pranks and trolls of Trump on the platform.[7]

Notwithstanding the justifications, the TikTok ban was blocked by federal courts in late September 2020 and rescinded by the Biden Administration in June 2021.[8] A similar ban on the Chinese social media platform WeChat ("WeChat ban") announced in conjunction with the TikTok ban was also blocked by a federal court in September 2020 and rescinded in June 2021.[9] Despite the legal setbacks and regime change, the social media bans, associated executive actions and court decisions have wide-ranging implications beyond TikTok and WeChat.

---

1. *See* Barbara Ortutay, *Did TikTok Teens, K-Pop Fans Punk Trump's Comeback Rally?*, AP NEWS (June 21, 2020), https://apnews.com/article/2f18f18a8b40a4635fd3590fd159241c.

2. *See id*.

3. *See* Exec. Order No. 13,943, 85 Fed. Reg. 48641 (Aug. 6, 2020) [hereinafter WeChat Order]; Exec. Order No. 13,942, 85 Fed. Reg. 48637 (Aug. 6, 2020) [hereinafter TikTok Order].

4. *See, e.g.*, Charles Creitz, *Pompeo Warns of Potential Restriction of Chinese TikTok App; US Users May Be Ceding Info to 'Chinese Communists'*, FOX NEWS (July 6, 2020), https://www.foxnews.com/media/mike-pompeo-tik-tok-china-communist-social-media-spying-fox-ingraham.

5. *See* Abram Brown, *Is This the Real Reason Why Trump Wants To Ban TikTok?*, FORBES (Aug. 1, 2020), https://www.forbes.com/sites/abrambrown/2020/08/01/is-this-the-real-reason-why-trump-wants-to-ban-tiktok/?sh=10ff128b4aed; Alex Wilhelm, *Trump Calls TikTok a Hot Brand, Demands a Chunk of Its Sale Price*, TECHCRUNCH (Aug. 3, 2020), https://techcrunch.com/2020/08/03/trump-calls-tiktok-a-hot-brand-demands-a-chunk-of-its-sale-price/.

6. *See* Brett Goodin, *Banning TikTok and Stoking Sinophobia Isn't Likely to Get Trump Re-Elected*, WASH. POST (Aug. 10, 2020), https://www.washingtonpost.com/outlook/2020/08/10/banning-tiktok-stoking-sinophobia-isnt-likely-reelect-trump/.

7. *See President Trump – TikTok Trolls Say He Want Revenge … Mad About Pranks!!!*, TMZ (Aug. 6, 2020), https://www.tmz.com/2020/08/06/donald-trump-tiktok-ban-trolls-take-responsibility-tulsa-pranks-china/.

8. *See infra* Part II(4).

9. *See id*.

Against the backdrops of a series of actions taken by the Trump Administration to curb foreign access to the U.S. internet, communication and telecommunication sectors (internet sector), citing national security threats posed by foreign adversaries like China, Russia, Iran and others,[10] the TikTok and WeChat bans highlighted the emerging role economic security issue plays in the broader national security debate, crystalized the breath and limit of the Executive Branch's policymaking authorities at the intersection of national security and digital economy, and provided meaningful lessons for policymakers and industry players alike as they adapt to the ever-changing landscape of cybersecurity threats.

This paper surveys new trends on the broader national security policy changes on foreign-owned Telecommunication, Media and Technology ("TMT") companies, platforms, applications and contents, and explore how the court decisions and administrative actions surrounding the TikTok and WeChat bans would shape future government actions in this area.[11]

II. MAJOR NATIONAL SECURITY REGIMES & RECENT CHANGES

Because of development of digital convergence, regulations over foreign access to the U.S. TMT sector have undergone significant changes over the past few decades, including increasing overlaps between regulations over corporate entities, hardwares, content and platforms.[12] Traditionally, foreign entities that operate in the U.S. market face many regulations, including market access limits (such as FCC licensing requirements).[13] However, as cutting-edge technologies, such as artificial intelligence and cloud computing, are increasingly used by industrial players in this sector, these entities start to also face headwinds from government regulations over technology concerns. The increased awareness and recognition of privacy as a national security concern also brings regulations over access to U.S. user data into the forefront of regulators' minds in this sector, with special emphasis in investment and market access limit.[14]

10. *See, e.g.*, Tim Starks, *Russia, China and Iran Trying to Hack Presidential Race, Microsoft says*, POLITICO (Sept. 10, 2020), https://www.politico.com/news/2020/09/10/russia-china-iran-cyberhack-2020-election-411853; OFF. OF DIR. OF NAT'L INTEL., ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY 8-14 (2021).

11. These government restrictions on foreign social media companies, platforms, applications and contents tend to focus on two sides of the issues: foreign access to US data and technologies, and US user access to foreign platforms. However, as government restrictions are primarily executed in the forms of market access restrictions and investment limits, the practical impact of these restrictions on the two sides of the issues are almost the same—limiting or eliminating U.S. user access to foreign-managed platforms and content inside the United States.

12. *See* Natalie Klym & David D. Clark, *The Impact of Application Convergence on Regulation: The Case of Social Media*, SSRN (Mar. 16, 2018).

13. *See, e.g.*, Rules and Policies on Foreign Participation in the U.S. Telecommunications Market, 62 Fed. Reg. 64741 (Dec. 9, 1997) (to be codified at 47 C.F.R. pts. 43, 63, 64).

14. *See* 50 U.S.C. § 4565 (2021).

A. ACCESS TO TECHNOLOGIES

Foreign persons are limited in their ability to acquire, use, or develop technologies with U.S. content by national security and foreign policy concerns. Export control, economic sanctions, and foreign investment review laws and regulations restricts the transfer of technologies between foreign persons and U.S. persons. Because of the close nexus between TMT platforms and emerging technologies, such as AI, machine learning and clout computing, recent regulatory reforms have significant potential implications.

Import-export regulations play a major role in limiting foreign access to U.S. technologies. The Constitution does not provide a right of export for individuals and businesses.[15] As such, the Federal Government has broad power in regulating transports of goods and services. The U.S. export control regimes are primary comprised of the Export Administration Regulations (EAR), [16] concerning export of goods that can be used for both military and civil purposes, the International Traffic in Arms Regulations (ITAR),[17] concerning with export of military and defense equipment, and Office of Foreign Asset Control (OFAC) regulations,[18] concerning financial and trade embargoes and sanctions.

Traditionally, export control regulations have narrow speech implications in the First Amendment context, except in the rare cases of export of technical data or technical assistance under ITAR, and export of software and source codes under EAR.[19] Besides, export control legislations and regulations provide for carve-outs for First Amendment activities, including public domain exceptions and exemptions for core First Amendment activities, such as academic research and education activities.[20] However, in 2018, 30 years after the original authorizing legislation was passed and 17 years after the statutory authority for the export control system

15. *See* U.S. CONST. art. I, § 10, cl. 2.

16. *See* 15 C.F.R. §§ 730–74 (2021).

17. *See* 22 C.F.R. §§ 120–30 (2021).

18. *See* 31 C.F.R. §§ 501–98 (2021).

19. *See* BUREAU OF INDUS. & SEC., U.S. DEP'T OF COM., ENCRYPTION AND EXPORT ADMINISTRATION REGULATIONS (EAR) (2021).

20. Export control regulations have not been without First Amendment challenges. *See* Bernstein v. U.S. Dep't of Just., 176 F.3d 1132 (9th Cir. 1999), *rehearing granted and opinion withdrawn*, 192 F.3d 1308 (9th Cir. 1999) (en banc) (challenging EAR regulating software); United States v. Edler Indus., Inc., 579 F.2d 516 (9th Cir. 1978) (challenging ITAR regulating technical assistance). Statutory and regulatory provisions do provide some carve-outs due to First Amendment concerns. *See, e.g.*, 15 C.F.R. §§ 734.2, 734.4(b)(1)(i), 734.7. However, the outdated languages in the public domain exceptions may not be able to meet the evolving landscape of First Amendment activities, or could have chilling effects if applied in some contexts of export and trade enforcement actions. *See* International Traffic in Arms: Revisions to Definitions of Defense Services, 80 Fed. Reg. 31525, 31527 (proposed June 3, 2015) (to be codified at 22 C.F.R. pt. 120, 123, 125, 127); Doron Hindin et al., *The Role of Export Controls in Regulating Dual Use Research of Concern: Striking a Balance between Freedom of Fundamental Research and National Security*, 2017 NAT'L ACADS. PRESS 17 (2017).

lapsed for the third time,[21] Congress enacted the Export Control Reform Act (ECRA) to reauthorize the EAR and expand the purview of the EAR to cover emerging and foundational technologies.[22] This expansion expands the scope of the EAR and requires the Commerce Department to regularly update technologies subject to export control, [23] including in response to national security threats in the internet sector.[24] The ECRA also made it explicit that it cannot be used to directly or indirectly regulate personal communication, an exception it incorporated form the International Economic Emergency Powers Act (IEEPA).[25]

Both the Trump and Biden Administrations have been slow in enacting regulations to expand the scope of the EAR as authorized by Section 1758 of the ECRA, given the shifting and complex nature of defining the regulatory scope and providing the right level of limit on accessing these intangible goods and services.[26]

In addition to the *explicit* regulation of software under export control measures,[27] which is a regulation of speech,[28] the terms of emerging technologies encompass a variety of identified technologies used for personal communications, including AI cloud technologies, Position, Navigation, and Timing (PNT) technologies, and speech and audio

21. *See* CHRISTOPHER A. CASEY ET AL., CONG. RSCH. SERV., THE INTERNATIONAL EMERGENCY ECONOMIC POWERS ACT: ORIGINS, EVOLUTION, AND USE 47 (2020).

22. *See* Export Control Reform Act of 2018, Pub. L. No. 115-232, 132 Stat. 1636, 2208 (2018) (codified as amended at 50 U.S.C. §§ 4801-4852) [hereinafter "ECRA"]. ECRA closed a long-standing gap identified by many national security observers—that the U.S. export control system does not direct regulate technology or the transfer of know-how. *See* U.S. CONG. OFF. OF TECH. ASSESSMENT, SCIENCE, TECHNOLOGY, AND THE FIRST AMENDMENT 49 (1988) (citing *the Bucy Report* to find that "the knowledge most vital to protect is not embedded in military weaponry per se, but knowledge that conveys design and manufacturing know-how"); *see also* Scott Jones, *Disrupting Export Controls: "Emerging and Foundational Technologies" and Next Generation Controls*, 6 STRATEGIC TRADE REV. 31, 36 (2020) (arguing that ECRA reflects a shifted approach identified and recommended in the *Bucy Report*).

