THE EXCEPTION THAT PERSISTS: TIKTOK, PAFACA, AND NATIONAL SECURITY

Anqi Wang & Jyh-An Lee***

The Protecting Americans from Foreign Adversary Controlled Applications Act ("PAFACA"), often referred to as the "TikTok ban," represents the first federal statute in the United States that could remove a major social media platform from the domestic market. Enacted in April 2024 with bipartisan support, the law requires TikTok's Chinese parent company, ByteDance, to divest the platform or face an effective nationwide ban. While its implementation has been complicated by constitutional challenges and executive suspensions, the saga finally reached a resolution after a deal was struck to restructure TikTok's U.S. operations under a majority-American joint venture.

The legal and political debate surrounding PAFACA highlights two broader patterns. First, courts reviewing challenges to the statute have shown significant deference to congressional and executive assessments of national security. This posture translates to a lowered evidentiary threshold once security concerns are invoked, allowing predictive judgments to sustain legislative action even in the absence of concrete proof. While the U.S. Supreme Court's reliance on "predictive judgments" to sustain national security measures has a long historical trajectory, PAFACA marks the first time this deferential doctrine has been applied to a major expressive digital platform.

Second, PAFACA illustrates how national security logics are migrating from physical infrastructure to digital platforms. On the one hand, as communication mediums shift from traditional print media to algorithmic recommender systems, the potential for covert foreign

* Ph.D. Candidate, The Chinese University of Hong Kong Faculty of Law.

** Professor and Executive Director, Centre for Legal Innovation and Digital Society (CLINDS), The Chinese University of Hong Kong Faculty of Law. An earlier draft of this Article was presented at the 4th Machine Lawyering Conference hosted by The Chinese University of Hong Kong Faculty of Law. We are grateful for the invaluable insights and constructive feedback offered by Ebrahim Afsah, Kui Cai, Ryan Mitchell, Raymond Ku, Gregory Magarian, Jacob Noti-Victor, and Dicky Tsang. We are deeply grateful to the editors of the *N.Y.U. Journal of Legislation and Public Policy* for their insightful feedback and outstanding editorial support. All errors are our own.

influence and data exploitation undergoes a qualitative upgrade, becoming more pervasive and difficult to detect. Under this context, if the judiciary continues to apply established frameworks of deference without ratcheting up the legal standard for invoking deference to match these heightened risks, it may constrain executive discretion and grant expressive interests a higher priority than they enjoyed in earlier eras. On the other hand, however, PAFACA occupies a fundamentally different position from the previous cases on which the judicial deference doctrine was built. Unlike the regulation of physical infrastructure, PAFACA targets an open, expressive platform where the underlying architecture does not allow for a neat separation between "national security-sensitive data" and "constitutionally protected speech." Consequently, when the logic of national security exceptionalism is extended to TikTok, this expressive platform seems inevitably dragged into a domain of lowered constitutional protection. This creates a profound quandary: while the government invokes data risks to justify its intervention, the judicial deference grants the state a blank check to regulate a vast forum of public discourse.

Introduction

Once regarded as the unrivaled leader in short-form video sharing among American youth,[1] TikTok rapidly ascended to the pinnacle of social media platforms in the United States with its algorithmic feed and content ecosystem. Yet, TikTok's meteoric rise did not occur in a vacuum; intertwined with its popularity was a palpable unease about the platform's potential for foreign influence and data exploitation. While prior scandals, such as Cambridge Analytica, had established anxieties over data exploitation on social media platforms, TikTok was the first major social media platform whose parent company was not only foreign-owned, but headquartered in a country designated as a foreign

1. *See, e.g.*, Anu Bradford, Digital Empires: The Global Battle to Regulate Technology 216 (2023) (noting that TikTok surpassed Facebook in 2019 to become the most popular social media platform in the United States); Katie Boyd Britt, *Logging Off: A Comprehensive Agenda for Social Media and Mental Health*, 62 Harv. J. on Legis. 295, 303 (2025) ("When asked whether they had ever used certain social media sites, forty-nine percent of respondents between nine and twelve years old said they had used Instagram, fifty-two percent said they had used Facebook, fifty-eight percent said they had used Snapchat, and sixty-nine percent said they had used TikTok.").

adversary. As ByteDance, TikTok's parent company, remained subject to China's regulatory and political landscape, American policymakers and national security experts expressed concerns that the Chinese government could exploit the app for propaganda purposes or pressure ByteDance to surrender sensitive TikTok user data.[2] Certain critics even viewed the Chinese Communist Party (CCP) as the ultimate authority behind TikTok.[3]

These national security concerns resulted in legislative and organizational efforts to ban TikTok across the United States. Over half of state governments, along with the federal government, prohibited TikTok on official devices. In the private sector, companies like Wells Fargo required employees to remove TikTok from corporate-owned devices.[4] On April 24, 2024, President Biden signed into law H.R. 815, which included the Protecting Americans from Foreign Adversary Controlled Applications Act ("PAFACA").[5] PAFACA, backed by bipartisan support, identified TikTok as a significant national security concern and required its Chinese parent company, ByteDance, to divest TikTok to a suitable entity, otherwise TikTok would face a blanket ban on operating in the United States.[6]

PAFACA represents a new phase in the evolving relationship between national security and digital regulation. Whereas prior interventions, such as export restrictions against Chinese telecommunications

---

2. *See, e.g.*, BRADFORD, *supra* note 1, at 152; Laura He, *If the US Bans TikTok, China Will Be Getting a Taste of Its Own Medicine*, CNN NEWS (March 14, 2024, 12:20 PM), https://www.cnn.com/2024/03/14/tech/china-reactions-tiktok-potential-ban-intl-hnk/index.html [https://perma.cc/YAV8-V8GW]; Sapna Maheshwari & David McCabe, *TikTok Sues U.S. Government over Law Forcing Sale or Ban*, N.Y. TIMES (May 7, 2024), https://www.nytimes.com/2024/05/07/business/tiktok-ban-appeal.html [https://perma.cc/QPD2-832V]; *see also* David Finkelstein et al., *Information Manipulation on TikTok and Its Relation to American Users' Beliefs About China*, FRONTIERS SOC. PSYCH., Jan. 28, 2025, at 8 (finding a disproportionately high ratio of pro-CCP to anti-CCP content on TikTok, despite users engaging significantly more with anti-CCP content, suggesting propagandistic manipulation).

3. George F. Will, *How, Exactly, Is TikTok a Threat to National Security?*, WASH. POST (May 15, 2024), https://www.washingtonpost.com/opinions/2024/05/15/tiktok-ban-no-national-security-issue/ [https://perma.cc/P7EE-S2ZC].

4. *See, e.g.*, Max Burman, *Wells Fargo Tells Workers to Delete TikTok as Security, Privacy Concerns Grow*, NBC NEWS (July 11, 2020, 2:59 PM), https://www.nbcnews.com/tech/tech-news/wells-fargo-tells-workers-delete-tiktok-security-privacy-concerns-grow-n1233582 [https://perma.cc/8JBU-VKKC].

5. Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, div. H, 138 Stat. 955 (2024).

6. *Id.* § 2(a)(1) ("It shall be unlawful for an entity to distribute, maintain, or update . . . a foreign adversary controlled application."); Anders Hagstrom, *TikTok Sues to Block US Law Requiring Sale to Non-Chinese Company,* FOX NEWS (May 7, 2024), https://www.foxbusiness.com/politics/tiktok-sues-block-us-law-requiring-sale-non-chinese-company [https://perma.cc/X3WJ-WM5T].

equipment companies, were primarily concerned with the control of physical infrastructure,[7] PAFACA regulates expressive platforms and algorithmic content distribution. This reflects a shift of national security concerns from the hardware layer of technology to the content layer, from the supply chain of technology infrastructure to the informational autonomy of platforms.[8] Even extensive institutional compliance measures implemented by TikTok could not neutralize political perceptions of risk.[9] Some criticized the United States for departing from its longstanding rhetorical commitment to a free and open internet and embracing a form of sovereign digital control that it has historically attributed to authoritarian regimes.[10] In addition, PAFACA utilizes foreign ownership as a legal hook to combat the locus of risk arising from a foreign adversary, rather than addressing the structural privacy vulnerabilities of the domestic data economy.[11] It externalizes the costs of institutional inaction, transforming a problem of internal privacy governance into an object of geopolitical threat.

Following its enactment, TikTok and ByteDance challenged the constitutionality of PAFACA, carrying their First Amendment claims to the Supreme Court in *TikTok v. Garland*, where the Court ultimately upheld the Act.[12] In *TikTok v. Garland*, the Court upheld PAFACA and organized its reasoning around two questions: the scope of First Amendment protection and the degree of judicial deference warranted in national security cases.[13] On the surface, the Court's decision fits within existing patterns: Federal courts have long deferred to Congress on matters framed as national security judgments, and the turn toward

7. *See infra* Section III.C (explaining that earlier interventions against companies like Huawei and ZTE, from the 2019 designation to the Entity List under the Export Administration Regulations to the FCC's subsequent denial of equipment authorizations, focused on their role as providers of hardware).

8. *See infra* Section III.C.

9. *See infra* Section I.C.

10. *Your Expert Guide to the Debate over Banning TikTok*, Atl. Council (Jan. 9, 2025), https://www.atlanticcouncil.org/blogs/new-atlanticist/your-expert-guide-to-the-debate-over-banning-tiktok/ [https://perma.cc/C9RZ-XPZX] ("A TikTok ban will be a setback to all these years of effort and will legitimize the narrative by other authoritarian states that the internet should be subject to government control and management."); Ganesh Sitaraman, *The Regulation of Foreign Platforms*, 74 Stan. L. Rev. 1073, 1085 (2022) (noting that "tech neoliberals" opposed the TikTok and WeChat bans as threatening the open internet).

11. *See generally* Hannah Moore, *De-Identified and Unregulated: How Data Brokers Outpace State Privacy Laws*, 27 Vand. J. Ent. & Tech. L. 863 (2025) (discussing the lack of state or federal regulation of data brokers); Justin Sherman, Data Brokers and Sensitive Data on U.S. Individuals (2021) (discussing unregulated data brokers and the issues they create).

12. TikTok Inc. v. Garland, 604 U.S. 56 (2025) (per curiam).

13. *See infra* Part III.

deference was already visible in earlier disputes involving physical infrastructure, such as Huawei.[14] In this sense, the judicial deference in TikTok's case can be understood as an extension of the inclination to credit congressional and executive judgments in national security matters.

However, PAFACA occupies a different position from the cases on which the judicial deference doctrine was built: It targets an open, expressive digital platform. This means that the regulation reaches not only expression that could conceivably threaten national security, but also large volumes of benign, non-sensitive content that becomes a target of the ban merely by virtue of residing on the same platform. This creates a profound constitutional dilemma. On one hand, as courts extend their deference beyond the regulation of physical-layer infrastructure like Huawei to encompass content-layer platforms like TikTok, the constitutional stakes for free speech are significantly raised. Yet, because the platform's architecture does not allow for a neat separation between "national security-sensitive data" and "constitutionally-protected speech," the entire expressive ecosystem seems inevitably dragged into the orbit of national security exceptionalism. This overlap creates a uniquely high cost to judicial deference: When courts defer to the executive and legislature on data risks, they inadvertently grant the state a blank check to suppress a vast forum of public discourse.

This Article also highlights a consideration that receives less attention in free speech analysis. Speech is always mediated by the properties of its technological environment. While First Amendment doctrine does not distinguish among mediums, the national security risks associated with different mediums can differ substantially. The shifts from print to broadcast, from early internet forums to algorithmic curation, have altered not only the scale and speed of dissemination, but also the state's potential capacity to intervene. These differences in turn influence how free speech claims are weighed against national security concerns. In assessing both national security risks and judicial deference, we have to take into account how different mediums generate different national security vulnerabilities.