23. *See* Scott A. Jones, *Trading Emerging Technologies: Export Controls Meet Reality*, 31 SEC. & HUMAN RTS. (SPECIAL ISSUE) 47 (2020).

24. *See* Jeffrey Richardson, *Is Your Software Transmission Subject to U.S. Export Controls under the EAR?*, MILLER CANFIELD (May 3, 2013), https://www.millercanfield.com/resources-alerts-845.html.

25. *See* ECRA, *supra* note 22, at § 1754.

26. Some limited regulations have been published. For example, under the emerging technology rules, many provisions touch on issues related to the First Amendment. For example, in Category 3, "software" related to EUV-Lithography has been classified for control, as well as "software" related to surveillance in Category 5; in Category 2, 3D printing machines have been added. However, the government has not acted on foundational technologies. *See* Implementation of Certain New Controls on Emerging Technologies, 85 Fed. Reg. 62583 (Oct. 5, 2020) (to be codified at 15 C.F.R. pts. 740, 772, 774); U.S. DEP'T OF COM., SECRETARY ROSS HIGHLIGHTS COMMERCE ACTIONS SUPPORTING STRATEGY FOR CRITICAL AND EMERGING TECHNOLOGIES (2020); Identification and Review of Controls for Certain Foundational Technologies, 85 Fed. Reg. 52934 (proposed Aug. 27, 2020) (to be codified at 15 C.F.R. at pts. 742, 774).

27. *See* 31 C.F.R. §§ 501–98 (2021).

28. *See, e.g.*, Bernstein v. U.S. Dep't of Just., 176 F.3d 1132, 1140–41 (9th Cir. 1999), *rehearing granted and opinion withdrawn*, 192 F.3d 1308 (9th Cir. 1999); Universal City Studios, Inc. v. Corley, 273 F.3d 429, 445–46 (2d Cir. 2001).

processing technologies, which have been considered to be regulated under the emerging technology rules.[29] A variety of TMT companies can be subject to export control for its use of emerging and foundational technologies.[30] For example, some have called for ByteDance, TikTok's Chinese parent company, to be added to the "entity list", which would essentially ban any US companies from transacting with ByteDance or TikTok.[31] Practical consequences would include delisting the app from Android and Apple app stores, or prohibiting US users to access to app in certain networks.[32] A TMT company under an export control ban, as in the case of mobile device producer Huawei, who is forced to sell its entire mobile device business,[33] can have devastating impact its livelihood.[34]

Alternatively, the foreign investment review regime, the Committee on Foreign Investment in the United States (CFIUS), also provides broad authority for the Federal Government to review transactions by foreign corporations to acquire U.S. assets and businesses involving sensitive personal data,[35] critical infrastructure (including telecommunication networks),[36] and critical technologies (including emerging and foundational

29. *See* Review of Controls for Certain Emerging Technologies, 83 Fed. Reg. 58201 (Nov. 19, 2018) (to be codified at 15 C.F.R. pt. 744).

30. *Cf.* Natasha Moore & Brian Mich, *Export Controls Become New Stick in US-China Tech Race*, FORBES (Dec. 15, 2020), https://www.forbes.com/sites/riskmap/2020/12/15/export-controls-become-new-stick-in-us-china-tech-race/?sh=ffe8341669a0.

31. *See* Adi Robertson, *How the Trump Administration Could "Ban" TikTok*, THE VERGE (Aug. 1, 2020), https://www.theverge.com/2020/7/9/21315983/trump-pompeo-ban-tiktok-bytedance-chinese-social-media-national-security-censorship-methods.

32. New smartphones produced by Huawei, a Chinese company added to the entity list, were unable to install Android operating system or update such system, absent exemptions provided by the Commerce Department. *See id.* As for the blocking of use of an application in a WiFi network, the University of Kansas blocked using of WeChat on its school-provided WiFi network, after the WeChat ban was announced. *See* Blake Ullmann & Nicole Dolan, *KU-owned Computers, Campus Wi-Fi Will Ban Use of WeChat*, THE UNIV. DAILY KANSAN (Sept. 15, 2020), https://www.kansan.com/news/ku-owned-computers-campus-wi-fi-will-ban-use-of-wechat/article_0d3326b8-f76b-11ea-bd4c-dbb1fe3ba1be.html.

33. *See* Julie Zhu, *Exclusive: Huawei to Sell Phone Unit for $15 Billion to Shenzhen Government, Digital China, Others - Sources*, REUTERS (Nov. 9, 2020, 9:05 PM), https://www.reuters.com/article/huawei-m-a-digital-china-exclusive/exclusive-huawei-to-sell-phone-unit-for-15-billion-to-shenzhen-government-digital-china-others-sources-idUSKBN27Q0HJ.

34. Therefore, it is not surprising that the key AI algorithms, which powered TikTok towards its success, was a main sticking point for the CFIUS negotiation. *See* Zoe Schiffer, *The Big Questions Behind TikTok's Looming National Security Investigation*, THE VERGE (Nov. 7, 2019, 3:26 PM), https://www.theverge.com/2019/11/7/20948613/tiktok-national-security-investigation-cfius-china-bytedance-hawley-rubio. The interesting issue, though, is that while TikTok's Chinese parent, ByteDance, owns the algorithms, its success in many sense was attributed towards its original acquisition of China-headquarter, U.S.-based Music.ly. *See id.*

35. *See* 50 U.S.C. § 4565(a)(4)(B)(iii)(III) (2018).

36. *See id.* § 4565(a)(4)(B)(iii)(I); *see also* PROSKAUER ROSE LLP, *CFIUS Proposed Rules Target Critical Technology, Sensitive Personal Data & Real Estate* (Oct. 4, 2019), https://www.proskauer.com/alert/cfius-proposed-rules-target-critical-technology-sensitive-personal-data-and-real-estate.

technologies).[37] In 2018, Congress specifically passed the Foreign Investment Risk Review Modernization Act (FIRRMA) to broaden the scope of the review regime,[38] including mandating the review of transactions involving emerging and foundational technologies, as defined under ECRA,[39] and involving sensitive personal data.[40] CFIUS may approve transactions, enter into and enforce mitigation agreements, or recommend to the President to block transactions, based on its review of the national security implications of the transaction, without judicial review.[41]

B. ACCESS TO DATA

Foreign persons are also somewhat limited in their ability to acquire, store, transfer and monetize personal data of U.S. persons. Measured by many standards, U.S. lacks robust data security and privacy laws and regulations, and existing laws and regulations are not often attached with national security or foreign policy considerations.[42] However, recent laws in foreign investment review as well as regulatory actions taken in the telecommunication sector, from which the TikTok and WeChat bans arise, signal significant change in the Federal Government's approach with regard to privacy as a national security concern.

First, as provided before in this article, CFIUS is specifically authorized under FIRRMA to review transactions that allow foreign access to "sensitive personal data of United States citizens that may be exploited in a manner that threatens national security."[43] In this context, CFIUS has blocked one transaction involving a Chinese company's attempted acquisition of a U.S. company that develops and operates hotel booking and management software, citing privacy concerns.[44] But its most landmark decision arises from forcing a Chinese private gaming company to divest ownership stake from Grindr, the U.S.-based social media app popular in the LGBTQ

37. *See* 50 U.S.C. § 4565(a)(6)(A)(vi) (2018) (incorporating Section 1758 of the ECRA).

38. *See* Foreign Investment Risk Review Modernization Act of 2018, Pub. L. No. 115-232, 132 Stat. 1636, 2174 (2018).

39. *See* 50 U.S.C. § 4565(a)(6)(A)(vi) (2018).

40. *See id.* § 4565(a)(4)(B)(iii)(III).

41. *See id.* § 4565(i).

42. *See* Robert D. Williams, *To Enhance Data Security, Federal Privacy Legislation Is Just a Start*, THE BROOKINGS INST. (Dec. 1, 2020), https://www.brookings.edu/techstream/to-enhance-data-security-federal-privacy-legislation-is-just-a-start/.

43. *See* 50 U.S.C. § 4565(a)(4)(B)(iii)(III) (2018); *see also* Austin Mooney, *Spotlight on Sensitive Personal Data as Foreign Investment Rules Take Force*, MCDERMOTT WILL & EMERY LLP (Feb. 18, 2020), https://www.mwe.com/insights/spotlight-on-sensitive-personal-data-as-foreign-investment-rules-take-force/.

44. *See* Order of Mar. 6, 2020 Regarding the Acquisition of StayNTouch, Inc. by Beijing Shiji Information Technology Co., Ltd., 85 Fed. Reg. 13719 (Mar. 10, 2020).

communities,[45] was the first reported CFIUS-blocked transaction in the TMT sector.

In the telecommunication sector, the Federal Communication Commission begins to play a more assertive role in national security arena as well. First, it exercises broad licensing and transaction review authority with regard to foreign telecommunication and communication providers. The most famous example includes its blocking of China Telecom, a Chinese state-owned telecommunication provider, from renewing its license to operate in the United States.[46] It also rejected an application from China Mobile, another Chinese state-owned telecommunication provider, to operate mobile networking services in the United States.[47] Second, it has also forced major telecommunication providers to move away from Huawei, a major communication network service provider in the Midwest and a leading 5G hardware provider in the world.[48] Under its newly acquired authority under a 2019 law, the FCC may designate foreign companies who pose national security threats to the U.S. communication networks, and may bar U.S. companies from tapping an $8.3 billion government fund to purchase equipment from the designated companies.[49] Five Chinese companies, including Huawei, have been added to the designation list.[50] Last but not the least, the FCC has formalized its Team Telecom regime to review national security related threats in the telecommunication sectors,[51] with a review and approval process akin to the CFIUS process but limited to the telecommunication sector.[52]

However, despite these significant actions, one of the most consequential executive actions was former President Trump's Executive

45. *See* Yuan Yang & James Fontanella-Khan, *Grindr Sold by Chinese Owner After US National Security Concerns*, THE FIN. TIMES (Mar. 7, 2020), https://www.ft.com/content/a32a740a-5fb3-11ea-8033-fa40a0d65a98.

46. *See* Matt Keeley, *FCC Should Ban China Telecom Over National Security Risks, Justice Department-Led Review Says*, NEWSWEEK (Apr. 10, 2020, 12:48 AM), https://www.newsweek.com/fcc-should-ban-china-telecom-over-national-security-risks-justice-department-led-review-says-1497222.

47. *See* China Mobile Int'l (USA) Inc., 34 FCC Rcd. 3361 (2019).

48. *See* Cecilia Kang, *Huawei Ban Threatens Wireless Service in Rural Areas*, N.Y. TIMES (May 25, 2019), https://www.nytimes.com/2019/05/25/technology/huawei-rural-wireless-service.html.

49. *See* Daniel Shepardson, *Five Chinese Companies Pose Threat to U.S. National Security: FCC*, REUTERS (Mar. 12, 2021, 10:13 AM), https://www.reuters.com/article/us-usa-china-tech/five-chinese-companies-pose-threat-to-u-s-national-security-fcc-idUSKBN2B42DW; *see also* FED. COMMC'N. COMM'N, FCC Publishes List of Communications Equipment and Services That Pose a Threat to National Security (Mar. 12, 2021), https://docs.fcc.gov/public/attachments/DOC-370755A1.pdf (citing Secure and Trusted Communications Networks Act of 2019).

50. *See* Shepardson, *supra* note 49. The FCC has also created a reimbursement program for U.S. companies to receive federal funding to switch from Chinese technologies and equipment to other those provided by other vendors. *See id.*

51. *See* Farhad Jalinous et al., *FCC Adopts New Rules and Procedures for Team Telecom Committee*, WHITE & CASE LLP (Oct. 21, 2020), https://www.whitecase.com/publications/alert/fcc-adopts-new-rules-and-procedures-team-telecom-committee.

52. *See* Brian D. Weimer et al., *Formalizing Team Telecom*, THE NAT'L L. REV. (Oct. 20, 2020), https://www.natlawreview.com/article/formalizing-team-telecom.

Order 13873 ("ICT Supply Chain EO" or "EO"), which created an independent, CFIUS-like review process in the TMT sector.

C. EXECUTIVE ORDER 13873

In May 2019, President Trump announced in the EO a one-year national emergency under IEEPA, and authorized the Commerce Secretary to promulgate rules, evaluate, make preliminary determinations, afford parties opportunities to respond, and make final determinations, to prohibit, unwind or mitigate a transaction involving Information and Communication Technologies ("ICTs"), including hardware and software "primarily intended to fulfill or enable function of information or data processing, storage, retrieval, or communications by electronic means",[53] if the transaction involves ICTs "designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary."[54] "Transactions" were defined to include "any acquisition, importation, transfer, installation, dealing in or use of" ICTs[55], which is broader than the definition of "transaction" in the CFIUS context.[56] Under the EO, any foreign country or entity can be designated as a foreign adversary.[57] In evaluating the proper remedy, the Secretary is entrusted to engage in a three-factor analysis under Section 1(a)(ii).[58]

The EO has been invoked three times thereafter. First, it was cited as the authority for the President to instruct the Commerce Secretary to block TikTok and WeChat from the U.S. market.[59] Second, in January 2021, the Commerce Department proposed an interim final rule ("ICT Rule") to enforce the EO, which called for the authority to review any transaction involving ICTs, including desktop, mobile, gaming and web-based software used by more than 1 million U.S. persons within a 12 month period.[60] Third, the Commerce Department under the Biden Administration issued various subpoena to Chinese companies to investigate alleged unfair practices under the EO.[61]

53. *See* Exec. Order No. 13,873, 84 Fed. Reg. 22,689, 22,691 (May 17, 2019); Securing the Information and Communications Technology, 84 Fed. Reg. 65,316, 65,320 (proposed Nov. 27, 2019) (to be codified at 15 C.F.R. pt. 7).

54. *See* Exec. Order No. 13,873, 84 Fed. Reg. at 22,690.

55. *See id.* at 22,689.

56. *See* 50 U.S.C. § 4565(a)(4)(B) (2018).

57. *See* Exec. Order No. 13,873, 84 Fed. Reg. at 22,691.

58. *See id.* at 22,690.

59. *See infra* Part II(4).

60. *See* Securing the Information and Communications Technology and Services Supply Chain, 86 Fed. Reg. 4909, 4912 (Jan. 19, 2021) (to be codified at 15 C.F.R. pt. 7) (interim final rule).

61. *See U.S. Subpoenas Chinese Communications Firms in Probe of National Security Risks* REUTERS (Mar. 17, 2021), https://www.reuters.com/article/us-usa-china-commerce-idUSKBN2B92OH.

Although the TikTok and WeChat bans have been blocked by courts and rescinded by the Biden Administration,[62] the national emergency has been extended by both administrations since 2019, and the Commerce Department has finalized the ICT Rule in 2021.

D. *TIKTOK* AND *WECHAT* LITIGATIONS

In May 2020, the President extended the national emergency declared under the ICT Supply Chain EO for one more year.[63] Three months later, the President issued a pair of new Executive Orders ("blocking orders") directing the Commerce Secretary to block transactions involving WeChat, the messaging app owned by private Chinese company Tencent, and TikTok, the video sharing app owned by private Chinese company ByteDance.[64] The blocking orders cite to authority granted to the Secretary under the EO as well as delegated authority granted to the President in times of national economic emergency under IEEPA.[65]

Under the WeChat blocking order, WeChat "threatens to allow the Chinese Communist Party access to Americans' personal and proprietary information" and "captures the personal and proprietary information of Chinese nationals visiting the United States, thereby allowing the Chinese Communist Party a mechanism for keeping tabs on Chinese citizens who may be enjoying the benefits of a free society for the first time in their lives."[66] The Secretary therefore was authorized pursuant to the delegated authority under IEEPA and the ICT Supply Chain EO to identify and block "any transaction that is related to WeChat by any person" or related to Tencent or its identified subsidiaries beginning on the 45 days after the issue date of the blocking order.[67] Under the blocking order, any evasive transactions and conspiracies formed to violate the order would also be blocked.[68] The blocking order made clear that it applies to any persons and entities subject to the jurisdiction of the United States.[69] On the same day, another order blocking TikTok was issued with similar rationale and delegation of authorities.[70]

On September 17, 2020, the Commerce Department issued the list of prohibited transactions against WeChat, including provision for download or

62. *See infra* Part II(4).

63. Continuation of the National Emergency with Respect to Securing the Information and Communications Technology and Services Supply Chain, 85 Fed. Reg. 29321 (May 13, 2020).

64. Exec. Order Banning WeChat From the U.S., 85 Fed. Reg. 48641 (Aug. 6, 2020); Exec. Order Banning TikTok From the U.S., 85 Fed. Reg. 48637 (Aug. 6, 2020).

65. Exec. Order Banning WeChat From the U.S.,85 Fed. Reg. at 48642; Exec. Order Banning TikTok From U.S., 85 Fed. Reg. at 48637.

66. Exec. Order Banning WeChat From the U.S.,85 Fed. Reg. 48641.

67. *Id.*

68. *Id.*at 48642.

69. *Id.*

70. *See* Exec. Order Banning TikTok from the U.S., 85 Fed. Reg. 48637.

update in app store, providing internet hosting, content delivery, internet transit or peering services for the app, use of the app for financial transaction, use of the app in functioning of other software or apps.[71] The prohibited transactions would be effectively on September 20. On September 24, the Department announced an almost identical list of prohibitions for TikTok, although it does not include a financial transaction ban because of the lack of a e-payment function on TikTok.[72] The delisting requirement would become effective on September 27, and the remaining provisions would become effective on November 12.[73]

On August 21, a groups of WeChat users sued the Government before the U.S. District Court in the North District of California, alleging Administrative Procedures Act (APA), IEEPA, First Amendment and Fifth Amendment challenges and asking for injunctive relief ("*WeChat* case").[74] The district court took two days to review the Commerce Department list and entered a preliminary injunction about 15 hours before the ban was supposed to become effective, rejecting other challenges but finding that the ban was violating the First Amendment against prior restraint, or was a overbroad time, place, manner (TPM) restriction.[75]

On September 18, TikTok and ByteDance filed suit in the District of Columbia, similarly asserting APA, First Amendment and Fifth Amendment challenges ("*TikTok* case").[76] On the same day, a group of three TikTok influencers filed suit in the Eastern District of Pennsylvania with similar statutory and constitutional challenges ("*Marland* case").[77] On September 27, a D.C. federal judge granted a preliminary injunction on the delisting requirement for TikTok, finding the government acted *ultra vire* under the APA and IEEPA's personal communication exception.[78] On October 30, the District Court in Philadelphia granted another injunction on all transactions for the influencers, similarly finding that the government action was *ultra*

71. U.S. DEP'T OF COM., Identification of Prohibited Transactions to Implement Executive Order 13943 and Address the Threat Posed by WeChat, 15 CFR Ch. 7 (Sept. 17, 2020) (updated on Sept. 21, 2020) (notice was withdrawn from Federal Register after court order precluding the notice from going into effect).

72. *See* U.S. DEP'T OF COM., Notice of E.D. Pa. Preliminary Injunction on the Identification of Prohibited Transactions with TikTok, 15 CFR Ch. 7 (Nov. 9, 2020); *see also* Identification of Prohibited Transactions with TikTok, 85 Fed. Reg. 60061 (Sept. 24, 2020) (enjoined by court from going into effect).

73. Exec. Order Banning WeChat From the U.S., 85 Fed. Reg. 48641 (Aug. 6, 2020).

74. Complaint for Declaratory and Injunctive Relief at 4-6, U.S. WeChat Users All. v. Trump, 488 F. Supp. 3d 912 (N.D. Cal. 2020).

75. *See* Motion for Preliminary Injunction, *WeChat*, 488 F. Supp. 3d 912 (N.D. Cal. Sept. 19, 2020).

76. Complaint for Declaratory and Injunctive Relief, TikTok Inc. v. Trump, 490 F. Supp. 3d 73 (D.D.C. Sept. 18, 2020).

77. Complaint for Declaratory and Injunctive Relief at 1-3, Marland v. Trump, 108 Fed. R. Serv. 3d 283 (E.D. Pa. 2020).

78. *See* TikTok v. Trump, 490 F. Supp.3d 73, 85-86 (D.D.C. Sept. 27, 2020).

vire.[79] And on December 7, the same D.C. District judge blocked the remaining transactions again in the suit brought forth by TikTok.[80]

At the waning days of the Trump Administration, the Government appealed all three injunctions.[81] The Ninth Circuit and the D.C. Circuit held oral arguments, but no appellate decision was issued.[82] Both appellate courts sounded skeptical of the Government's arguments,[83] and the Ninth Circuit denied to stay the injunction issued by the lower court.[84] With the Biden Administration's decision to rescind both bans, all court proceedings were later dismissed.[85]

III. *WECHAT*, THE FIRST AMENDMENT AND NATIONAL SECURITY

The immediate impact of the *WeChat* litigation is different from the two decisions in *TikTok* and *Marland*, because *WeChat* was decided on First Amendment grounds, while *TikTok* and *Marland* were decided on narrower statutory grounds under IEEPA and APA. This section will discuss *WeChat* first, as the district court in that case directly weighed the Government's proffered national security concerns. The section will conclude with a broader discussion on the Government's approach in initiating the bans and in contesting these set of litigations.