In TikTok's case, the algorithmic environment presents a more fragile and potentially far-reaching set of national security risks than those associated with earlier, more traditional mediums. As a result, security considerations may carry unprecedented weight when placed in tension with free speech.[15] This creates a paradoxical situation for the judiciary. While the national security risks associated with digital

14. *See infra* Section III.C.
15. *See infra* Section IV.B.

platforms have arguably undergone an upgrade, becoming more pervasive and sophisticated than those in the analog era, the question arises whether the legal standard for deference should likewise be heightened. If the Court adheres to its established frameworks of deference to Congress and does not ratchet up the level of deference to match these heightened risks, it actually constrains the executive's discretionary space. In doing so, it grants free speech interests a higher priority than they have traditionally enjoyed. TikTok therefore creates a quandary the doctrine has not previously confronted: Should judicial deference expand, in the face of heightened uncertainty and speculation surrounding national security risks, or narrow, when a law targets a medium that enables one of the most expressive and open technologies?

The "exception" in this Article's title carries a dual meaning. On one level, the TikTok ban exemplifies the persistence of foreign affairs exceptionalism, i.e., the longstanding judicial posture of deference to the political branches in matters of national security and foreign relations.[16] On another, TikTok stands as an exception to internet exceptionalism, i.e., the traditional notion that expressive platforms should remain insulated from governmental restrictions. By extending national security concerns to content governance, PAFACA makes TikTok the exception that unsettles established First Amendment doctrine and the traditional commitment to a free and open internet.

The Article unfolds in four parts. Following the Introduction, Part I examines the meteoric rise of TikTok and the national security controversies it has sparked within the evolving political and legislative landscape. It also discusses TikTok's failure to assuage deep-seated national security anxieties through expansive data privacy projects, resulting in the passage and implementation of PAFACA. Part II analyzes the potential impact of PAFACA and the TikTok ban on both TikTok and the United States. Part III then delves into the constitutional challenges against PAFACA in *TikTok v. Garland*. It focuses on three frameworks that predate the TikTok ban: the First Amendment doctrine as applied to content-neutral speech restrictions, the judicial deference given to predictive judgments of national security concerns, and the expanded use of predictive national security judgments for products manufactured in China. Together, these developments reveal how PAFACA and *TikTok v. Garland* extend these longstanding frameworks from the regulation of physical infrastructure to that of digital platforms. Part IV discusses the expanded posture of judicial deference and the narrowing of free speech in *TikTok v. Garland*, reflecting the judiciary's

16. *See infra* Section III.B.2.

attempt to accommodate the new national security risks associated with algorithmic recommendations. It cautions that extending the decision's logic beyond its context would risk normalizing broad governmental assertions of national security in situations where such exceptional circumstances are absent. The Article concludes by cautioning that TikTok is unlikely to be an endpoint in debates over whether predictive national security reasoning will be treated as sufficient to override the First Amendment interests of an expressive platform.

I. The Rise of TikTok and PAFACA

A. TikTok's Rise and Influence, and the National Security Concerns They Created

In 2017, the Chinese tech giant ByteDance acquired the renowned lip-syncing app Musical.ly and rebranded it as TikTok.[17] The app serves as a platform for various activities, ranging from sharing viral dances to political commentary.[18] TikTok skyrocketed in popularity, emerging as the dominant force in short-form video. With approximately 170 million American users, roughly half the nation's population,[19] it has firmly cemented its place in digital culture. Over one-third of young Americans rely on TikTok as a source of news,[20] and younger generations are even increasingly turning to TikTok for career guidance.[21] It has become deeply ingrained in people's daily lives, particularly for the content creators who depend on it as a primary source of income.

TikTok's prominence is closely tied to its recommendation system: By drawing on detailed behavioral signals ranging from viewing duration to patterns of engagement, the platform is able to construct individualized content streams with remarkable efficiency.[22]

---

17. *See, e.g.*, Bobby Allyn, *President Biden Signs Law to Ban TikTok Nationwide Unless It Is Sold*, NPR (Apr. 24, 2024), https://www.npr.org/2024/04/24/1246663779/biden-ban-tiktok-us [https://perma.cc/F75J-FHJ5].

18. Maheshwari & McCabe, *supra* note 2.

19. *Id.*

20. Emily Tomasik & Katerina Eva Matsa, *1 in 5 Americans Now Regularly Get News on TikTok, Up Sharply from 2020*, Pew Rsch. Ctr. (Sep. 25, 2025), https://www.pewresearch.org/short-reads/2023/11/15/more-americans-are-getting-news-on-tiktok-bucking-the-trend-seen-on-most-other-social-media-sites/ [https://perma.cc/9GW8-FUQA].

21. *For Gen-Z Job-Seekers, TikTok Is the New LinkedIn*, Economist (May 9, 2024), https://www.economist.com/business/2024/05/09/for-gen-z-job-seekers-tiktok-is-the-new-linkedin [https://perma.cc/7DYA-V26Z].

22. *See How TikTok Recommends Content*, TikTok Support, https://support.tiktok.com/en/using-tiktok/exploring-videos/how-tiktok-recommends-content [https://perma.cc/ZS5T-2WXK] (noting that user interactions, such as what content users watch in full or skip, influence what appears in their "For You" feed).

The opacity of the recommender system has been linked to concerns about user well-being from a consumer's perspective,[23] and it also has significant implications for American national security because of the possibility that TikTok's algorithm could be mobilized to serve foreign strategic interests.[24] Specifically, there is a concern that the Chinese government could exploit the app to spy on Americans or shape the content "U.S. users see on their TikTok feeds," a matter that gained heightened urgency in the 2024 election year.[25] There is no shortage of empirical studies suggesting a correlation between TikTok's content environment and the amplification of pro-China narratives.[26] Behavioral research has shown that users, particularly in politically sensitive regions like Taiwan,[27] are more likely to encounter TikTok content that aligns with Chinese state positions or minimizes perspectives critical of the Chinese government.[28] This pattern has raised concerns

23. Concerns about TikTok's recommender algorithm are increasingly supported by empirical evidence. *See* Ctr. for Countering Digit. Hate, Deadly by Design: TikTok Pushes Harmful Content Promoting Eating Disorders and Self-Harm into Young Users' Feeds 7 (2022) (finding that accounts registered as 13-year-olds were quickly saturated with videos related to eating disorders, body image issues, self-harm, and suicide); *Inside TikTok's Algorithm: A WSJ Video Investigation*, Wall St. J. (July 21, 2021), https://www.wsj.com/articles/inside-tiktoks-dangerous-algorithm-video-investigation-11626877477 [https://perma.cc/2WKR-3DKR] (revealing that TikTok's algorithm traps users in a "rabbit hole"). The State of North Carolina has also alleged that TikTok violated a state law prohibiting unfair or deceptive trade practices by employing numerous design features that exploit minors' developmental vulnerabilities to foster compulsive use. *See* State *ex rel*. Jackson v. TikTok Inc., No. 24CV032063-910, 2025 WL 2399525, at *7 (N.C. Super. Ct. Aug. 19, 2025).

24. Allyn, *supra* note 17; Johana Bhuiyan, *TikTok Has Become a Global Giant. The US Is Threatening to Rein It In*, Guardian (Oct. 31, 2022), https://www.theguardian.com/technology/2022/oct/30/tiktok-regulation-data-privacy-china [https://perma.cc/U39J-JRR3] (reporting that Senator Mark Warner claimed that access to "biometrics such as faceprints and voiceprints, poses a great risk to not only individual privacy but to national security.").

25. Allyn, *supra* note 17.

26. *See* Finkelstein et al., *supra* note 2, at 1 (identifying "a disproportionately high ratio of pro-CCP to anti-CCP content on TikTok"); Cole Henry Highhouse, *China Content on TikTok: The Influence of Social Media Videos on National Image*, 1 Online Media & Glob. Commc'n 697, 697 (2022) ("The most viewed China related TikToks portray the country and people in a largely positive or neutral tone.").

27. *See* Helen Davidson, *Frequent TikTok Users in Taiwan More Likely to Agree with Pro-China Narratives, Study Finds*, Guardian (June 6, 2025), https://www.theguardian.com/world/2025/jun/06/frequent-tiktok-users-in-taiwan-more-likely-to-agree-with-pro-china-narratives-study-finds [https://perma.cc/GW97-BHKL] ("The DoubleThink Lab report claimed the more active TikTok users showed stronger correlations with an openness to Chinese propaganda and the idea that [Taiwan's] unification with China is inevitable and democracy should be sacrificed for peace.").

28. Alicia Clanton & Aisha Counts, *TikTok Shows Less 'Anti-China' Content Than Rivals, Study Finds*, Bloomberg (Aug. 9, 2024), https://www.bloomberg.com/news/articles/2024-08-09/tiktok-shows-less-anti-china-content-than-rivals-study-finds

that TikTok may be using a combination of moderation practices and opaque algorithmic incentives to systematically shape what users see.[29] The concern is not merely that foreign influence is possible, but rather that it could be structurally baked into the platform's design, gradually shaping public opinion without users' awareness and selectively promoting geopolitical narratives that could alter public understanding in ways that implicate national security.

Beyond its algorithmic influence, the platform's sheer scale creates a data protection minefield. TikTok aggregates vast troves of granular personal data, from location history to behavioral patterns, at a depth and breadth unmatched by most U.S. platforms. Critics warn that because TikTok is owned by a Chinese parent company, this data stockpile could be subject to China's expansive national security and intelligence laws, whereby TikTok could be compelled to share this data with state authorities.[30] The sheer size and sensitivity of the data could render TikTok's data ecosystem an instrument for strategic profiling and surveillance of Americans.[31]

B. TikTok Bans Before PAFACA

The concerns about TikTok's national security risks did not emerge overnight; anxieties about the platform and its Chinese parent company,

---

[https://perma.cc/E45P-YJFJ] ("'What sets TikTok apart is that the accurate information about China's human rights abuses are most successfully crowded out on the platform,' says Joel Finkelstein, director and chief science officer of NCRI.")

29. *See* Anisha Kohli, *Why the FBI Is Concerned About TikTok*, TIME (Dec. 3, 2022, 3:42 PM), https://time.com/6238540/tiktok-fbi-security-concerns/ [https://perma.cc/L87Y-RXWK] (FBI Director Chris Wray "voiced similar concerns last month at a House Homeland Security Committee hearing, claiming that China's ruling Communist Party could use the app to push influence through TikTok's powerful recommendation algorithm and by collecting user data or controlling software for espionage purposes."); *see also* David Shepardson, *TikTok Will Go Dark in US Without Chinese Approval of Sale Deal, US Commerce Secretary Says*, REUTERS (July 24, 2025), https://www.reuters.com/business/media-telecom/tiktok-will-go-dark-us-without-chinese-approval-sale-deal-us-commerce-secretary-2025-07-24/ [https://perma.cc/2LSE-2NCJ] (U.S. Commerce Secretary Howard Lutnick, "speaking on CNBC, also said the United States must control the algorithm that makes the social media platform work.").

30. *Your Expert Guide to the Debate over Banning TikTok*, *supra* note 10 (observing that China's National Intelligence Law "give[s] the government broad leeway to potentially compel the company to grant it access to TikTok's data, including on Americans").

31. *See* James Andrew Lewis, *TikTok and National Security*, CSIS (Mar. 13, 2024), https://www.csis.org/analysis/tiktok-and-national-security [https://perma.cc/HL2W-KSU8] (emphasizing that even if there is no direct evidence of espionage, the platform could serve to "identify targets for recruitment" or support counterintelligence efforts by correlating TikTok data with other intelligence).

ByteDance, have gradually permeated U.S. national security discourse since 2019. The origins of PAFACA can be traced all the way back to the first Trump Administration when President Trump issued Executive Order 13873 under the International Emergency Economic Powers Act ("IEEPA") in May 2019.[32] Rather than targeting specific companies, the order gave the Secretary of Commerce general authority to prohibit information and communications technology transactions linked to "foreign adversaries" that posed "an undue risk" to national security.[33] The Department of Commerce subsequently issued implementing regulations in November 2019, laying out case-by-case review procedures to "identify, assess, and address" the critical infrastructure risks posed by foreign adversaries in information and communications technology transactions.[34] While TikTok was not mentioned by name in the 2019 order, the order and its implementing rules created a general toolbox for government intervention in digital transactions. Executive Order 13873 soon gave rise to a barrage of Trump-era executive orders aimed explicitly at Chinese applications, including TikTok.[35]

Around the same time, Senators Chuck Schumer and Tom Cotton jointly sent a letter to the Office of the Director of National Intelligence requesting an assessment of the national security risks posed by TikTok, explicitly describing it as a "potential counter-intelligence threat."[36] The Department of Defense followed suit and issued a cyber awareness message, warning that TikTok has "potential security risks associated with its use" and advising military personnel to uninstall the app from government-issued devices.[37]

Lawmakers also flagged ByteDance's 2017 acquisition of Musical.ly to the Committee on Foreign Investment in the United States ("CFIUS"), urging a review of whether the deal might provide

32. Exec. Order No. 13,873, 84 Fed. Reg. 22689 (May 15, 2019).

33. *Id.*

34. Securing the Information and Communications Technology and Services Supply Chain, 15 C.F.R. § 791 (2024).

35. *See, e.g.*, Exec. Order No. 13,942, 85 Fed. Reg. 48637 (Aug. 6, 2020) (addressing TikTok); Exec. Order No. 13,943, 85 Fed. Reg. 48641 (Aug. 6, 2020) (addressing WeChat); Exec. Order No. 13,971, 86 Fed. Reg. 1249 (Jan. 5, 2021) (addressing Alipay and other Chinese applications).