In *WeChat*, while the district court did not reject the proffered reasoning of national security interests, it held, in the decision granting the injunction ("*WeChat I*"), that the speech interests are simply too significant, that there were no alternative channels of speech, and that the government's ban was simply too overbroad to succumb those speech interests to the government ban.[86] Additionally, the court later in a motion to stay the injunction ("*WeChat II*") examined the alternative government actions the Commerce Department considered, and concluded that the government failed to advance a narrowly tailored TPM regulation.[87]

79. Marland v. Trump, 498 F. Supp. 3d 624, 625 (E.D. Pa. Oct. 20, 2020).

80. *See* TikTok v. Trump, 507 F. Supp 3d 92, 92 (D.D.C. Dec. 7, 2020).

81. *See* Notice of Appeal, U.S. WeChat All. v. Trump, No. 20-16908 (9th Cir. 2020); Notice of Appeal, Marland v. Trump, No. 20-3322 (3d Cir. 2020); Notice of Appeal, TikTok v. Trump, No. 20-05302 (D.C. Cir. 2020).

82. *See* Notice of Appeal, *WeChat*, No. 20-16908 (9th Cir. 2020); Notice of Appeal, *TikTok*, No. 20-05302 (D.C. Cir. 2020).

83. *See* Edvard Petterson, *WeChat Ban Urged by U.S. Gets Skeptical Review by Appellate Court*, BLOOMBERG (Jan. 14, 2021), https://www.bloomberg.com/news/articles/2021-01-14/wechat-ban-urged-by-u-s-gets-skeptical-review-by-appeals-court; *D.C. Circuit Skeptical of Trump Claims on TikTok Security Risks*, LAW 360 (Dec. 14, 2020), https://www.law360.com/articles/1337489/dc-circ-skeptical-of-trump-claims-on-tiktok-security-risks.

84. Nicholas Iovino, *WeChat Ban Will Stay on Hold, Ninth Circuit Rules*, COURTHOUSE NEWS SERV. (Oct. 26, 2020), https://www.courthousenews.com/wechat-ban-will-stay-on-hold-ninth-circuit-panel-rules/.

85. *See infra* footnote 112.

86. U.S. WeChat All. v. Trump, 488 F. Supp. 3d 912, 927-28 (N.D. Cal. 2020).

87. U.S. WeChat All. v. Trump, 2020 WL 6891820, at *1, *8-9 (N.D. Cal. Nov. 24, 2020).

A. *WECHAT I*

In *WeChat I*, the court, applying jurisprudence on prior restraints and content-neutral restrictions, blocked the government's actions. Specifically, the court granted the preliminary injunction against the WeChat ban based on two defects in the government action: first, the ban amounts to a prior restraint analogous to the ban of signposting in *City of Ladue v. Gilleo* (1994);[88] second, even if the ban is only a TPM restriction, it is too overbroad to survive intermediate scrutiny.[89]

In considering the second issue on content-neutral restrictions (or TPM restrictions), courts must first weigh the significance of the government interests unrelated to the content the speech.[90] Then, it must consider the relatedness between the government interest raised and the measure adopted.[91] Lastly, courts consider on whether the government restriction leaves open adequate alternative channels of communication.[92] Some have framed the narrow tailoring test—in combination of the second and third prongs of the test—as essentially requiring that the government restrictions are "no more burdensome than necessary" to advance the government interests at stake.[93] Courts therefore weigh the government's justification against its own action to see if those government interests would be substantially advanced by the restrictions.

In the blocking order, the government identified several national security risks at issue. It argues that the application allows the Chinese Government to: (1) access Americans' personal and proprietary information, (2) surveil Chinese citizens who are enjoying the benefit of a free society for the first time in their lives in the United States, (3) censor content that it deems politically sensitive, and (4) create disinformation campaigns that benefit itself.[94] In its court filings before the *WeChat I* decision, the government reiterates the same four interests at stake.[95]

However, while *WeChat I* admitted the overarching national security interests at stake and identified risks, it noted that the government "put in

88. City of Laude et al v. Gilleo, 512 U.S. 43, 54-59 (1994).

89. *See WeChat*, 488 F. Supp. 3d at 927.

90. *See* Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989).

91. *Intermediate Scrutiny*, CORNELL LAW SCH., https://www.law.cornell.edu/wex/intermediate_scrutiny (last visited Apr. 6, 2021).

92. *See* Pac. Coast Horseshoeing Sch., Inc. v. Kirchmeyer, 961 F.3d 1062, 1073 n.9 (9th Cir. 2020).

93. *See, e.g.*, Doe v. Prosecutor, Marion County, 705 F.3d 694, 698 (7th Cir. 2013); Joel Alicea & John D. Ohlendorf, *Against the Tiers of Constitutional Scrutiny*, 41 NAT'L AFFS. 72, 72-73 (2019).

94. *See* Addressing the Threat Posed by WeChat, 85 Fed. Reg. 48641 (Aug. 11, 2020).

95. *See* Opp'n to Mot. for Prelim. Inj. at 26, U.S. WeChat Users All. v. Trump, 488 F. Supp. 3d 912 (N.D. Cal. Sep. 19, 2020) (No. 20-cv-05910-LB),ECF No. 22 (the Executive Order was enacted to "prevent [] the Chinese Government from using WeChat to surveil the American people, censor information, sow misinformation, and collect and use 'vast swaths of personal and proprietary information from American users to advance its own interests."); *see also* Opp'n to Renewed Mot. for Prelim. Inj., at 7–8, *WeChat*, 488 F. Supp. 3d 912 (No. 20-cv-05910-LB),ECF No. 51.

scant little evidence" that an effective ban on all U.S. WeChat users would be necessary to address those risks.[96] It also suggested the alternatives, such as barring WeChat from government devices and taking industry best practices on data security, may be sufficient.[97] The court eventually settled on two points to rule against the government: first, the ban restricted more speech than is necessary, and second, the ban did not give substitute channels of communication.[98]

B. *WECHAT II*

In subsequent filings before the *WeChat II* decision, the government furnished a memorandum provided by John K. Costello, Deputy Assistant Secretary for Intelligence and Security, to Secretary Ross, in which he expanded on the national security threats at issue: (1) "[t]he PRC presents a national security, foreign policy, and economic threat to the United States given its long-term effort to conduct espionage against the U.S. government, corporations, and persons", (2) "[t]he CCP exerts influence over private Chinese companies such as Tencent and its employees through direct ties to personnel and corporate 'Party Committees'", (3) "PRC Law Requires that Companies Subject to PRC Jurisdiction, such as Tencent, assist with PRCISS intelligence and surveillance efforts", and (4) "Tencent has complied with and assisted the PRC with its domestic and global monitoring".[99]

After laying out WeChat's vulnerabilities, such as storage of data on Hong Kong servers, potential background roaming, access by law enforcement agencies by request, and weak data protections, the memo predicted several consequences for not restricting the use of WeChat: (1) "Exploitation of WeChat user data imperils the privacy of U.S. citizens, the security of U.S. government personnel, and, at scale, directly threatens the economic security and national security of the United States", (2) "Exploitation of WeChat for censorship or propaganda for U.S.-based users directly threatens U.S. national security by surreptitiously influencing U.S. public opinion to those that align with Chinese government objectives."[100]

The memo went on to suggest that Tecent's proposal to create a separate U.S. version of the app, with U.S.-government approved governance structure, a U.S.-based cloud provider, security measures to protect new source code, and regular audits and approvals over source code and data access, was not enough. It suggested that a "baseline level of trust" in the

96. 488 F. Supp. 3d 912, at 927.

97. *Id.*

98. *Id.* at 928.

99. Notice of Corrected Ex. in Support of Mot. to Stay, Ex. A, *WeChat*, 488 F. Supp. 3d 912 (No. 3:20-cv-05910-LB), ECF. No. 76-1.

100. *Id.*

parent company will be needed for any mitigation plan, but the government cannot trust Tencent to retain ownership interests in the app due to its close relationship with the Chinese government.[101]

In *WeChat II*, the court rejected the government motion to stay, finding that its consideration of the narrowly tailoring prong of the test remained the same. Specifically, the court rejected the government action for its failure to consider alternatives than a total ban, citing two alternatives: first, it cited a measure recommended by the Department of Homeland Security but rejected by the Department of Commerce—to ban WeChat on government devices; second, it suggested that the government could also adopt data security mitigation plans proposed by Tencent and a former Motorola executive (furnished by the plaintiffs) which are consistent with industry best practices.[102]

C. BROADER IMPLICATIONS

The back-and-forth between the government and the court reflects two central themes of arguments.

First, the court characterized the proposed ban as a "ban", but the government treated it a series of actions to reduce WeChat's functionality and data collection that "do not directly prohibit the downloading and use" of the app but "ultimately make [it] less effectively and challenging" to use.[103]

Second, the court engaged in extensive probing of the scope of the ban and the alternative means to achieve the end-goals, but the government hoped for a more deferential court.[104] Indeed, the government briefs repeatedly cited two national security cases, *Haig v. Agee* and *Holder v. Humanitarian Law Project* to suggest that the government's interests are of the highest importance, that the measures are prospective, and that the court should defer to the government's judgment.[105] However, in *WeChat I*, the court seemed to give credit only to the "overarching" national security interests at stake, which it suggests are "certainly" significant, but did not credit the government's specified WeChat-related national security risks. In the related question on alternative means of TPM restrictions, the government also hoped for a deferential court, citing *Trump v. Hawaii* to caution the court not to second guess or substitute its own assessment for that

101. *Id.*

102. *See id.*

103. *Id.*

104. *See* Opp'n to Renewed Mot. for Prelim. Inj. at 7–8, *WeChat*, 488 F. Supp. 3d 912 (No. 20-cv-05910-LB) (ECF No. 51).

105. *id.*; *see also* Opp'n to Mot. for Prelim. Inj. at 26–30, *WeChat*, 488 F. Supp. 3d 912 (No. 20-cv-05910-LB) (ECF No. 22).

of the Executive.[106] However, in both decisions, the court put a stronger emphasis on the burden of evidentiary support on the government's side to show why the proposed ban was not substantially overbroad, and found the government to have failed that in both decisions.

While the court's intrusive probing of the national security justifications might be problematic, and the appellate court might overturn it if given the opportunity,[107] it does show that the measure was a constitutionally novel but dubious and a court might put the government on the spot to show that the mean justifies the end.

To its credit, the government's justifications are consistent throughout the litigation process, where it maintained, generally, that the continued functioning of WeChat in the United States would deprives user privacy and data security, facilitates censorship and surveillance, sows misinformation and propaganda, and assists espionage and intelligence activities. These identified risks generally track the Trump Administration's identified issues in the internet sector, where it focused on three parts of issues: data security and privacy, surveillance and intelligence, disinformation and censorship. However, one particular issue that was not explicitly addressed by the government in the *WeChat* case but was evident in the broader policy debate was the issue of economic security.

1. *Cyber Exploitation*

The Trump Administration has been more active in enacting a national security focused "cyber" policy. Given the raising awareness of the issue after frequent cyberattacks by foreign state and non-state adversaries, against both the government and private entities, a more active government response is urgently needed.[108] Both attacks that predate the Trump Administration, including the hack of the Office of Personnel Management networks, and attacks that happened during the Trump Administration, including the recent SolarWinds hack, continued to show significant gaps in the government's ability to effectively deal with cybersecurity issues.[109]

106. Opp'n to Mot. for Prelim. Inj. at 26–30, *WeChat*, 488 F. Supp. 3d 912 (No. 20-cv-05910-LB) (ECF No. 22).

107. *See* Dorothy Atkins,, *9th Cir. Weighs Nat'l Security, Free Speech in WeChat Appeal*, LAW360 (Jan. 14, 2021), https://www.law360.com/articles/1345133/9th-circ-weighs-nat-l-security-free-speech-in-wechat-appeal. Some members of the Ninth Circuit panel seemed to want to find in favor for the WeChat plaintiffs under IEEPA grounds, but looked skeptical of the district court.

108. *See* Wade H. Atkinson, *A Review of the Trump Administration's National Cyber Strategy: Need for Renewal and Rethinking of the Public-Private Partnership in U.S. National Security Policy*, INST. OF WORLD POLITICS (Oct. 22, 2020), https://www.iwp.edu/active-measures/2020/10/22/a-review-of-the-trump-administrations-national-cyber-strategy-need-for-renewal-and-rethinking-of-the-public-private-partnership-in-u-s-national-security-policy/; *see also* U.S. DEP'T OF DEF., *Summary of Department of Defense Cyber Strategy* 1 (Sept. 18, 2018), https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

109. *See* Brendan I. Koerner, *Inside the Cyberattack That Shocked the US Government*, THE WIRED (Oct. 23, 2016), https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/; Dina

In its 2017 National Security Strategy, the Administration identified "Keep America Safe in the Cyber Era" as a key theme of its first pillar of national strategy to protect American people and homeland, and emphasized cyberspace as an area to enhance defense capabilities, along with military, defense industry, nuclear, space and intelligence capabilities.[110] The Administration also published the first National Cyber Strategy in more than 15 years in 2018.[111] Using the same four-pillar approach in the National Security Strategy, the document recognized the "growing centrality" of cyberspace to America's financial, social, government and political life, reviewed cyberattacks by foreign nation-state adversaries, terrorists and criminals, and committed to actions to address cyber threats and protect U.S. cyberspace.[112] It emphasized the importance of strengthening and safeguarding federal networks and critical infrastructure, combat and deter foreign espionage and intelligence, promote internet freedom and internet governance, and foster a vibrant and resilient U.S. digital economy.[113]

Threats in the cybersecurity arena often arise from hacking, malware, network intrusion, and other forms of cyber-attacks, targeting managed service providers (MSPs), government networks, and even critical infrastructure.[114] These concerns were central to Trump's finding in Executive Order 13873, where it provided that "foreign adversaries are increasingly creating and exploiting vulnerabilities in information and communications technology and services, which store and communicate vast amounts of sensitive information, facilitate the digital economy, and support critical infrastructure and vital emergency services, in order to commit malicious cyber-enabled actions, including economic and industrial espionage against the United States and its people."[115]

The involvement of nation-state actors who are foreign adversaries of the United States make the issue of cyber exploitation of U.S. persons more

Temple-Raston, *A "Worst Nightmare" Cyberattack: The Untold Story of the SolarWinds Hack*, NPR (Apr. 16, 2021), https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.

110. *See* THE WHITE HOUSE, *National Security Strategy of the United States of America*, (Dec. 2017), 12, 31, https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

111. Atkinson, *supra* note 108.

112. *See* THE WHITE HOUSE, *National Cyber Strategy of the United States of America* (Sept. 2018), 1–3, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

113. *See id.*

114. *See, e.g.*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, U.S. DEP'T OF HOMELAND SEC., *Chinese Malicious Cyber Activity*, https://us-cert.cisa.gov/china (last visited Apr. 6, 2021); Alex Marquartdt et al., *Florida Water Treatment Facility Hack Used a Dormant Remote Access Software, Sheriff Says*, CNN (Feb. 10, 2021), https://www.cnn.com/2021/02/10/us/florida-water-poison-cyber/index.html; David E. Sanger, *Russian Hackers Broke Into Federal Agencies, U.S. Officials Suspect*, N.Y. TIMES (Dec. 13, 2020), https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-us-government-treasury-commerce.html.

115. Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 22689 (May 17, 2019).

significant. Digital extortion of military officers are a primary example.[116] In the Grindr acquisition, one of the reported concerns for CFIUS is the potential exploitation by Chinese state actors against US military or government personnel.[117] Another example would be the using of social media to acquire information from government contractors.[118] These concerns are expressed not just by the intelligence community, but by congressional leaders as well.[119]

Recently updated national security laws have also demonstrated prominent concerns over these issues. In addition to the authority to regulate foreign investment over or near critical infrastructure, FIRRMA specifically added the sensitive personal data provision.[120] Although the FIRRMA reforms do not pre-date the rising awareness of privacy as a national security concerns, it certainly helps crystalize the understanding of the government regulators on how to deal with foreign access to U.S. user data.

One of the benefits of the WeChat and TikTok debate is that it elevates the status of data privacy issue as an issue of national security.[121] While the debate has been prominent in the past due to cases of cyber-attacks, economic espionages, and foreign intelligence activities, the debate has been expanded to foreign access to U.S. user data through backdoors and kill

116. *See* DEF. SEC. SERV. & NAT'L COUNTERINTELLIGENCE & SEC. CTR., *Cyber Threats*, https://www.dcsa.mil/Portals/91/documents/pv/mbi/Cyber_Threats.pdf (last visited Apr. 6, 2021); CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, U.S. DEP'T OF HOMELAND SEC., *Ransomware Guidance & Resources*, https://www.cisa.gov/ransomware (last visited Apr. 6, 2021).

117. *See* Sarah B. Danzman & Geoffrey Gertz, *Why is the U.S. Forcing a Chinese Company to Sell the Gay Dating App Grindr*, WASH. POST (Apr. 3, 2019), https://www.washingtonpost.com/politics/2019/04/03/why-is-us-is-forcing-chinese-company-sell-gay-dating-app-grindr/.

118. *See* Catalin Cimpanu, *FBI Warning: Foreign Spies Using Social Media to Target Government Contractors*, ZERO DAY NET (June 18, 2019), https://www.zdnet.com/article/fbi-warning-foreign-spies-using-social-media-to-target-government-contractors/; *see also* Press Release, Off. of Dir. of Nat'l Intel., FBI And NCSC Release New Movie to Increase Awareness of Foreign Intelligence Threats on Professional Networking Sites and other Social Media Platforms (Sept. 29, 2020), https://www.dni.gov/index.php/ncsc-newsroom/item/2145-nevernight-press-release#:~:text=%E2%80%9CSocial%20media%20deception%20continues%20to,said%20NCSC%20Director%20William%20Evanina.

119. *See* NAT'L COUNTERINTELLIGENCE AND SECURITY CTR, *Unclassified NCSC Info for Re. Lynch* (July 10, 2020), https://oversight.house.gov/sites/democrats.oversight.house.gov/files/Unclassified%20NCSC%20Info%20for%20Rep%20Lynch_0.pdf; OFF. OF U.S. REP. STEPHEN F. LYNCH, *Chairman Lynch Seeks Info on Foreign Entities Accessing U.S. Mobile Application Data* (Dec. 13, 2019), https://lynch.house.gov/2019/12/chairman-lynch-seeks-info-foreign-entities-accessing-us-mobile-application-data.

120. *See* Austin Mooney, *Spotlight on Sensitive Personal Data as Foreign Investment Rules Take Force*, 10 NAT'L L. REV. 49 (2020).

121. *See* Mishaela Robison & Jack Karsten, *What the Debate Over TikTok Means for the Future of Social Media*, BROOKINGS INST. (Oct. 12, 2020), https://www.brookings.edu/blog/techtank/2020/10/12/what-the-debate-over-tiktok-means-for-the-future-of-social-media/.

switches through which state actors may access and exploit such data or persons with such data.[122]

2. *Economic Security*

Economic security has been a recurring theme in the Trump Administration's cyber policy agenda. In the National Cyber Strategy, it elevated economic security interest to the forefront of its policy agenda by identifying "Promoting American Prosperity" as one of the four pillars of its strategies. Specifically, it identified three focal points for actions—foster a vibrant and resilient digital economy, foster and protect United States ingenuity, and develop a superior cybersecurity workforce.[123]

Now of these focal points, on its face, seems to fit into the traditional realm of national security considerations, and it was not reflected in the *WeChat* litigation either. However, as with other areas of national security actions taken by the Administration, the Federal Government during the past four years have often incorporated industrial policy considerations into its national security policy agenda. Setting aside the question on whether or not this is another attempt to hide the Administration's America-First, protectionist agenda in the name of "national security", it does show a willingness on the part of the government to take actions to protect and facilitate a U.S. industry to thrive internationally.[124]

Moving beyond policy targets it set, the government seems to have kept its words. Many of the Trump actions also had an industrial or economic policy undertone that shift the conversation of national security to the issues of economic security and industrial competitiveness. For example, Trump's Executive Order 13873 specifically cover transactions that "poses an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of information and communications technology or services in the United States", as well as those that "poses an undue risk of catastrophic effects on … the digital economy of the United States."[125] This is a theme confirmed by the Department of Commerce's Strategic Plan as well as Department of

122. *See e.g.*, NAT'L COUNTERINTELLIGENCE AND SECURITY CTR, *Unclassified NCSC Info for Re. Lynch* (July 10, 2020), https://oversight.house.gov/sites/democrats.oversight.house.gov/files/Unclassified%20NCSC%20Info%20for%20Rep%20Lynch_0.pdf.

123. *See* THE WHITE HOUSE, *National Cyber Strategy of the United States of America* (Sept. 2018), 1–3, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

124. *See* Keman Huang & Stuart Madnick, *The TikTok Ban Should Worry Every Company*, HARVARD BUS. REV. (Aug. 28, 2020), https://hbr.org/2020/08/the-tiktok-ban-should-worry-every-company.

125. Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 22689 (May 17, 2019).

Homeland Security's analysis on national security in the age of digital economy.[126]

Whether or not the Biden Administration is going to beyond this economic security argument, the Interim National Security Strategic Guidance issued by the new Administration seems to suggest that at least some of these policies will stay for the foreseeable future.[127]

IV. *TIKTOK*, IEEPA AND EXECUTIVE AUTHORITY

The government action also led to two additional adverse court decisions against it under the IEEPA personal communication and information material exceptions. These two decisions may prove problematic in the future for the government if it attempts to restrict TMT platforms under the IEEPA again, as the statute is not the only one with a public information exception.[128]

A. *TIKTOK*

As noted by the district court in *TikTok*, under IEEPA, "the authority granted to the President . . . does not include the authority to regulate or prohibit, directly or indirectly either (a) the importation or exportation of information or informational materials; or (b) personal communications, which do not involve a transfer of anything of value."[129]

By finding that the TikTok ban to be, at the very least, an indirect regulation over information materials and personal communication, the *TikTok* court found the government action to be *ultra vire* and in violation of both IEEPA and the APA.[130]

In addition, in evaluating the balance of hardship and public interests under a motion for preliminary injunction, the Court took note of the necessity to "give deference to the Executive Branch's 'evaluation of the facts' and the 'sensitive and weighty interests of national security and foreign affairs'" and acknowledged that the Government advanced "ample evidence that China presents a significant national security threat."[131] However, it found "specific evidence of the threat posed by Plaintiffs, as well as whether

126. U.S. DEP'T OF COM., *U.S. Department of Commerce Strategic Plan 2018-2022: Helping the American Economy Grow* 19, https://www.commerce.gov/sites/default/files/us_department_of_commerce_2018-2022_strategic_plan.pdf (last visited Apr. 6, 2020); U.S. DEP'T OF HOMELAND SEC. & OFF. OF DIR. OF NAT'L INTEL., *Emerging Technology & National Security* 10 (July 26, 2018), https://www.dhs.gov/sites/default/files/publications/2018_AEP_Emerging_Technology_and_National_Security.pdf.

127. *See* THE WHITE HOUSE, *Interim Nat'l Sec. Strategic Guidance* 20 (Mar. 2021), https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.

128. *See, e.g.*, Trading with the Enemy Act, Pub. L. No. 65–91, 40 Stat. 411 (1917).

129. *See TikTok*, 507 F. Supp. 3d at 102 (citing 50 U.S.C. §§ 1702(b)(1), (3)) (cleaned up).

130. *See id.* at 111.

131. *See id.* at 114.

the prohibitions are the only effective way to address that threat, remains less substantial."[132]

However, the Court declined to rule against the Government based on the scant evidence the Government advanced. Rather, on the issue of balance of equity and public interests, the Court reiterated that the Government cannot suffer any harm or sacrifice any public interest when a court enjoins an "unlawful practice".[133]

B. *MARLAND*

The Philadelphia District Court in *Marland* went further than *TikTok*.

To begin with, in *Marland*, the Government argued that the case to be unreviewable, because: first, the cited authorities of IEEPA and the National Emergency Act preclude judicial review; second, under the APA, the TikTok ban was an action committed to agency discretion that preclude judicial review. The Court rejected both arguments.

Then, similar to the *TikTok* decision, the *Marland* court found the plaintiffs would likely succeed on the APA claim because IEEPA's personal communication and information material exceptions were clearly violated.[134]

Last, in evaluating the balance of hardship and public interests, the Court sidestepped the Government's proffered national security threats as merely "hypothetical", and IEEPA's personal communication exceptions represented a congressional judgment that "President's ability to exercise his IEEPA authority to respond to a national emergency does not extend to actions that directly or indirectly regulate the importation or exportation of informational materials."[135]

C. BROADER IMPLICATIONS

If anything, the *TikTok* and *Marland* decisions may prove to be more problematic for the Government than the *WeChat* decision, at least from a short-term perspective.

First, the *Marland* court explicitly rejected the argument that the government ban is not justiciable. While some of the regulatory authorities mentioned in earlier sections of this article, such the President's and CFIUS' authorities to review transactions, are often nonjusticiable because of the statutes' non-reviewability clauses, there is no such a provision under the IEEPA. Besides, the *Marland* court intentionally draws the distinction between the President's executive actions and the Secretary's decisions by suggesting that it was not reviewing "essentially political questions surrounding the declaration or continuance of a national emergency" but

132. *See id.*
133. *See id.* at 115.
134. *See* Marland v. Trump, 498 F. Supp. 3d 624, 641 (E.D. Pa. 2020).
135. *See id.* at 642.

"whether the actions taken pursuant to a national emergency comport with the power delegated by Congress." As such, future challenges over actions from the Government's decisions from the ICT Supply Chain EO, for example, may be subject to judicial review.

Second, both courts provided clear and concise interpretation of IEEPA's personal communication and information material exceptions, adding two more adverse precedents to a small but increasing number of case laws in a less-tested area of law. By drawing analogies between TikTok videos and "films", "photographs", "artworks", "newswire feed", the courts found that delisting of a social media app amounts to prohibition of a foreign newswire service. This analysis foreshadows future attempt to regulate mobile apps and software that carries at least some non-commercial personal communication and information materials.[136]

It is also important to note that under the ECRA, the IEEPA personal communication exception is incorporated into the export control context.[137] As such, any case law applying the IEEPA personal communication exception would have the same interpretative effect on the ECRA.

Third, while the Government warned of a "IEEPA free zone" where foreign adversaries would swamp U.S. with malign cyber actors and data services, both courts suggested that such a free zone could exist by the design of the statute and the Government cannot do anything about it, until the law is revised.[138]

V. AFTERMATH

In June, the government informed the court that it would rescind the two bans, and therefore would moot the court proceedings.[139] This is consistent with the approach the Biden Administration has taken in many litigations it inherits from the Trump Presidency.[140] Like the new administration's break from the Trump Administration in abandoning or reversing course in the WeChat and TikTok cases, it had reversed course in a slew of administrative and regulatory actions on issues ranging from immigration, environment, labor, trade to antitrust.[141] Like the past where

136. Note that under *TikTok*'s interpretation of 50 U.S.C. §§ 1702(b)(3), as along as at least some personal communication has no economic value, such as the case of some messages on WeChat or some videos on TikTok clearly would do, the personal communication exception would preclude bans like the TikTok and WeChat ban. *See TikTok*, 507 F. Supp. 3d at 108.

137. *See* Export Control Reform Act of 2018, *supra* note 8, at § 1754.

138. *See TikTok*, 507 F. Supp. 3d at 108; *Marland*, 498 F. Supp. 3d at 641.

139. *See* David Shepardson, *Biden administration asks courts to dismiss government appeals of TikTok ruling*, REUTERS (July 12, 2021), https://www.reuters.com/business/retail-consumer/us-asks-court-dismiss-government-appeal-tiktok-ruling-2021-07-12/.

140. *See* Lawrence Hurley, *Biden pivots away from old court battles, helps ignite new ones*, REUTERS (Jan. 21, 2021), https://www.reuters.com/article/us-usa-biden-court/biden-pivots-away-from-old-court-battles-helps-ignite-new-ones-idUSKBN29Q2UH.

141. *See id.*

new administration came in to reverse courses in regulatory actions with pending litigations extended beyond a former administration, the reversal would often resolve the underlying legal controversial at issue and therefore allow the government to moot the pending litigations with cases dismissed and opinions vacated.

Curiously, while the government chose to reverse the bans and seeks dismissal, it has chosen not to seek a vacatur of the courts' orders in any of the district court litigations. In the *TikTok* litigations, it sought and secured the courts' dismissal of all district court and appellate court proceedings.[142] However, because the court opinions are not vacated, they remain on the book with limited but persuasive precedential value.[143]

Although the two bans were rescinded in an executive order,[144] there are some suggestion that the Biden Administration may continue to seek other ways to limit WeChat and TikTok's national security risks.[145] But the tumultuous history of the WeChat and TikTok bans and the complicating judicial defeats may pose significant challenges for the Government beyond the short-term.

VI. A TUMULTUOUS PAST AND A TROUBLED FUTURE

In his first year in office, President Biden has generally maintained the status quo of his predecessor's policies in the TMT sector, despite his decision to abandon the WeChat and TikTok bans.

His Secretary of Commerce, Gina Raimondo, pledged to be "very aggressive" against Chinese trade practices and to "play" both defense and offensive against Chinese actions.[146] In her confirmation hearing, she also reiterated Biden's whole-of-government approach against China, without specifying what actions she would take on export control, trade remedies and ICT supply chains.

On the ICT front, the Trump Administration enacted an Interim Final Rules under the ICT Supply Chain Executive Order on the last day of the administration, providing with the Commerce Secretary the authority to

142. *See, e.g.*, U.S. WeChat Users All. v. Trump, No. 20-16908 (9th Cir. 2020); Marland v. Trump , No. 20-3322 (3d Cir. 2020); TikTok v. Trump , No. 20-05302 (D.C. Cir. 2020).

143. *Contra* Robert P. Deyling, *Dangerous Precedent: Federal Government Attempts to Vacate Judicial Decisions upon Settlement*, 27 J. MARSHALL L. REV. 689 (1994). The most significant example of this approach is the Supreme Court's application of the *Munsingwear* vacatur to the Ninth Circuit's first travel ban decision. *See* Josh Blackman, *A Nonchalant Conclusion to Trump v. IRAP*, LAWFARE (Oct. 13, 2020), https://www.lawfareblog.com/nonchalant-conclusion-trump-v-irap.

144. *See* Exec. Order No. 14,034, 86 Fed. Reg. 13423 (2021).

145. *See* John D. McKinnon & Alex Leary, *U.S. Moving—Some Say Too Slowly—to Address TikTok Security Risk*, WALL ST. J. (Feb. 2, 2022), https://www.wsj.com/articles/tiktok-security-risk-china-biden-11643807751.