36. Adam Gabbatt, *TikTok App Poses Potential National Security Risk, Says Senior Democrat*, GUARDIAN (Oct. 24, 2019), https://www.theguardian.com/technology/2019/oct/24/tiktok-foreign-interference-chuck-schumer-tom-cotton [https://perma.cc/DZ99-VG4Y].

37. Matthew Cox, *Army Follows Pentagon Guidance, Bans Chinese-Owned TikTok App*, MILITARY.COM (Dec. 30, 2019), https://www.military.com/daily-news/2019/12/30/army-follows-pentagon-guidance-bans-chinese-owned-tiktok-app.html [https://perma.cc/94MT-M27T].

the Chinese government access to U.S. behavioral and device data.[38] As an administrative review mechanism, CFIUS typically addresses potential national security concerns posed by foreign acquisitions of U.S. businesses through negotiated mitigation agreements, though its determinations are ultimately binding.[39] CFIUS had two core concerns about TikTok. First, there was apprehension that ByteDance, as a Chinese-based parent company, could be subject to obligations under China's national security and cybersecurity laws, thereby rendering U.S. user data susceptible to extraterritorial government access.[40] Second, the platform's algorithmic architecture, combining sophisticated recommendation systems with the collection of U.S.-sourced behavioral and device data, could create opportunities for profiling, influence operations, or other foreign intelligence-related activities.[41] In August 2020, following CFIUS's determination that the acquisition posed national security risks, President Trump ordered ByteDance to divest TikTok's U.S. operations in August 2020,[42] but multiple federal courts issued preliminary injunctions that blocked immediate implementation of the order.[43]

The concerns about TikTok's national security risks persisted into the Biden Administration. Although then-President Biden revoked several Trump-era TikTok measures,[44] he implemented a more systematic "risk-based" approach to address the same concerns previously

38. *See generally* STEPHEN P. MULLIGAN, CONG. RSCH. SERV., LSB10940, RESTRICTING TIKTOK (PART I): LEGAL HISTORY AND BACKGROUND (2023) (describing the post-transaction investigation of ByteDance's acquisition of Musical.ly). CFIUS is an interagency body empowered under federal law to review foreign acquisitions of U.S. businesses for national security risks. *The Committee on Foreign Investment in the United States (CFIUS): CFIUS Overview*, U.S. DEP'T OF THE TREASURY, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-overview [https://perma.cc/6HTU-ZZEQ].

39. *See* Anupam Chander & Paul Schwartz, *The President's Authority over Cross-Border Data Flows*, 172 U. PA. L. REV. 1989, 2004–06 (2024) (describing CFIUS as an executive-branch mechanism focused on assessing and mitigating national security risks arising from foreign control of U.S. businesses).

40. *See* PETER J. BENSON, CLARE Y. CHO & MICHAEL D. SUTHERLAND, CONG. RSCH. SERV., R48023, TIKTOK: FREQUENTLY ASKED QUESTIONS AND ISSUES FOR CONGRESS 5–6 (2025) (listing numerous interrelated laws, economic security measures, and data restrictions in China which could influence ByteDance operations).

41. *Id.* at Summary.

42. *Id.* at 9 (detailing that, by August 2020, CFIUS recommended divestiture and the issuance of the presidential order).

43. *See e.g.*, TikTok Inc. v. Trump, 507 F. Supp. 3d 92 (D.D.C. 2020) (granting a preliminary injunction); Marland v. Trump, 498 F. Supp. 3d 624 (E.D. Pa. 2020) (same).

44. Exec. Order No. 14,034, 86 Fed. Reg. 31423 (June 9, 2021) (revoking three prior executive orders targeting Chinese applications, including EO 13942 (TikTok), EO 13943 (WeChat), and EO 13971 (Alipay and other apps)).

expressed by the Trump Administration. This new strategy emphasized the evaluation of sensitive data flows rather than the identification of specific companies.[45] At the same time, the Biden Administration engaged in extensive negotiations with TikTok, closely examining the inner workings of both TikTok's and ByteDance's operations.[46] Federal agencies devoted considerable resources to scrutinizing the companies. The Federal Bureau of Investigation and Department of Justice both conducted criminal investigations regarding breaches into U.S. journalists' location and contact data, and the Federal Trade Commission investigated potentially misleading practices regarding user data access.[47] Congress eventually codified this restriction through the No TikTok on Government Devices Act, which was incorporated into the Consolidated Appropriations Act of 2023, mandating the removal of TikTok from federal government devices and systems.[48] The U.S. government's broader data protection concerns were reinforced in December 2022 when ByteDance admitted that certain employees had improperly accessed the TikTok data of two U.S. journalists.[49]

State governments moved in parallel with the federal government. By early 2023, a broad swath of states had enacted prohibitions against TikTok on government-issued devices and networks.[50] Professors at public universities contested such a ban in Texas in 2023, arguing that

45. *See President Biden Amends Restrictions on Connected Software Applications Linked to Chinese Companies,* DAVIS POLK & WARDWELL LLP (June 14, 2021), https://www.davispolk.com/insights/client-update/president-biden-amends-restrictions-connected-software-applications-linked [https://perma.cc/6Z7Y-8KFG] ("Rather than targeting specific companies or applications, EO 14034 directs the Commerce Department to use existing authorities under another Trump administration executive order, EO 13873, to review and mitigate national security risks of transactions involving 'connected software applications.'").

46. Emily Baker-White, *Nine Things We Learned from TikTok's Lawsuit Against the US Government*, FORBES (May 8, 2024), https://www.forbes.com/sites/emilybaker-white/2024/05/08/nine-things-we-learned-from-tiktoks-lawsuit-against-the-us-government [https://perma.cc/3BRF-BGPM].

47. *Id.*

48. Consolidated Appropriations Act, 2023, Pub. L. No. 117-328, div. R, 136 Stat. 4459, 5258–59 (codified at 44 U.S.C. § 3553 note).

49. David Shepardson, *ByteDance Finds Employees Obtained TikTok User Data of Two Journalists*, REUTERS (Dec. 22, 2022), https://www.reuters.com/technology/bytedance-finds-employees-obtained-tiktok-user-data-two-journalists-2022-12-22/ [https://perma.cc/PV8S-BLK7].

50. Sapna Maheshwari, Cecilia Kang & David McCabe, *Bans on TikTok Gain Momentum in Washington and States*, N.Y. TIMES (Dec. 20, 2022), https://www.nytimes.com/2022/12/20/technology/tiktok-ban-government.html [https://perma.cc/LPV2-CMVM] (indicating that, by the end of 2022, at least 14 states had banned TikTok on government-issued devices).

it hindered their ability to conduct research on the app.[51] Nonetheless, a federal judge upheld Texas's ban, deeming it a "reasonable restriction" considering Texas's concerns and the ban's limited impact, which only affected state employees.[52] Montana took an unprecedented step by attempting to ban TikTok in the state.[53] However, this effort proved unsuccessful after a court found that the ban impermissibly burdened expressive activity protected by the First Amendment.[54]

C. Beyond Platform Promises: The Persistent Perception of TikTok's National Security Risk

Amidst federal and state government actions imposing or threatening varying degrees of restriction on TikTok, the platform sought to reassure both the public and the government of its commitment to data security through implementing privacy safeguards and corporate compliance measures. Despite these endeavors and evidence that TikTok's privacy practices matched or exceeded those of other platforms, U.S. officials continued to have apprehensions about TikTok's national security risks and pressed for divestiture.[55] Therefore, TikTok's predicament cannot be understood as a problem of inadequate privacy safeguards or insufficient corporate compliance. It instead arises from a deeper geopolitical distrust of China's legal and institutional framework. The concerns about TikTok are anchored in the structural premise that any Chinese company ultimately remains subject to state authority. In this context, even TikTok's most elaborate institutional fixes are not enough to overcome the entrenched perception that Chinese law offers few meaningful transparent or reliable avenues of redress.

It would be misguided to assume that TikTok remains unaware that the suspicions it faces in the United States is not merely a matter

51. *Federal Judge Upholds Texas' TikTok Ban on State-Owned Devices*, Associated Press (Dec. 12, 2023), https://apnews.com/article/texas-tiktok-ban-lawsuit-first-amendment-c71e03601bb1ba60ef7465b4526532dd [https://perma.cc/86E3-D2T3] (describing that the lawsuit, filed by the Knight First Amendment Institute at Columbia University, claimed the prohibition "imped[ed] academic freedom and compromise[ed] the ability of professors to teach and do research about the social media app").

52. *Id.* (stating that Judge Pitman described the measure as "a reasonable restriction on access to TikTok in light of Texas's concerns").

53. S.B. 419, 68th Leg., Reg. Sess. (Mont. 2023).

54. *See* TikTok Inc. v. Knudsen, Nos. CV-23-56-M-DWM, CV-23-61-M-DWM, slip op. (D. Mont. Nov. 30, 2023) (granting preliminary injunction against Montana's TikTok ban for violating the First Amendment).

55. *See, e.g.*, Justin Hendrix, *Transcript: TikTok CEO Testifies to Congress,* Tech. Pol'y (Mar. 24, 2024) https://www.techpolicy.press/transcript-tiktok-ceo-testifies-to-congress/ [https://perma.cc/B5RA-Q7DW] (documenting that Rep. Cathy McMorris Rogers, chair of the House Energy and Commerce Committee, viewed Project Texas as a "marketing scheme").

of technical privacy safeguards. From its initial interaction with CFIUS, TikTok has floated a series of compromises—as far-reaching as proposing an independent U.S. board, Oracle-operated gateways, or even a government "kill switch"—to address the structural concerns about ByteDance's ownership and the reach of Chinese law.[56] It also undertook a bold, if not unprecedented, institutional response: The creation of the TikTok U.S. Data Security Inc. entity.[57]

1. TikTok's Expansive Data Privacy Projects

It is tempting to think that better privacy infrastructure makes for better data security. TikTok has invested heavily in this premise. In 2022, TikTok established a dedicated U.S.-based company, TikTok U.S. Data Security Inc. ("USDS"), which is staffed by over 2,000 U.S.-based employees and operates on the cloud infrastructure of the American company Oracle.[58] The creation of this separate entity is part of "Project Texas," an initiative intended to bolster data security and enhance transparency surrounding the information collected from U.S. users.[59] Project Texas was developed by ByteDance as a mitigation proposal during its negotiations with CFIUS, intended to address the Committee's national security concerns without requiring divestiture.[60] TikTok and ByteDance claim that they have poured over $2 billion into Project Texas.[61]

More than a technical firewall, USDS is constructed as a stand-alone corporate entity that oversees data security operations, is staffed under U.S. control, and is entrusted with the exclusive governance of

56. Drew Harwell, *TikTok Offered an Extraordinary Deal. The U.S. Government Took a Pass*., Wash. Post (May 29, 2024), https://www.washingtonpost.com/technology/2024/05/29/tiktok-cfius-proposal-rejected/ [https://perma.cc/B2SS-K7YR] (summarizing TikTok's 2022 offer to CFIUS, which included allowing federal officials to select its U.S. board of directors, granting the government veto power over each new hire, contracting a Department of Defense vendor to monitor its source code, and even providing a government-controlled "kill switch" to shut down the app if deemed necessary).

57. *See What is USDS and How is it Governed?*, TikTok USDS, https://usds.tiktok.com/what-is-usds [https://perma.cc/K4AU-DZP4] (describing that the company created a new entity, USDS, "tasked with managing all business functions that require access to U.S. user data identified by the U.S. government as needing additional protection").

58. *Facts Matter: How TikTok Protects U.S. User Data*, TikTok (Feb. 7, 2025), https://newsroom.tiktok.com/facts-matter-how-tiktok-protects-us-user-data [https://perma.cc/6QZH-SGFZ].

59. *See* David Ingram, *TikTok Tries to Sell 'Project Texas' as It Fights for Survival in the U.S.*, NBC News (Jan. 26, 2023), https://www.nbcnews.com/tech/security/tiktok-tries-sell-project-texas-fights-survival-us-rcna67697 [https://perma.cc/SVS8-HWPG]

60. Harwell, *supra* note 56.

61. Baker-White, *supra* note 46.

U.S. user data and access protocols.[62] It aims to construct a sovereign trust architecture to demonstrate that data concerning U.S. citizens will remain under U.S. jurisdiction and control, preempting unauthorized foreign access to both user data and the recommendation algorithms that drive content delivery.[63]

Unlike conventional data governance systems, USDS is an independent corporate structure, legally and operationally separate from ByteDance.[64] Under the terms of TikTok's mitigation agreement with CFIUS, USDS is subject to restrictions on personnel, such as limiting employment to U.S. citizens or lawful permanent residents.[65] Few, if any, private enterprises would emphasize that they hire Americans as a point of pride. USDS, however, was proudly launched on TikTok's official website in a two-minute video, during which TikTok emphasized multiple times that USDS employees and board members are American citizens.[66] This striking emphasis on its employees' national origin signals TikTok's willingness to offer regulatory reassurance.

According to TikTok's own statements, "[a]s of June 2022, 100% of U.S. user traffic is routed to Oracle and USDS infrastructure in the United States," and "all access to that environment is managed exclusively by TikTok U.S. Data Security, a team led by Americans, in America."[67] The performative patriotism of USDS goes even further. According to the D.C. Circuit, "[t]he key management personnel of TTUSDS were to be subject to approval by the Government."[68]

TikTok's establishment of USDS is an institutional anomaly. No other entertainment or social media platform of comparable scale has,

62. *See Who Has Access to U.S. User Data?*, TikTok USDS, https://usds.tiktok.com/who-has-access-to-u-s-user-data [https://perma.cc/Y5TC-V7EG] (pointing out that "only vetted employees of TikTok USDS have access to new U.S. user data").

63. Echo Wang & David Shepardson, *Exclusive: TikTok Steps Up Efforts to Clinch U.S. Security Deal*, Reuters (Dec. 22, 2022), https://www.reuters.com/technology/tiktok-steps-up-efforts-clinch-us-security-deal-2022-12-22/ [https://perma.cc/HVW5-93BU].

64. *What is USDS and How is it Governed?*, *supra* note 57 ("TikTok USDS will be overseen by an independent board of directors, each with strong backgrounds in U.S. national and cyber security. USDS leads will report directly to this board, and there will be no reporting lines outside of it.").

65. Matt Perault, *Has TikTok Implemented Project Texas?*, Lawfare (May 10, 2024), https://www.lawfaremedia.org/article/has-tiktok-implemented-project-texas [https://perma.cc/K4EF-WMFF].

66. *About USDS*, TikTok USDS, https://usds.tiktok.com/ [https://perma.cc/86MV-4QZA].

67. *Myths vs. Facts*, TikTok USDS, https://usds.tiktok.com/usds-myths-vs-facts [https://perma.cc/J7E2-GKFU].

68. TikTok Inc. v. Garland, 122 F.4th 930, 943 (D.C. Cir. 2024).

to date, undertaken a similar experiment in national data sequestration. TikTok has characterized the system as "truly the first of its kind."[69]

Yet, this extensive effort by TikTok to demonstrate its commitment to data privacy has done little to alter the tenor of the political debate. Not only did CFIUS cease meaningful engagement with Project Texas, but the government to whom these elaborate gestures of accommodation were made remained unmoved.[70] As the D.C. Circuit noted in its *TikTok v. Garland* decision, the Executive Branch found TikTok's proposed mitigation measures insufficient.[71] However, ByteDance still "voluntarily" retained some elements of the plan.[72] This can be understood as a strategic choice: By preserving components of Project Texas and USDS, TikTok sought to signal continued willingness to accommodate U.S. national security concerns and to project itself as a cooperative stakeholder, rather than an adversarial foreign actor.

TikTok has made several other visible efforts to demonstrate compliance with privacy norms, both in the United States and abroad. It inaugurated a Transparency and Accountability Center in Los Angeles, California, where regulators and scholars can inspect its content moderation and security systems first hand.[73] It also established regional transparency and compliance centers in South America and Europe.[74] Additionally, TikTok sought to replicate its USDS strategy in Europe with "Project Clover," which promised to build local data centers to

69. *About USDS*, *supra* note 66 ("This data management and security system is truly the first of its kind.").

70. Harwell, *supra* note 56 (reporting that TikTok submitted the proposal in August 2022, but "CFIUS without explanation stopped engaging," and that the companies "repeatedly asked why discussions had ended and how they might be restarted, but they did not receive a substantive response"); BENSON, CHO & SUTHERLAND, *supra* note 40 ("Several experts and Members of Congress contend that even if Project Texas were to be fully implemented, it would not address the core problem of ByteDance employee access to U.S. user data.").

71. TikTok Inc. v. Garland, 122 F.4th 930, 943–44 (D.C. Cir. 2024).

72. *Id.* at 944.

73. Alex Heath, *TikTok's Transparency Theater*, VERGE (Feb. 2, 2023), https://www.theverge.com/2023/2/2/23583853/tiktok-transparency-center-visit [https://perma.cc/9SHQ-ZUMN].

74. *Project Clover: €1 Billion Investment in Finland for New Data Center*, TIKTOK (May 6, 2025), https://newsroom.tiktok.com/finlanddatacenter [https://perma.cc/WCW9-WLZ4]; *Brazil to Begin Construction on TikTok Data Center in Six Months, Minister Says*, REUTERS (Oct. 10, 2025), https://www.reuters.com/technology/brazil-begin-construction-tiktok-data-center-six-months-minister-says-2025-10-10/ [https://perma.cc/7CEG-RUZF]; *TikTok to Open Two New Data Centers in Europe*, IAPP (Feb. 22, 2023), https://iapp.org/news/b/tiktok-to-open-two-new-data-centers-in-europe [https://perma.cc/4TU5-TGHG].

localize user data within the EU.[75] Project Clover has deployed three data centers across Europe.[76] TikTok also has published semi-annual transparency reports since 2019.[77]

While skepticism remains about the efficacy of these measures,[78] particularly in context of China's legal environment, the scale and formality of TikTok's internal compliance architecture is at least comparable to, and in some respects exceeds, that of its peers. For instance, Citizen Lab at the University of Toronto found that TikTok largely adheres to international industry norms, with no significant deviations in privacy, security, or censorship compared to competitors like Facebook.[79] GLAAD's 2025 index finds that TikTok outperforms peers like Meta and YouTube in maintaining stronger and more explicit protections for LGBTQ users, including detailed enforcement guidelines and bans on conversion therapy, while competitors have weakened their hate speech policies.[80] TikTok's privacy safeguards also embody comparatively higher standards of governance, distinguishing it from

75. *Project Clover One Year On*, TikTok (Feb. 23, 2024), https://newsroom.tiktok.com/project-clover-one-year-on?lang=en-150 [https://perma.cc/53QZ-H8A5].

76. Paul Sawers, *With Project Clover, TikTok Touts New EU Data Privacy and Security Efforts*, TechCrunch (Mar. 8, 2023), https://techcrunch.com/2023/03/08/with-project-clover-tiktok-touts-new-eu-data-privacy-and-security-efforts/ [https://perma.cc/GS8P-3ADG] (noting that TikTok plans to open three data centers across Europe, with two located in Ireland and one in Norway).

77. Spandana Singh & Leila Doty, *The Transparency Report Tracking Tool: How Internet Platforms Are Reporting on the Enforcement of Their Content Rules*, New Am. (Dec. 9, 2021), https://www.newamerica.org/oti/reports/transparency-report-tracking-tool/ [https://perma.cc/8796-XG4T] (explaining that TikTok's transparency reports track how the platform enforces its content rules, such as the number of videos removed, appeal outcomes, spam and fake account removals, and responses to COVID-19 and election misinformation, without breaking data down by content category).

78. Drew Harwell, *A Former TikTok Employee Tells Congress the App Is Lying About Chinese Spying*, Wash. Post (Mar. 10, 2023), https://www.washingtonpost.com/technology/2023/03/10/tiktok-data-whistleblower-congress-investigators/ [https://perma.cc/J3RT-QZDD] (A former TikTok Trust and Safety employee "told congressional investigators that Project Texas does not go far enough and that a truly leakproof arrangement for Americans' data would require a 'complete re-engineering' of how TikTok is run.").

79. Pellaeon Lin, *TikTok vs Douyin: A Security and Privacy Analysis*, Citizen Lab (Mar. 22, 2021), https://citizenlab.ca/2021/03/tiktok-vs-douyin-security-privacy-analysis/ [https://perma.cc/N7BE-J45V].

80. Justin Hendrix, *TikTok Leads Dismal Pack in LGBTQ Social Media Safety Rankings*, Tech Pol'y (May 18, 2025), https://www.techpolicy.press/tiktok-leads-dismal-pack-in-lgbtq-social-media-safety-rankings/ [https://perma.cc/CD3C-9UL8] (reporting that, "[a]ccording to GLAAD, TikTok scores relatively better than other platforms because it offers the strongest protections for LGBTQ users among major platforms, with clear policies against hate, harassment, misgendering, and deadnaming," while "social media platforms like Meta and YouTube are rolling back hate speech policies").

other widely used Chinese applications.[81] Furthermore, TikTok claims that Congress has not presented any evidence indicating that TikTok spreads foreign propaganda or poses the types of data security risks that "could conceivably justify" the law and has failed to demonstrate that the app specifically causes harm in these domains.[82] Overall, the available evidence does not support the view that TikTok lags behind other firms in privacy investment or institutional design.

Although TikTok has attracted regulatory scrutiny for its data practices in the United States and abroad, its record does not, in quantitative terms, deviate sharply from that of other technology companies. In 2023, TikTok was fined €345 million under the European Union's ("EU") General Data Protection Regulation ("GDPR") for mishandling children's data,[83] and in 2025, the Irish Data Protection Commission imposed an additional €530 million penalty related to unlawful cross-border transfers to China.[84] These fines, although substantial, are not anomalous. Meta was fined €1.2 billion in 2023 for similar cross-border data transmission violations.[85] Amazon was found to have engaged in impermissible behavioral advertising and was fined €746 million in 2021.[86] Google has reached cumulative settlements exceeding $1 billion just in the state of Texas over invasive geolocation, private search, and biometric data practices.[87]

---

81. *See* Lianrui Jia & Lu Ruan, *Going Global: Comparing Chinese Mobile Applications' Data and User Privacy Governance at Home and Abroad*, INTERNET POL'Y REV., Sep. 16, 2020, at 14 (noting that the international-facing TikTok provides relatively higher levels of data protection (especially in the EU) compared to its Chinese-facing counterpart, Douyin).

82. *See* Petition for Review of Constitutionality of the Protecting Americans from Foreign Adversary Controlled Applications Act at 40–41, TikTok Inc. v. Garland, 122 F.4th 930 (D.C. Cir. 2024) (No. 24-1113) [hereinafter Petition for Review].

83. Tom Gerken & Liv McMahon, *TikTok Fined €345m over Children's Data Privacy*, BBC NEWS (Sep. 15, 2023), https://www.bbc.com/news/technology-66819174 [https://perma.cc/9LVD-4UG8].

84. Adam Satariano, *TikTok Fined $600 Million for Sending European User Data to China*, N.Y. TIMES (May 2, 2025), https://www.nytimes.com/2025/05/02/business/tiktok-eu-data-china.html [https://perma.cc/HB98-SEML].