146. See Jeanne Whalen, *Biden's Commerce Secretary Pick Pledges a Tough Line on Chin But Doesn't Detail How She'd Deal With Huawei*, WASH. POST (Jan. 26, 2021), https://www.washingtonpost.com/technology/2021/01/26/gina-raimondo-confirmation-china/.

review and block any foreign-related services, platforms, and transactions involving ICTs, defined to cover anything from mobile network software, cable routers, fiber optical cables, cloud service platforms, drones, video games, mobile apps, to quantum computing devices.[147] The Biden Administration not only allowed the measure to go into effect on March 22, 2021,[148] but sought to expand the scope of the Rule in November 2021 to cover "connected software applications", including "software, a software program, or a group of software programs, that is designed to be used on an end-point computing device and includes as an integral functionality, the ability to collect, process, or transmit data via the internet."[149]

Significantly, the final rule has been interpreted by leading trade groups to give "nearly unlimited authority" to the Commerce Department "to intervene in virtually any commercial transaction between U.S. companies and their foreign counterparts that involves technology, with little to no due process."[150] This action, interpreted by the business community as antithetical to the Biden Administration's approach with industrial innovation for the broad scope of that proposed rule and its promise to enact a government-wide approach in dealing with foreign adversary like China, seems to be consistent, though, with the administration's effort to re-evaluate its industrial policy with regards to supply chain worries.

Additionally, in the new Executive Order on June 11, 2021 calling for an expansion of the final rule to cover "connected software applications", it also asks agencies to prepare a report on measures to "protect Americans' sensitive data from foreign adversaries."[151] The Administration also maintained an Office of Intelligence and Security within the Commerce Department formed under the direction of the ICT Supply EO, under which it had issued subpoenas and conducted investigations into several Chinese technology companies, including e-Commerce Giant Alibaba's cloud service unit.[152]

147. *See* 15 C.F.R. § 7.3 (2021).

148. *See* John D. McKinnon, *U.S. to Impose Sweeping Rule Aimed at China Technology Threats*, WALL ST. J. (Feb. 26, 2021), https://www.wsj.com/articles/u-s-to-impose-sweeping-rule-aimed-at-china-technology-threats-11614362435.

149. U.S. DEP'T OF COMM., *Securing the Information and Communications Technology and Services Supply Chain; Connected Software Applications*, 86 Fed. Reg. 67379 (Nov. 26, 2021).

150. *See* David Shepardson & Karen Freifeld, *U.S. Seeks Input on Licensing Rules for Information Tech Security*, REUTERS (Mar. 26, 2021), https://www.reuters.com/article/us-usa-china-telecommunications-idUSKBN2BI2QX.

151. *See* Exec. Order No. 14,034, 86 Fed. Reg. 13423 (2021).

152. *See* U.S. DEP'T OF COMM., *U.S. Secretary of Commerce Gina Raimondo Statement on Actions Taken Under ICTS Supply Chain Executive Order* (Mar. 17, 2021), https://www.commerce.gov/news/press-releases/2021/03/us-secretary-commerce-gina-raimondo-statement-actions-taken-under-icts; REUTERS, *U.S. examining Alibaba's cloud unit to determine whether it poses a national security risk: Reuters, citing sources*, CNBC (JAN. 19, 2022), https://www.cnbc.com/2022/01/19/us-examining-alibabas-cloud-unit-for-national-security-risks-reuters.html.

However, as the Biden Administration continues to roll out its whole-of-government approach in countering foreign threat in the TMT sector, it should bear in mind of the tumultuous history of the Trump era and avoid the numerous pitfalls his predecessor experienced.

A. PATCHWORK OF GOVERNMENT REGULATORS AND POLICIES

Regulatory authorities in internet regulation of the Trump era fall within different federal regulators. First, the Federal Communication Commission continued to enjoy broad, independent authority to enact licensing and transaction limits and take enforcement actions on foreign access to the telecommunication sectors due to national security concerns.[153] Second, the Department of Commerce, under the ICT Supply Chain EO, enjoys the authority to review any transaction involving ICTs,[154] with primary authority delegated to the National Telecommunications and Information Administration.[155] It also enjoyed the authority, through the Bureau of Industry and Security, in issuing export license and reviewing export transactions involving U.S. technologies, including emerging and foundational technologies.[156] Third, the Department of Treasury chaired CFIUS in reviewing FDIs into the U.S. internet sectors.[157] Lastly, other agencies can also played significant role in these policy initiatives, including the National Security Division of the Department of Justice in the Team Telecom initiative,[158] the Defense Technology Security Administration of

153. *See, e.g.*, Communication Acts of 1934, Pub. L. No. 73-416, § 214, 48 Stat. 1064, 1075 (1934); John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 889, 132 Stat. 1636, 1917 (2018); Secured and Trusted Communications Networks Acts of 2019, Pub. L. No. 116-124, §§ 2, 4, 134 Stat. 158, 158, 160 (2020).

154. *See* Exec. Order No. 13,873, 84 Fed. Reg. 22689 (2019).

155. *See* Josephine LeBeau et al., *Take Two: Another Executive Order Addresses U.S. Personal Data Concerns by Prohibiting Business with Companies That Develop or Control Eight Specified Applications with Connections to China*, JDSUPRA (Jan. 7, 2021), https://www.jdsupra.com/legalnews/take-two-another-executive-order-4209045/; NAT'L TELECOMM. & INFO. ADMIN., U.S. DEP'T OF COM., *NTIA Announces Supply Chain Information-Sharing program* (July 8, 2020), https://www.ntia.doc.gov/blog/2020/ntia-announces-supply-chain-information-sharing-program; NAT'L TELECOMM. & INFO. ADMIN., U.S. DEP'T OF COM., *ICT Supply Chain*, https://www.ntia.doc.gov/category/ict-supply-chain (last visited Mar. 12, 2020).

156. *See* John R. Shane & Lori E. Scheetz, *Commerce Publishes new Controls on Emerging Technologies*, WILEY REIN LLP (Oct. 7, 2020), https://www.wiley.law/alert-Commerce-Publishes-New-Controls-on-Emerging-Technologies.

157. *See* U.S. DEP'T OF TREASURY, *The Committee on Foreign Investment in the United States (CFIUS)*, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius (last visited Apr. 6, 2021).

158. *See* U.S. DEP'T OF JUSTICE, *The Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector* (updated Apr. 23, 2020), https://www.justice.gov/nsd/committee-assessment-foreign-participation-united-states-telecommunications-services-sector-0.

the Department of Defense in the CFIUS review process,[159] and the Cyber and Infrastructure Security Agency of the Department of Homeland Security in the ICT Supply Chain risk assessment initiatives.[160]

While the CFIUS process and the Team Telecom initiative will help foster better communications and policymaking in regulating the internet sector, it is still too early to say if Biden Administration will bring a whole-of-government perspective into the fight against foreign exploitation of social media platforms and content.

B. CONTRADICTORY TOWARDS FIRST AMENDMENT VALUE

Amici briefs filed by the Internet Society and EFF with the appellate courts ask the courts to rule against the government, because of the broad prior restraint implications of the cases, especially in the domestic context.[161] Some of these amici seem to point towards potential dangerous domestic implications of the government far-reaching interpretation and application of national emergency law, given that all the proposed ban requires is a foreign nexus of the platform. Some of these *amici* briefs even equate the proposed bans with the prior restraint in the *Pentagon Papers* case—citing national security to limit the free flow of speech. The government disagreed in an answer to Judge Ryan Nelson's question in the *WeChat* oral argument, suggesting that they do not have any power to regulate domestic social media platforms, even when a group of domestic users attempt to use a social media app to overthrow the government.[162]

However, setting aside the question on the broader *domestic* implications of the proposed bans, the *WeChat* and *TikTok* bans were also inconsistent with the pronounced policy of the Trump Administration. In the National Cyber Strategy, the government repeatedly emphasized the importance of promoting internet freedom on the world stage. However, it would only seem more ironic that the most landmark action the Trump Administration has taken at the end of its four-year term was one of the most

159. *See* DEF. TECH. SEC. ADMIN., U.S. DEP'T OF DEF., *Committee on Foreign Investment in the United States (CFIUS)*, https://www.dtsa.mil/SitePages/assessing-and-managing-risk/committee-on-foreign-investement-in-us.aspx (last visited Apr. 6, 2021).

160. *See* CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, U.S. DEP'T OF HOMELAND SEC., *Information & Communications Technology Supply Chain Risk Management (SCRM)*, https://www.cisa.gov/supply-chain (last visited Apr. 6, 2021).

161. *See* Dkt. No. BL-51, U.S. WeChat All. v. Trump, No. 20-16908 (9th Cir. Dec. 4, 2020); Dkt. No. BL-29, Marland v. Trump, No. 20-03322 (3rd. Cir. Jan. 22, 2021); Keman Huang & Stuart Madnick, *The TikTok Ban Should Worry Every Company*, HARV. BUS. REV. (Aug. 28, 2020), https://hbr.org/2020/08/the-tiktok-ban-should-worry-every-company; Haille Laws, *When Viral Videos Become A National Security Threat: TikTok Inc. v. Trump*, MINN. L. REV. ONLINE (Dec. 29, 2020), https://minnesotalawreview.org/2020/12/29/when-viral-videos-become-a-national-security-threat-tiktok-inc-v-trump/.

162. Edvard Pettersson, *WeChat Ban Urged by U.S. Gets Skeptical Review by Appeals Court*, BLOOMBERG (Jan. 14, 2021), https://www.bloomberg.com/news/articles/2021-01-14/wechat-ban-urged-by-u-s-gets-skeptical-review-by-appeals-court.

restrictive and dramatic action ever taken by the Federal Government since the *Pentagon Papers* case. This approach would only undermine the government's own credibility in promoting and advocating for freedom of speech and internet freedom, while giving the foreign adversaries more ammunition to attack internet freedom in their own countries.

C. LOSING CREDIBILITY

While neither the two district courts that ruled under IEEPA nor the district court that ruled under the First Amendment interpreted it that way, many commentators have serious doubts about the legitimacy of the national security interests claimed by the government.[163] Some view it as personal revenge for TikTok and many other platforms' popular revolt against his re-election campaign, specifically for the role K-pop fans and TikTok played in tanking his Tulsa event turnout;[164] others suggest the TikTok ban as a move to Americanize the company.[165] But what is clear is that the courts were never fully convinced with the government's on-the-surface justifications, at least initially. The *WeChat* court did not go as far as plaintiffs wanted to call it a content-based restrictions for the President's alleged racial animus, but acknowledged that "while the government has established that China's activities raise significant national security concerns — it has put in scant little evidence that its effective ban of WeChat for all U.S. users addresses those concerns."[166] After the setbacks in the *WeChat* proceedings, the government prepared confidential filings for Judge Nichols in the D.C. District Court to review *ex parte*, but the court did not give a better time to the government by noting that although it "has provided ample evidence that China presents a significant national security threat, although the specific evidence of the threat posed by Plaintiffs, as well as whether the prohibitions are the only effective way to address that threat, remains less substantial."[167]

A more important issue is that the court really did go into details in its consideration of the government's consideration of alternatives under the narrowly tailoring prong of intermediate scrutiny. Several courts considered the government's proffered memo, drafted by an advisor to Commerce

163. *See* Brown, *infra* note 164; Zachary Karabell, *Trump's TikTok Policy Is Just a New Kind of "Security Theater"*, POLITICO MAG. (Sept. 15, 2020), https://www.politico.com/news/magazine/2020/09/15/trumps-tiktok-policy-is-just-a-new-kind-of-security-theater-415088.