85. Natasha Lomas, *Meta Ordered to Suspend Facebook EU Data Flows as It's Hit with Record €1.2BN Privacy Fine Under GDPR*, TECHCRUNCH (May 22, 2023), https://techcrunch.com/2023/05/22/facebook-eu-us-data-flows-decision/ [https://perma.cc/7RBD-Z3S4].

86. Sam Schechner, *Amazon Hit with Record EU Privacy Fine*, WALL ST. J. (July 30, 2021), https://www.wsj.com/tech/amazon-hit-with-record-eu-privacy-fine-11627646144 [https://perma.cc/AF2K-8SET].

87. Anthony Ha, *Google Will Pay Texas $1.4B to Settle Privacy Lawsuits*, TECHCRUNCH (May 10, 2025), https://techcrunch.com/2025/05/10/google-will-pay-texas-1-4-billion-to-settle-privacy-lawsuits/ [https://perma.cc/8YUV-EFES].

From the standpoint of the average user, there is also little reason to believe that personal data is better protected in the hands of one global platform than another.[88] Compliance failures, whether involving location tracking,[89] biometric identifiers,[90] or unauthorized sharing,[91] are not unique to any single platform.

In practice, TikTok's actual privacy practices are not demonstrably inferior to those of its competitors. Two factors contribute to this outcome. First, large firms tend to maintain extensive compliance infrastructures.[92] Measured against its peers, TikTok's data security investments are of a comparable, if not greater, scale. Meta claimed that, between 2019 and 2025, it invested over $8 billion in overhauling its privacy programs for products like Facebook and Instagram,[93] whereas TikTok's Project Clover initiative in Europe alone cost €12 billion.[94] Second, TikTok, as a Chinese-owned company operating around the world, is subject to overlapping regulatory demands, including those of the United States and the European Union.[95] Unlike Meta, which

88. Colleen McClain et al., *How Americans View Data Privacy,* Pew Rsch. Ctr. (Oct. 18, 2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/ [https://perma.cc/VA2J-9VT9] (reporting that 77% of Americans have little or no trust in leaders of social media companies to publicly admit mistakes and take responsibility for data misuse and that 76% have little or no trust that such leaders will not sell users' personal data to other companies without user consent).

89. Johana Bhuiyan, *Google to Pay $93m in Settlement over Deceptive Location Tracking*, Guardian (Sep. 14, 2023), https://www.theguardian.com/technology/2023/sep/14/google-location-tracking-data-settlement [https://perma.cc/5XGD-S99E] (reporting that Google continued to collect and store users' location data even after they turned off location history, misleading consumers about their ability to opt out).

90. Ravie Lakshmanan, *Meta Settles for $1.4 Billion with Texas over Illegal Biometric Data Collection*, Hacker News (July 31, 2024), https://thehackernews.com/2024/07/meta-settles-for-14-billion-with-texas.html [https://perma.cc/44RR-5UWE] (detailing how Meta was accused of illegally collecting Texans' facial recognition and other biometric data without proper consent).

91. Ivan Mehta, *Facebook Again Admits to Wrongly Sharing User Data with Third-Party Apps*, Next Web (July 2, 2020), https://thenextweb.com/news/facebook-again-admits-to-wrongly-sharing-user-data-with-third-party-apps [https://perma.cc/88TN-VFDG].

92. *See generally* Robert C. Bird & Stephen Kim Park, *Turning Corporate Compliance into Competitive Advantage*, 19 U. Pa. J. Bus. L. 285 (2017) (explaining that large corporations' ability to build robust compliance structures becomes a barrier to entry or a source of competitive advantage).

93. *See* Michel Protti, *Reflecting on Meta's $8 Billion Investment in Privacy*, Meta Newsroom (Jan. 28, 2025), https://about.fb.com/news/2025/01/meta-8-billion-investment-privacy [https://perma.cc/MZY7-LFXA] (introducing that, from 2019 to 2025, Meta has invested more than $8 billion into overhauling its privacy program).

94. *Project Clover One Year On*, *supra* note 75 ("Project Clover represents a €12 billion investment in European data security from TikTok over the next ten years.").

95. Meaghan Tobin, *TikTok Is Facing Legal Backlash Around the World*, N.Y. Times (Jan. 9, 2025), https://www.nytimes.com/2025/01/09/technology/tiktok-ban-global-legal-battles.html [https://perma.cc/SPM8-9ZWW] (noting that TikTok

faces no obligation to accommodate Chinese rules, TikTok is subject to a heightened level of compliance pressure from Chinese and Western authorities' overlapping regulatory expectations.[96] Although a platform being subject to a greater number of jurisdictions' regulations does not necessarily entail stricter privacy compliance,[97] exposure to multiple regulatory regimes may, in certain contexts, lead platforms to adopt more stringent practices, which could advance consumer interests. For instance, data subjects' rights to disclosure illustrate the different levels of protection across jurisdictions. Under both the EU's GDPR and the California Privacy Rights Act of 2020, a data controller satisfies "the right to know" by informing individuals of the categories of recipients to whom personal information is disclosed, without identifying each recipient in detail.[98] By contrast, China's Personal Information Protection Law requires a higher level of specificity in disclosures: The data controller is required to disclose the actual identity and contact information of each data recipient.[99] If TikTok were in fact required to comply with Chinese law, such compliance would enhance consumer data protection, since it provides a degree of transparency about data processors that goes beyond what is guaranteed under U.S. or even European law.

But it is not difficult to see why TikTok's extensive efforts have yielded little traction. A platform's internal privacy standards cannot neutralize national security concerns attached to the data itself. Even with a sophisticated and technically superior privacy infrastructure, a platform remains powerless if the host state mandates the surrender

---

is facing total bans in India and Nepal and "fines and forced local tie-ups" in Russia and Indonesia).

96. *Id.* (describing how governments across the world, including Russia, Albania, the United States, India, Indonesia, Canada, and the European Union, have imposed fines, bans, and other regulatory measures on TikTok).

97. This is especially evident among national security regulations. For instance, the U.S. CLOUD Act obligates American companies to disclose data to U.S. law-enforcement authorities regardless of whether the data is located within or outside of the United States, *see* 18 U.S.C. § 2713, while China's Cybersecurity Law imposes data-localization requirements for certain categories of personal information and "important data," mandating that such data be stored domestically and allowing cross-border transfer only after undergoing government-organized security assessments. Zhonghua Renmin Gongheguo Wangluo Anquan Fa (中华人民共和国网络安全法) [Cybersecurity Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., November 7, 2016, effective June 1, 2017) arts. 37–39 [hereinafter China's Cybersecurity Law].

98. Council Regulation 2016/679, art. 15(1)(c), 2016 O.J. (L 119) 51; CAL. CIV. CODE §§ 1798.110(c)(1), 1798.115(c).

99. Zhonghua Renmin Gongheguo Geren Xinxi Baohu Fa (中华人民共和国个人信息保护法) [Personal Information Protection Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2021) art. 17.

of user data under national security laws. Increasingly, data privacy no longer functions solely as a safeguard for individuals against state overreach. It has also acquired the characteristics of a national security tool,[100] especially in light of data's ability to expose underlying patterns in a nation's socioeconomic dynamics and industrial workflows. A study by Didi's Research Institute, for instance, showed that traffic flows around central government buildings mapped directly onto the overtime schedules of key ministries, most notably China's Ministry of Public Security and Ministry of Natural Resources during hot summer nights.[101] What seems like innocuous mobility data thus acquires the quality of an institutional X-ray that exposes the operational details of government entities. Thus, beyond protecting individuals' privacy, data regulation also safeguards the informational autonomy of a country against the extractive capacities of foreign states.

2. *Unequal Geopolitical Trust Despite Shared National Security Concerns: An EU-Based Comparison of U.S. and Chinese Data Regimes*

TikTok's efforts to bolster user data protections through architectural redesigns and arguably some of the most robust compliance initiatives in the industry hardly addressed the question of governmental access.[102] TikTok's data compliance leaves untouched the institutional dynamics that fueled the distrust in the first place. After all, no amount of technical safeguards or encryption protocols can compensate for a company's lack of independence to refuse state demands for data.

At the heart of the U.S. government's concerns about TikTok lies a set of suspicions that ByteDance, TikTok's Chinese parent company, sits within the jurisdictional reach of a foreign adversary; that Chinese law compels corporate cooperation with state intelligence efforts; and that, as long as TikTok's core algorithmic infrastructure and decision-making authority remain tethered to ByteDance and the Chinese government,

100. *See generally* Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 Emory L.J. 677 (2015) (illustrating the shift of "international Internet regulation from efforts to prevent data from flowing in to a country through censorship, to include efforts to prevent data from flowing out through data localization").

101. Tōng guò dà shù jù jiān cè guó jiā gè bù wěi chū xíng guī lǜ, gōng ān bù zuì máng zhōng jì wěi zuì dī diào. (通过大数据监测国家各部委出行规律, 公安部最忙中纪委最低调) [*Monitoring Travel Patterns of Various National Ministries and Commissions Through Big Data*], China Digit. Times (July 7, 2015) https://chinadigitaltimes.net/chinese/667978.html [https://perma.cc/5SU5-MD9P].

102. *See supra* Section I.C.1.

its assurances of independence ring hollow.[103] The fear lies less in any demonstrated weaponization of TikTok's data or content flows than in the possibility that it *could* be so deployed, which renders the platform a latent instrument of foreign influence.

Regulatory findings abroad lend further weight to the U.S. government's concerns. In May 2025, the Irish Data Protection Commission ("DPC") imposed an administrative fine of €530 million on TikTok.[104] Central to this decision were the determinations that remote access by employees in China constitutes a form of data transfer to a third country and that TikTok had neither adequately assessed nor demonstrated that Chinese law affords protections comparable to those guaranteed within the EU.[105] Crucially, the DPC found that TikTok had not adequately assessed the potential legal conflicts posed by China's Counter-Espionage Law,[106] Cybersecurity Law,[107] National Intelligence Law,[108] and Counter-Terrorism Law[109]—all statutes that authorize

103. *See, e.g.*, TikTok Inc. v. Garland, 604 U.S. 56, 63–64 (2025) (per curiam) (noting ByteDance is "subject to Chinese laws requiring it to 'assist or cooperate'" with state intelligence efforts and to provide the Chinese government "the power to access and control private data").

104. Satariano, *supra* note 84.

105. *Irish Data Protection Commission Fines TikTok €530 Million and Orders Corrective Measures Following Inquiry into Platform Settings and Transparency Information for Child Users*, Irish Data Prot. Comm'n (May 2, 2025), https://www.dataprotection.ie/en/news-media/latest-news/irish-data-protection-commission-fines-tiktok-eu530-million-and-orders-corrective-measures-following [https://perma.cc/9DAR-UK6L].

106. Zhonghua Renmin Gongheguo Fanjiandie Fa (中华人民共和国反间谍法) [Counter-Espionage Law] (promulgated by the Standing Comm. Nat'l People's Cong., Apr. 26, 2023, effective July 1, 2023), art. 41 (When conducting investigations into espionage activities in accordance with the law, state security organs may require postal, courier, and other logistics operators, as well as telecommunications and internet service providers, to provide necessary support and assistance.).

107. China's Cybersecurity Law, *supra* note 97, at art. 28 (imposes a duty on network operators to provide technical support and assistance to public security and state security agencies engaged in criminal investigations or activities related to safeguarding national security).

108. Zhonghua Renmin Gongheguo Guojia Qingbao Fa (中华人民共和国国家情报法) [National Intelligence Law] (promulgated by the Standing Comm. Nat'l People's Cong., June 27, 2017, effective June 28, 2017), arts. 7, 14, 16, (authorizes intelligence organs to request support, assistance, and cooperation from both organizations and individuals in the conduct of intelligence work and permits intelligence personnel to access restricted areas, request information from entities and individuals, and examine or retrieve documents, materials, and objects deemed relevant).

109. Zhonghua Renmin Gongheguo Fankongbu Zhuyi Fa (中华人民共和国反恐怖主义法) [Counter-Terrorism Law] (promulgated by the Standing Comm. Nat'l People's Cong., Dec. 27, 2015, effective Jan. 1, 2016), art. 51 (empowers public security authorities, when investigating suspected terrorist activity, to collect and obtain relevant information and materials from any individual or organization, with a mandatory obligation to comply).

state access to data without meaningful procedural safeguards.[110] The DPC found these statutes to be incompatible with Article 46(1) of the GDPR, as they mandate remote state access to data in a manner that fundamentally conflicts with the level of data protection guaranteed within the EU.[111] This enforcement action also underscores the systemic nature of concerns about TikTok, specifically the structural lack of limits, transparency, and redress mechanisms in the Chinese legal regime. More broadly, European regulators have withheld recognition of China's adequacy agreement under GDPR, denying that China is eligible for data transfers with the EU.[112]

This skepticism towards China's data laws is also reflected in broader institutional actions. In early 2025, multiple European research funding agencies, including those in Germany, Sweden, and Switzerland, suspended cooperation with Chinese partners over concerns that China's Data Security Law creates legal uncertainty for foreign collaborators.[113] A 2021 assessment by the European Union Institute for Security Studies warned that China's "security-centered" model of cyberspace governance presents a multifaceted risk to EU citizens, business operations, and cross-border data flows.[114] The European Parliament has repeatedly voiced concern that China's approach to AI and social credit systems is inconsistent with fundamental rights protections and democratic accountability.[115]

---

110. *See, e.g.*, Jyh-An Lee, *Hacking into China's Cybersecurity Law*, 53 WAKE FOREST L. REV. 57, 83–86, 99–102 (2018).

111. *Irish Data Protection Commission Fines TikTok €530 Million . . . , supra* note 105.

112. Samm Sacks & Justin Sherman, *The Global Data War Heats Up*, ATLANTIC (June 26, 2019), https://www.theatlantic.com/international/archive/2019/06/g20-data/592606/ [https://perma.cc/X6LH-RSR7] ("EU officials have indicated that China may never be eligible for a legal arrangement under the General Data Protection Regulation (GDPR) called an 'adequacy agreement,' which would allow for data exchange with the EU.").

113. Andrew Silver, *China's Data Protection Rules Prompt Pause by Major European Research Funders*, REUTERS (Apr. 25, 2025), https://www.reuters.com/sustainability/society-equity/chinas-data-protection-rules-prompt-pause-major-european-research-funders-2025-04-25/ [https://perma.cc/T8PK-U8NE].

114. *See* CAMILLE BOULLENOIS, EUR. UNION INST. FOR SEC. STUD., CHINA'S DATA STRATEGY: CREATING A STATE-LED MARKET 2 (2021) ("China's data strategy creates risks of abusive data collection on EU nationals and companies and challenges the European Union's strong emphasis on individual data rights.").

115. *See* ULRIKE FRANKE, EUR. PARLIAMENT POL'Y DEP'T. FOR ECON., SCI. & QUALITY OF LIFE POL'YS, ARTIFICIAL INTELLIGENCE DIPLOMACY 17 (2021) ("Elsewhere in China, the idea of a social credit score had been tested, a 'pervasive, highly intrusive AI-enabled surveillance system that tracks you all day every day and that largely determines all of your life chances.'").

But the problem is not unique to China or TikTok. The United States, too, has faced doubts about whether its national security laws hinder an adequate level of protection for EU data. The EU-U.S. partnership has weathered similar privacy challenges because of U.S. surveillance statutes, such as Foreign Intelligence Surveillance Act ("FISA") §702 and Executive Order 12333.[116] The EU Court of Justice ("CJEU") has twice invalidated U.S.-EU data transfer agreements (Safe Harbor and Privacy Shield), first in *Schrems I* in 2015 and then again in *Schrems II* in 2020, due to the reach of these surveillance laws.[117]

The U.S. has sought to mitigate these concerns by introducing new redress mechanisms and limiting executive discretion via executive orders.[118] In 2022, then-President Biden issued an executive order creating the Data Protection Review Court, an independent redress mechanism designed to address complaints from EU residents.[119] In 2023, the European Commission adopted a new adequacy decision for the EU-U.S. Data Privacy Framework, recognizing the Executive Order on "Enhancing Safeguards for United States Signals Intelligence Activities," describing it as an improvement that "addresses the concerns raised by the Court of Justice of the European Union."[120]

---

116. Nigel Cory, Daniel Castro & Ellysse Dick, *'Schrems II': What Invalidating the EU-U.S. Privacy Shield Means for Transatlantic Trade and Innovation*, Info. Tech. & Innovation Found. (Dec. 3, 2020), https://itif.org/publications/2020/12/03/schrems-ii-what-invalidating-eu-us-privacy-shield-means-transatlantic [https://perma.cc/DUK2-GRJE] ("Specifically, the court identified Section 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333, which allow U.S. intelligence agencies to collect data on foreign nationals, as inconsistent with rights guaranteed in the EU Charter.").

117. Case C-362/14, Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650, ¶ 94 (Oct. 6, 2015) ("[L]egislation permitting the public authorities to have access on a generalized basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life."); Case C-311/18, Data Prot. Comm'r v. Facebook Ir., ECLI:EU:C:2020:559, ¶ 156 (July 16, 2020) ("[T]he US legislation governing the access to personal data transferred under that privacy shield and the use of that data by the public authorities of that third country for national security, law enforcement and other public interest purposes does not ensure an adequate level of protection.").

118. *See, e.g.*, *Fact Sheet: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework*, The White House (Oct. 7, 2022), https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/ [https://perma.cc/8A6J-B2QP].

119. *Id.*; *see, e.g.*, Natasha Lomas, *EU, US Agree on Data Transfer Deal to Replace Defunct Privacy Shield*, TechCrunch (Mar. 25, 2022), https://techcrunch.com/2022/03/25/eu-and-us-agree-data-transfer-deal-to-replace-defunct-privacy-shield [https://perma.cc/5JFF-WVGP].

120. Press Release, Eur. Comm'n, IP/23/3721, Data Protection: European Commission Adopts New Adequacy Decision for Safe and Trusted EU-US Data Flows (July 10, 2023).

In comparison, TikTok's initiatives to mitigate governmental concerns, most prominently USDS, Project Texas, and other data localization projects, are corporate-level attempts to signal compliance within an environment of deep geopolitical distrust. These gestures, however elaborate, do not alter the structural premise that TikTok's data flows through a Chinese-controlled ecosystem. By contrast, the United States' response to European concerns were legal instruments, most notably the EU-U.S. Privacy Shield framework after *Schrems I* in 2016[121] and President Biden's creation of the Data Protection Review Court via executive order in response to *Schrems II*.[122] The contrast underscores that, whereas sovereign-level concerns demand sovereign-level responses, TikTok's remedies remained confined to the corporate level.[123]

Both China and the United States maintain national security laws that may, at times, conflict with other countries' data protection principles. However, the United States has secured a new adequacy decision under the EU-U.S. Data Privacy Framework, but China has never been considered for an adequacy decision. In the eyes of European regulators, the differential treatment is justified by the broader constitutional, judicial, and institutional constraints, or lack thereof, surrounding China's laws.[124] A similar logic informs the United States' approach to China. Fundamentally, its regulation of TikTok is premised on skepticism of China's institutional transparency and legal redress mechanisms.[125]

---

121. Klint Finley, *Privacy Shield Will Let US Tech Giants Grab Europeans' Data*, WIRED (July 12, 2016), https://www.wired.com/2016/07/privacy-shield-will-let-us-tech-giants-grab-europeans-data/ [https://perma.cc/6BQM-XHYQ].

122. Lomas, *supra* note 119.

123. This is not to suggest that TikTok's corporate-level efforts were entirely without consequence. When TikTok finalized its divestiture deal in January 2026, TikTok USDS Joint Venture LLC was built upon the data security architecture that TikTok had developed through Project Texas and USDS.

124. PAUL DE HERT & VAGELIS PAPAKONSTANTINOU, EUR. PARLIAMENT POL'Y DEP'T, THE DATA PROTECTION REGIME IN CHINA 5 (2015) (explaining that analyzing data protection in China "is further burdened when the country in question is China, where the essential human rights' conditions (horizontal application, independent courts and legal certainty) are not in place"); KENNETH PROPP, ATL. COUNCIL, WHO'S A NATIONAL SECURITY RISK? THE CHANGING TRANSATLANTIC GEOPOLITICS OF DATA TRANSFERS 4 (2024) (summarizing a report which concluded that "Chinese law legitimizes broad and unrestricted access to personal data by the government").

125. Rose Jackson et al., *TikTok: Hate the Game, Not the Player*, DFRLAB (Feb. 14, 2024), https://dfrlab.org/2024/02/14/tiktok-hate-the-game-not-the-player/ [https://perma.cc/4A9Y-EYUW] (finding that, "while foreign ownership of a company is not a national security threat in and of itself, the Chinese government's legal and extra-legal ability to compel China-headquartered companies to comply with government requests, including access to user data or changes to the platform's product, is unique").

D. TikTok Ban Under PAFACA

The multiyear endeavor by the U.S. government to ban TikTok culminated when President Biden signed PAFACA, more commonly referred to as "the TikTok ban," into law on April 24, 2024.[126] PAFACA was designed to "protect the national security of the United States from the threat posed by foreign adversary controlled applications, such as TikTok" and therefore mandated that the Chinese company ByteDance, TikTok's parent company, divest TikTok.[127] Under the law, if ByteDance failed to divest TikTok within 270 days, web-hosting services would be required to cease supporting TikTok, and Google and Apple would be compelled to remove the app from their stores.[128] TikTok could continue operating in the United States if ByteDance did sell it within 270 days, which could be extended by 90 days by the President if he certifies that there is a path to divestiture and "significant progress" toward executing it.[129] President Biden's signing of the law on April 24, 2024 set January 19, 2025 as ByteDance's deadline to sell TikTok.[130]

Supporters of PAFACA argue that the law does not constitute a regulatory taking as it presents ByteDance with an alternative to a shutdown. ByteDance can avoid prohibition by executing a "qualified divestiture" that severs TikTok's ties with a foreign adversary.[131] However, ByteDance and TikTok counter that ByteDance's option to divest is illusory due to its commercial, technological, and legal impracticality, particularly within the 270-day timeframe outlined by

126. Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, div. H, 138 Stat. 955 (2024).

127. *Id.*

128. *See id.* § 2(a)(1)–(2) (prohibiting providing services to distribute or update foreign adversary controlled applications through an online mobile application store, or providing internet hosting services to enable the distribution or maintenance of such applications).

129. Peter J. Benson & Valerie C. Brannon, Cong. Rsch. Serv., LSB11261, TikTok Inc. v. Garland: Supreme Court Rejects Challenge to TikTok Divestiture Law 2 (2025) ("The President can extend that date up to 90 days upon certification to Congress that (1) a path to a qualified divestiture has been identified; (2) evidence of significant progress toward the divestiture has been produced; and (3) binding legal agreements are in place to enable execution of the divestiture within the extended time period.").

130. Brian Fung, *Biden Just Signed a Potential TikTok Ban into Law. Here's What Happens Next*, CNN Bus. (Apr. 24, 2024), https://www.cnn.com/2024/04/23/tech/congress-tiktok-ban-what-next [https://perma.cc/6RBK-UUPM].

131. Kevin Marien, *TakeTok: Does a TikTok Ban Violate the Takings Clause?*, 2024 U. Chi. Legal F. 515, 536–38 (2024) (arguing that PAFACA's forced divestiture or ban of TikTok does not constitute a compensable regulatory taking because the Supreme Court's regulatory takings jurisprudence primarily involves physical property and does not involve any takings justified by national security).

the law.[132] In their view, the law mandates the sale of TikTok by its Chinese owner or else the application will face an outright ban in the American market.[133]

Critics of PAFACA argue that privacy issues should be addressed through comprehensive legislation covering the entire tech industry, rather than a crude, platform-specific intervention singling out TikTok.[134] They also argue that lawmakers and the government have failed to adequately explain the unique dangers posed by TikTok's possession of its users' data.[135] Some experts have highlighted that, even in the absence of TikTok, China retains avenues to acquire or pilfer American personal data from other platforms, a practice it already engages in.[136]

PAFACA narrowed TikTok's chances for survival under its current operating structure in two ways. First, by mandating divestiture through a statute, Congress eliminated the bargaining space that typically exists in CFIUS review, such as mitigation agreements, data localization projects, third-party auditing, or other compliance-based remedies.[137] The law thus transformed what was previously an administrative negotiation under CFIUS into a "divest or be banned" ultimatum. With ByteDance viewing a qualified divestiture as practically impossible,

---

132. Ryan Knappenberger, *TikTok Sues Feds over 'Obviously Unconstitutional' Potential Ban*, Courthouse News Serv. (May 7, 2024), https://www.courthousenews.com/tiktok-sues-feds-over-obviously-unconstitutional-potential-ban [https://perma.cc/4HMD-9CX5].