164. *See* Abram Brown, *Is This the Real Reason Why Trump Wants To Ban TikTok?*, FORBES (Aug. 1, 2020), https://www.forbes.com/sites/abrambrown/2020/08/01/is-this-the-real-reason-why-trump-wants-to-ban-tiktok/.

165. *See* David Pierce, *How Trump's TikTok Ban Might Actually Work—Or Not*, PROTOCOL (Aug. 1, 2020), https://www.protocol.com/tiktok-ban.

166. *See* U.S. WeChat All. v. Trump, 488 F. Supp. 3d 912, 927 (N.D. Cal. Sept. 19, 2020).

167. Todd Spangler, *Trump Administration Likely Exceeded Legal Authority with TikTok Ban, Judge Rule*, VARIETY (Sept. 28, 2020), https://variety.com/2020/digital/news/trump-tiktok-ban-exceeded-legal-authority-ruling-1234785547/.

Secretary Wilbor Ross, in which the advisor conceded the existence of other less drastic alternatives.[168] In fact, a Department of Homeland Security study recommends banning the use of the app on the devices of government agencies and critical infrastructure operators, and implement steps to address data exposure risks, such as location-data exposures, rather than an outright ban.[169] That seems to be enough, for the court, to rule against the government.

The government may have one disadvantage in its arguments—it was hard to carve out a narrowly tailored restriction on the alleged cyber-security and privacy concerns. One may argue that this is a self-imposed wound, because the concerns were simply too speculative.[170] However, the fact that no similar measure has ever been adopted in the United States also underscored the significance of the challenges and controversial nature of the action. Regardless, the government still has the option in TikTok's case to address the fundamental issues through CFIUS.[171]

Another complicating factor in the *WeChat* case is that WeChat is a social media platform with predominantly users from the Chinese American and Chinese diaspora communities.[172] As such, justifying reasonable alternatives for the affected communities can be difficult, especially if the platform offers Chinese-language services and plaintiffs characterize the platform as one for Chinese American to communicate with people from their mother land.

But in any case, because of the dramatic nature of the actions taken in these two cases and the pretext national security justifications proffered,[173]

168. *See* Notice of Corrected Ex. in Support of Mot. to Stay, Ex. A, U.S. WeChat v. Trump, No. 3:20-cv-05910-LB (N.D. Cal. Sept. 28, 2020) ECF. No. 76-1;*see also* U.S. WeChat All. v. Trump, No. 3:20-cv-05910-LB, 2020 WL 6891820, at *8 (N.D. Cal. Nov. 24, 2020) (denying motion to stay injunction) (rather than taking narrowly tailored approaches "such as barring WeChat from government devices" or "adopting mitigation procedures like those in Tencent's mitigation proposal and Joe Hildebrand's best practices about data security", the restrictions "burden substantially more speech than is necessary to further the government's legitimate interests.").

169. *See id.* at *1.

170. *See* Zachary Karabell, *Trump's TikTok Policy Is Just a New Kind of "Security Theater"*, POLITICO MAG. (Sept. 15, 2020), https://www.politico.com/news/magazine/2020/09/15/trumps-tiktok-policy-is-just-a-new-kind-of-security-theater-415088; Neil Davey, *While the DOJ Appeals the Preliminary Injunction on President Trump's TikTok Ban, the Administration's National Security and Privacy Concerns Seem Unfounded*, JOLT DIGEST (Oct. 20, 2020), https://jolt.law.harvard.edu/digest/while-the-doj-appeals-the-preliminary-injunction-on-president-trumps-tiktok-ban-the-administrations-national-security-and-privacy-concerns-seem-unfounded.

171. *See* Davey, *supra* note 170.

172. *See* U.S. WeChat Users All. v. Trump, 488 F. Supp. 3d 912 (N.D. Cal. Sept. 19, 2020).

173. For example, in *Xiaomi v. Dep't of Def.*, a federal judge found the Defense Department's decision to designate Xiaomi as a company linked to the Chinese military as an arbitrary and capricious, and blocked the Department's decision to force U.S. companies to stop invest in the Chinese smartphone manufacturer. *See* Xiaomi v. Dep't of Def., No. 21-280, 2021 WL 950144 (D.D.C. Mar. 12, 2021).

the government lost, not just its two proposed bans but potentially its credibility in the future.[174]

D. MOVING BEYOND THE PAST

Beyond the persuasive effect of the court decisions, the long-term effect of the Trump Administration's approach in these litigations will not and cannot be easily eliminated.

What the two litigations reveal are two pairs of dilemma that the government is faced with: on the one hand, it is emphasizing the importance of privacy and data security against foreign adversaries; on the other hand, its respect for U.S. users' privacy and data security are lacking at best, and legislative efforts by the Federal Government to protect user privacy are nowhere near to be complete. Similarly, on the one hand, free speech advocates are crying aloud against the government actions in *WeChat* and *TikTok*; on the other hand, the government is complaining to the court that it has no power to regulate social media absent a foreign nexus.

First, these bans provide courts with more ammunition and justification to sidestep the justiciability and reviewability issues in the national security context. Constitutional challenge over national security decision-making has already been recognized by some courts. For example, the D.C. Circuit in *Ralls v. CFIUS* determined that the courts could directly intervene in constitutional challenges over national security determination processes of CFIUS, citing a rarely cited exception for constitutional challenge over agency action.[175] The *TikTok* litigations opened further for administrative law challenge over national security decisions. While the *Marland* and *TikTok* courts did not challenge the underlying national security declarations or the Executive Order, both courts did find that they have authority to

174. Trump Administration has lost about 77% of its regulatory and administrative moves. *See Roundup: Trump-Era Agency Policy in the Courts*, INST. FOR POLICY INTEGRITY (last updated Apr. 1, 2021), https://policyintegrity.org/trump-court-roundup. As Professor Saikrishna Prakash wrote for Harvard Law Review, as the Executive Branch stretched and strained its power, the courts would intervene more. Sometimes, the government seems to be engaged in a self-contradictory battle:

"One imagines that lawyers receive recurring calls with the following directive: Find a plausible (meaning non-laugh-inducing) legal argument that permits the President to take some act or adopt some measure. If the argument prevails in court, fantastic. If the argument fails, at least we tried to advance the President's agenda. Moreover, we can spin any judicial defeat as a partisan decision that refused to credit our winning arguments." *See* Saikrishna B. Prakash, *The Age of the Winning Executive: The Case of Donald J. Trump*, 134 HARV. L. REV. FORUM 141, 143 (2020).

However, the result may not necessarily be great for future administrations because of the frequent court interventions. *See, e.g.*, Lee Epstein & Eric A. Posner, *The Decline of Supreme Court Deference to the President*, 166 U. PENN. L. REV. 829 (2018).

175. *See* Ralls v. CFIUS, 758 F.3d 296 (D.C. Cir. 2014). One of the most significant developments of the *Ralls* decision is that the D.C. Circuit explicitly rejected the district court's declination to take up jurisdiction and cite to a narrow, historical exception for constitutional challenge over statutory provision. *See id.* at 308 (citing Griffith v. FLRA, 842 F.2d 487, 494 (D.C. Cir. 1988); Ungar v. Smith, 667 F.2d 188, 193 (D.C. Cir. 1981)).

review whether the government actions are *ultra vires* against IEEPA. [176] These are the only two IEEPA decisions since *Holy Land Foundation v. Ashcroft* where a court has recognized a cause of action under IEEPA.[177] However, the *TikTok* court went even further to hold that not only did TikTok prevail under an ultra vires challenge under Section 706(2)(c) the Administrative Procedures Act, but also did it prevail under an arbitrary and capricious challenge under Section 706(2)(A).[178]

Second, it may put the government in a more difficult position to justify their actions. In the case of *WeChat*, the court's application of traditional First Amendment jurisprudence in that case shows that courts, while not directly putting their thumbs on the scale on the national security interests asserted by the government, may and could read into the rationale to see if there is a mismatch between the national security interests asserted and the alternative government regulations or actions considered and rejected. This could lead to increasing hostilities against government justifications and more expansive review over government discretions.

Third, but probably most importantly, the WeChat and TikTok decisions show the limit of government authority in safeguarding informational national security at the cross sections of foreign ownership and domestic usership. While the litigations and the ongoing ICT rulemaking process highlight the pressing needs for congressional actions, how far can congressional actions go remains another question.

For example, while congressional actions may help address some of the problems, such as reforming the IEEPA personal communication exceptions or instituting a permanent ICT review regime, it may not necessarily be able to address any constitutional issue. Besides, congressional actions will always lag behind the rapid changes of national security challenges in the information and communication sectors. In the national security context, it took more than a decade for Congress to completely revamp the CFIUS review regime, and four decades to revamp the Export Control regimes.

Another issue that will be front-and-center in the future congressional debates on ChinaTech or foreign social media platforms is the issue of privacy. Congress has been actively discussing privacy legislations for more than half a decade. If and when it does pass a national landmark privacy protection legislation, the issue of national security will likely come up. There are more questions than answers on how national security interests may be balanced against privacy interests, especially if a federal legislation

176. The government did raise reviewability issue in both *Marland* and *TikTok*, but both courts cite to Section 706(2)(C) of the Administrative Procedure Act for reviewing ultra vires actions and found that the government's actions in the TikTok ban context were ultra vires and in direct violation of the command of IEEPA. *See* Marland v. Trump, 498 F. Supp. 3d 624 (E.D. Pa. 2020); TikTok Inc. v. Trump, 507 F. Supp. 3d 92 (D.C. Cir. 2021).

177. *See* Holy Land Found., 333 F.3d at 172.

178. *See* TikTok, 507 F. Supp. 3d at 92.

will provide more rights and safeguards for individuals, such as a right to be forgotten or limitation on government access to private data. Can the government restricts, prohibits or conditions foreign ownership or access to U.S. user data? Can the government, for example, prohibits newly-emerged Chinese fashion site Shein from accessing the U.S. market? Can the government ask networking app Clubhouse to drop its Chinese audio technology provider?

While we know that the government has temporarily lost the battle against WeChat and TikTok, for U.S. users like you and me, we are still left in a digital wild west, where national security risks remain unaddressed, and free speech remain under attack.