133. *See, e.g.*, Sapna Maheshwari & David McCabe, *Congress Passed a Bill That Could Ban TikTok. Now Comes the Hard Part*, N.Y. Times (Apr. 23, 2024), https://www.nytimes.com/2024/04/23/technology/bytedance-tiktok-ban-bill.html [https://perma.cc/75H5-FAQX].

134. *See, e.g.*, Allyn, *supra* note 17.

135. *See, e.g.*, Will, *supra* note 3; Aziz Z. Huq, *Book Review: The Geopolitics of Digital Regulation*, 92 U. Chi. L. Rev. 833, 898 (2025) (indicating that Congress's TikTok ban suggests how these priorities can be shaped in illogical and perverse ways by the influence of the commercial sector within digital political capitalism).

136. Will, *supra* note 3 (noting that the Chinese government can buy personal data from private sellers); Eric Tucker & Michael Balsamo, *US Says Chinese Military Stole Masses of Americans' Data*, Associated Press (Feb. 10, 2020), https://apnews.com/article/ap-top-news-theft-indictments-china-hacking-05aa58325be0a85d44c637bd891e668f [https://perma.cc/G36C-J6TK] (describing how the Chinese military stole the personal information of roughly 145 million Americans by hacking a credit reporting agency); Kevin Collier, *China Spent Years Collecting Americans' Personal Information. The U.S. Just Called It Out.*, NBC News (Feb. 11, 2020), https://www.nbcnews.com/tech/security/china-spent-years-collecting-americans-personal-information-u-s-just-n1134411 [https://perma.cc/WC3X-489U] (noting that China's Ministry of State Security orchestrated hacks of various American organizations starting around 2014).

137. *See* Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, div. H, 138 Stat. 955 (2024) (establishing explicit limitations on judicial review, providing that any challenge to the Act itself must be filed within 165 days of enactment and any challenge to subsequent administrative actions within 90 days of such action).

TikTok's survival hinged almost entirely on the outcome of its legal challenges against the statute's constitutionality. Second, even when TikTok pursued relief via litigation, PAFACA adopted an unusual jurisdictional design by vesting the U.S. Court of Appeals for the District of Columbia Circuit with original and exclusive review authority, thereby bypassing federal district courts altogether.[138] This structural choice compressed the traditional process of judicial review. Rather than proceeding through the conventional three-tier sequence with two opportunities for appellate review, TikTok's challenge began in the D.C. Circuit and had only one opportunity for appellate review in the Supreme Court. This arrangement also constrained opportunities for fact-finding because the D.C. Circuit would not have a factual record created by a trial court to rely on.[139]

On May 7, 2024, TikTok and ByteDance filed a lawsuit against the U.S. government in the D.C. Circuit, contending that PAFACA violated constitutional protections of free speech.[140] TikTok emphasized that, although PAFACA ostensibly offers a choice between divestiture and a nationwide ban, in reality, no such choice exists.[141] The companies further argued that ByteDance cannot divest TikTok within the Act's 270-day timeframe, maintaining that divestiture "is simply not possible: not commercially, not technologically, not legally. And certainly not on the 270-day timeline required by the Act."[142] They alleged that the Chinese government would not allow the divestment of the algorithms integral to TikTok's operation, asserting that "the Chinese government has made clear that it would not permit a divestment of the recommendation engine that is a key to the success of TikTok in the United States."[143] Eight TikTok content creators filed a separate parallel lawsuit against the U.S. government, arguing that PAFACA violated users' First Amendment

138. *See generally* Han Liu, *The Algorithmic Iron Curtain: How the TikTok Case Was "National-Security-ized,"* WENHUA ZONGHENG (2024) (noting that PAFACA directly grants the D.C. Circuit original jurisdiction, thereby reducing TikTok's potential avenues for judicial relief from three to two and limiting factual review).

139. *See* Julien Berman & Alan Z. Rozenshtein, *The TikTok Case Will Be Determined by What's Behind the Government's Black Lines*, LAWFARE (Aug. 13, 2024), https://www.lawfaremedia.org/article/the-tiktok-case-will-be-determined-by-what-s-behind-the-government-s-black-lines [https://perma.cc/WG3V-89SV] (explaining that PAFACA's requirement that any challenges be brought directly in the D.C. Circuit, coupled with the government's reliance on classified submissions, makes it difficult for the D.C. Circuit to evaluate key factual questions "especially in the absence of a trial court factual record").

140. *See* Petition for Review, *supra* note 82, at 30–56.

141. *Id.* at 1–2.

142. *Id.* at 42.

143. *Id.* at 18.

rights to free speech, echoing the legal arguments advanced by TikTok and ByteDance.[144]

On December 6, 2024, the D.C. Circuit rejected TikTok's constitutional challenge to PAFACA, holding that Congress had acted within its authority and that the law did not violate either the First Amendment or the Due Process Clause because the U.S. government had compelling national security interests.[145] In response, TikTok promptly filed a motion with the Supreme Court, seeking an injunction to halt enforcement of the Act pending further review.[146]

On January 17, 2025, the Supreme Court affirmed the D.C. Circuit's decision and upheld the constitutionality of PAFACA, in a decision that appeared to mark the end of TikTok's lawful presence in the United States.[147] The Court held that PAFACA is sufficiently tailored to the government's national security interests to pass constitutional muster.[148] The Court also emphasized the weight of the legislative record, noting Congress's broad consensus that TikTok's data practices posed serious national security risks and that the statute passed with rare bipartisan support.[149]

Major U.S. technology companies started to comply with PAFACA's de-platforming requirement even before the January 19, 2025 divesture deadline. Apple and Google removed TikTok from their app stores; Oracle terminated its cloud support; and TikTok itself temporarily disabled access for U.S. users.[150] Yet, this corporate compliance unraveled almost immediately. On the evening of January 19, 2025, Oracle and Akamai resumed their services for TikTok, reportedly in response to assurances from the second Trump Administration, which had not yet taken office, that they would not face legal repercussions for doing so.[151] The following day, on his first day in office, President Trump

144. Petition for Review and Complaint for Declaratory and Injunctive Relief at 1, Firebaugh v. Garland, 122 F.4th 930 (D.C. Cir. 2024) (No. 24-1130).

145. TikTok Inc. v. Garland, 122 F.4th 930, 961–65 (D.C. Cir. 2024) (holding that PAFACA was narrowly tailored to serve compelling governmental interests in national security).

146. Application for Injunction Pending Supreme Court Review at 1, TikTok Inc. v. Garland, 604 U.S. 56 (2025) (Nos. 24-656 & 24-657).

147. TikTok Inc. v. Garland, 604 U.S. 56 (2025) (per curiam).

148. *Id.* at 76.

149. *Id.* at 79.

150. Jonathan Vanian, *Apple, Google Remove TikTok from Stores as App Halts Service in U.S.*, CNBC (Jan. 19, 2025), https://www.cnbc.com/2025/01/18/apple-google-remove-tiktok-from-stores-as-app-halts-service-in-us.html [https://perma.cc/YK2A-2Y5V]; Bobby Allyn, *TikTok Is Back Online in the U.S., Following Trump's Promise to Pause the Ban*, NPR (Jan. 19, 2025), https://www.npr.org/2025/01/19/nx-s1-5267568/tiktok-back-online [https://perma.cc/EJU5-X592].

151. Allyn, *supra* note 150.

issued an executive order suspending enforcement of PAFACA for 75 days and directing the Department of Justice to issue letters to internet service providers stating that continued support for TikTok would neither violate the statute nor incur liability.[152] A second, third, and fourth extension were granted on April 4, June 19, and September 23, 2025, respectively, ultimately deferring the statutory deadline to December 16, 2025.[153] Through these four successive extensions, President Trump postponed enforcement of the duly enacted PAFACA beyond the 90-day extension limit permitted under the law, notably without certifying any of the statutory conditions required for such a delay. In a letter to Google's Vice President of Regulatory Affairs, Attorney General Bondi conveyed the administration's rationale that enforcement of the TikTok ban amid ongoing U.S.-China negotiations, technical consultations, and intelligence strategies would introduce instability into diplomatic channels and disrupt the "execution of the President's constitutional duties" in foreign affairs.[154]

Trump's repeated extensions of the non-enforcement period have been widely interpreted as evidence of his lack of genuine interest in pursuing divestment during much of 2025.[155] Indeed, he has expressed a particular fondness for the app, crediting it with mobilizing young voters.[156] The White House's decision to open an official TikTok account

152. Exec. Order No. 14,166, 90 Fed. Reg. 8611 (Jan. 20, 2025) (first 75-day delay).

153. *See* Exec. Order No. 14258, 90 Fed. Reg. 15209 (Apr. 9, 2025) (second 75-day delay to June 19, 2025); Exec. Order No. 14310, 90 Fed. Reg. 26913 (June 24, 2025) (third 90-day delay to Sep. 17, 2025); Exec. Order No. 14350, 90 Fed. Reg. 45903 (Sep. 23, 2025) (fourth 90-day delay, ultimately deferring full enforcement to Dec. 16, 2025).

154. Letter from Pamela Bondi, Att'y Gen., to Lee-Anne Mulholland, Vice President, Regul. Affs., Google LLC (Apr. 5, 2025), https://embed.documentcloud.org/documents/25989866-25-3980-nd-cal-response-07032025 [https://perma.cc/63Y8-RFMR] ("The President has previously determined that an abrupt shutdown of the TikTok platform would interfere with the execution of the President's constitutional duties to take care of the national security and foreign affairs of the United States.").

155. *See* John Cassidy, *Donald Trump's TikTok Deal Looks Like Crony Capitalism*, New Yorker (Sep. 29, 2025), https://www.newyorker.com/news/the-financial-page/donald-trumps-tiktok-deal-looks-like-crony-capitalism [https://perma.cc/2NA8-CQSJ] (interpreting the extensions as disregard for the divestment mandate in favor of politically motivated deals); David Shepardson, *Senator Wants Trump to Answer Questions on TikTok Divestiture Plan*, Reuters (Nov. 24, 2025), https://www.reuters.com/legal/transactional/senator-wants-trump-answer-questions-tiktok-divestiture-plan-2025-11-24/ [https://perma.cc/8Z59-ZLP6] (quoting Senator Ed Markey as stating that the extensions raise doubts about President Trump's genuine pursuit of divestment).

156. Jill Colvin et al., *Trump Joins TikTok and Calls It 'An Honor,' as President He Once Tried to Ban the Video-Sharing App*, Associated Press (June 3, 2024), https://www.ap.org/news-highlights/elections/2024/trump-joins-tiktok-and-calls-it-an-honor-as-president-he-once-tried-to-ban-the-video-sharing-app [https://perma.cc/Q2UV-9YFV].

on August 19, 2025 further underscores the dissonance between the TikTok ban and the current administration's embrace of the platform.[157]

Trump's executive orders increasingly appear as efforts to subvert PAFACA altogether.[158] Some commentators have suggested that the president has effectively claimed a power to indefinitely suspend enforcement of duly enacted laws, raising the prospect that PAFACA may be functionally defunct.[159] The repeated postponements to enforce PAFACA may, thus, be an assertion of power that exceeds the traditional bounds of executive discretion.[160] Whereas past presidents confined nonenforcement of laws to particularized cases or temporary suspensions grounded in resource constraints, President Trump issued executive orders that categorically set aside PAFACA's operation and affirmatively assured private actors that they would incur no legal liability for defiance.[161] In effect, this nonenforcement amounts to a claim of dispensing power, which is a prerogative formally abolished by the English Bill of Rights of 1689 and fundamentally incompatible with the democratic principle of legislative supremacy.[162] If President Trump's position that he can broadly suspend enforcement of PAFACA were accepted, statutes would become mere suggestions and subject

157. Steve Holland, *White House Launches TikTok Account with Trump Saying "I Am Your Voice,"* Reuters (Aug. 19, 2025), https://www.reuters.com/world/us/white-house-launches-tiktok-account-with-trump-saying-i-am-your-voice-2025-08-19/ [https://perma.cc/JM3H-HN4B].

158. Alan Z. Rozenshtein, *Trump's TikTok Executive Order and the Limits of Executive Non-Enforcement*, Lawfare (Jan. 21, 2025), https://www.lawfaremedia.org/article/trump's-tiktok-executive-order-and-the-limits-of-executive-non-enforcement [https://perma.cc/3TYF-FPE5] ("The order is transparently an attempt to undermine PAFACAA, rather than implement it in good faith.").

159. Alan Z. Rozenshtein, *The TikTok Ban That Wasn't*, Brookings Inst. (June 20, 2025), https://www.brookings.edu/articles/the-tiktok-ban-that-wasnt/ [https://perma.cc/RC7X-HXUC]; Zack Beauchamp, *Trump Quietly Claimed a Power Even King George Wasn't Allowed to Have*, Vox (July 10, 2025, 7:00 AM), https://www.vox.com/politics/419393/trump-tik-tok-letters-dispensing-power-king [https://perma.cc/R6EN-KVTN].

160. Jack Goldsmith, *An Authority to License Illegal Conduct*, Exec. Functions (July 3, 2025), https://executivefunctions.substack.com/p/an-authority-to-license-illegal-conduct [https://perma.cc/E9SV-RU42].

161. Charlie Savage, *Trump Claims Sweeping Power to Nullify Laws, Letters on TikTok Ban Show*, N.Y. Times (July 3, 2025), https://www.nytimes.com/2025/07/03/us/politics/trump-bondi-tiktok-executive-power.html [https://perma.cc/AX93-ZP6Q] (arguing that the executive branch may exercise "prosecutorial discretion" by declining enforcement in "particular instances" or by setting enforcement priorities under limited resources); Jack Goldsmith, *Trump's Continuing Illegal Refusal to Enforce the TikTok Ban*, Am. Enter. Inst. (June 19, 2025), https://www.aei.org/op-eds/trumps-continuing-illegal-refusal-to-enforce-the-tiktok-ban/ [https://perma.cc/J5WW-K9JN].

162. Savage, *supra* note 161 ("[T]he Constitution does not give presidents the power to dispense with laws—a power that the British king used to have.").

to presidential disregard whenever inconvenient.[163] Such a view would pose a fundamental threat to the constitutional architecture of separated powers and the rule of law itself.[164]

On September 25, 2025, Trump issued Executive Order 14352, *Saving TikTok While Protecting National Security*.[165] The order amends earlier prohibitions by introducing a proposed framework agreement that would be considered a "qualified divestiture."[166] The agreement would divest TikTok's U.S. operations to a new U.S.-based joint venture, thereby satisfying PAFACA's statutory requirement to remove TikTok from foreign adversary "control." The agreement is subject to four principal conditions: 1) ByteDance and affiliated foreign adversary entities must hold less than 20% ownership in the new U.S.-based joint venture; 2) operation of TikTok's algorithms, source code, and content-moderation decisions must be transferred to the new venture; 3) sensitive U.S. user data must be stored in a cloud environment operated by an American company, precluding foreign adversary access; and 4) all software updates, algorithms, and data flows would be subject to continuous monitoring by "trusted security partners," including a requirement that TikTok's recommendation models be retrained and verified within this system.[167]

The September 25, 2025 order offers some clarity to ByteDance and TikTok by specifying the conditions under which compliance may be achieved, thereby shifting the framework from repetitive, temporary deferrals to a qualified exemption, which appears more akin to a genuine solution. However, the order has vague and imprecise language that leaves fundamental questions unresolved, such as who

163. *See* Savage, *supra* note 161 ("Recent past presidents have been aggressive in exercising law enforcement discretion, but they haven't suspended the operation of a law entirely or immunized its violation prospectively.").

164. Alan Z. Rozenshtein, *The Government's Astonishing Constitutional Claims on TikTok*, LAWFARE (July 3, 2025), https://www.lawfaremedia.org/article/the-government-s-astonishing-constitutional-claims-on-tiktok [https://perma.cc/9LLT-8AXV] ("The battle over TikTok is a major rule-of-law crisis in its own right.").

165. *Saving TikTok While Protecting National Security*, THE WHITE HOUSE (Sep. 25, 2025), https://www.whitehouse.gov/presidential-actions/2025/09/saving-tiktok-while-protecting-national-security/ [https://perma.cc/BM9Y-XKNK].

166. *Id.* ("To achieve a 'qualified divestiture,' TikTok must execute a transaction that would result in the application no longer being controlled by a foreign adversary and that would preclude formerly affiliated entities from maintaining an 'operational relationship' with the application's United States operations . . . A plan has been presented to me to undergo a qualified divestiture of TikTok's United States operations, as outlined in a framework agreement.").

167. *Id.*

will ultimately exercise control over the recommendation algorithm[168] or how the platform's corporate governance will function under the proposed structure.[169] For instance, the statute prohibits an "operational relationship" or data sharing agreement with a foreign adversary,[170] yet the agreement imposes no explicit restrictions on remote data access, cross-border personnel interactions, or informal channels of technical cooperation, all of which could plausibly fall within a broad reading of "operational relationship" or "data sharing."

On January 23, 2026, TikTok announced that, in compliance with Executive Order 14352, a new joint venture called TikTok USDS Joint Venture LLC was established to acquire TikTok's U.S. assets.[171] The company stated that the joint venture will operate under defined safeguards designed to protect national security, including comprehensive data protections, algorithm security, content moderation, and software assurances.[172] President Trump said the company would now be owned by a "group of Great American Patriots and Investors, the Biggest in the World," and thanked Chinese President Xi Jinping for working with his administration and for "ultimately, approving the Deal."[173] The closing of the transaction marks the formal conclusion of the divestiture process to both secure TikTok's future in the United States and address national security concerns.

II. Impacts of the TikTok Ban

This section analyzes the impact of PAFACA in both the United States and around the world. Domestically, the law risks undermining constitutional values by granting the executive branch unprecedented power to suppress free expression on digital platforms and also disrupts

168. Jeff Mason et al., *Trump Signs Order Declaring TikTok Sale Ready and Values It at $14 Billion*, Reuters (Sep. 26, 2025), https://www.reuters.com/world/trump-signs-order-declaring-tiktok-sale-plan-meets-us-requirements-2025-09-25/ [https://perma.cc/738Q-E2X5] (citing legal scholar Alan Rozenshtein, who pointed out that "the executive order left unanswered questions, including whether ByteDance would still control the algorithm").

169. Max Zahn, *These Key Questions Loom over TikTok Deal, Experts Say*, ABC News (Sep. 26, 2025), https://abcnews.go.com/Business/key-questions-loom-tiktok-deal-experts/story?id=125961673 [https://perma.cc/WB9A-NEGX] (citing Vance's remark that the deal involves a "blue-chip group of investors," with further details to be disclosed in the coming days).

170. *Saving TikTok While Protecting National Security*, *supra* note 165.

171. *Announcement from the New TikTok USDS Joint Venture LLC*, TikTok (Jan. 23, 2026), https://newsroom.tiktok.com/announcement-from-the-new-tiktok-usds-joint-venture-llc?lang=en [https://perma.cc/C7PK-M6WG].

172. *Id.*

173. Donald J. Trump (@realDonaldTrump), Truth Social (Jan. 23, 2026), https://truthsocial.com/@realDonaldTrump/posts/115942147803684675.

the short-form video economy on which content creators and small businesses increasingly rely. Internationally, PAFACA reshapes foreign investment incentives and signals a departure from the United States' long-standing commitment to an open global internet.

A. Domestic Impacts

1. Free Speech

A major legal concern surrounding PAFACA is its potential threat to the protection of free expression as a constitutional value. Civil liberties organizations have consistently cautioned that PAFACA endows the executive branch with powers that run counter to the First Amendment. The ACLU argued that the statute "gives the president unprecedented power to shut down Americans' speech and access to information under the guise of protecting national security."[174] In a joint amicus brief, the ACLU, the Knight First Amendment Institute, and the Electronic Frontier Foundation urged the Court to block enforcement, contending that PAFACA is "a sweeping ban on the speech of TikTok and its users."[175] They further criticized the D.C. Circuit's opinion for assuming that TikTok's millions of American users could simply migrate to other platforms "with little consequence for their First Amendment rights," a premise they deemed "mistaken."[176] This critical issue of PAFACA's implications for free speech will be examined in greater depth in Part III.[177]

2. Short-Form Video Economy

PAFACA also generates a host of unintended consequences for the short-form video economy, namely diminished advertising revenue and reduced competitiveness for domestic content creators.

U.S. advertisers spend an estimated $12.3 billion per year on TikTok before the TikTok ban,[178] largely because the platform's influencer-driven viral marketing offers uniquely high returns on investment

174. Ashley Gorski & Patrick Toomey, *Banning TikTok is Unconstitutional. The Supreme Court Must Step In.*, ACLU (Jan. 15, 2025), https://www.aclu.org/news/national-security/banning-tiktok-is-unconstitutional-the-supreme-court-must-step-in [https://perma.cc/C9JE-K9BJ].

175. Brief for the American Civil Liberties Union et al. as Amici Curiae Supporting Petitioners at 8, TikTok Inc. v. Garland, 604 U.S. 56 (2025) (Nos. 24-656, 24-657).

176. *Id.* at 3.

177. *See infra* Section III.B.1.

178. Sheila Dang & Chibuike Oguh, *TikTok Advertisers Stay Put After US Appeals Court Upholds Law Forcing Sale*, REUTERS (Dec. 6, 2024), https://www.reuters.com/technology/meta-shares-hit-record-high-after-us-appeals-court-upholds-tiktok-ban-2024-12-06/ [https://perma.cc/9ZWQ-323D].

and conversion rates, particularly for small and medium-sized brands seeking cost-effective customer acquisition.[179] By contrast, domestic platforms like Meta and Google typically charge higher ad prices and deliver lower engagement efficiency for short-form and creator-driven promotions,[180] meaning small businesses could face higher marketing costs and reduced reach without access to TikTok. Indeed, TikTok estimates that U.S. small businesses and social media creators stand to lose $1.3 billion in revenue and earnings within just one month of the ban's implementation.[181]

The TikTok ban would also eliminate a low-cost, high-impact conduit for innovation, thereby risking the stifling of new ideas and the limitation of opportunities for emerging market players, especially small businesses that rely on TikTok as an affordable advertising channel.[182]

---

179. Oxford Econ., The TikTok Effect: The Socioeconomic Impact of TikTok in Five European Countries 3 (2024) (stating that "[s]mall and medium-sized enterprises (SMEs) are particularly well placed to use TikTok for growth, given its low barriers to entry and content algorithm designed to allow users to discover lesser-known brands"); *id.* at 20 (noting that SMEs, such as BiSilver, achieved cost-effective growth through the platform by utilizing TikTok's unique algorithm to reach niche audiences while keeping advertising costs low); *id.* at 24 (highlighting another SME, HolySmile, which reported that light-hearted content on TikTok halved their cost per acquisition (CPA) and increased orders tenfold).

180. For purposes of cross-platform comparison, this Article uses engagement rate and average CPM as proxies for engagement efficiency and advertising prices, respectively, each measured on a per-exposure basis. *See* Carly Carioli, *The True Cost of Social Media Ads in 2025*, Gupta Media (June 27, 2025), https://www.guptamedia.com/social-media-ads-cost [https://perma.cc/AA2G-HN6U] (analyzing tens of billions of ad impressions to show that domestic platforms maintain significantly higher pricing benchmarks, with Meta's average CPM ($8.19) and YouTube's ($4.99) consistently exceeding TikTok's ($4.82)); Sabina Varga & Elena Cucu, *TikTok vs. Reels vs. Shorts*, Socialinsider (Oct. 6, 2025), https://www.socialinsider.io/blog/tiktok-vs-reels-vs-shorts/ [https://perma.cc/HCT2-5SW4] (comparing short-form video engagement across platforms and reporting average 2024 engagement rates of 2.8% on TikTok, 0.65% on Instagram Reels, and 0.3% on YouTube Shorts).

181. Dan Mangan, *TikTok Says Ban Would Cost U.S. Small Businesses, Creators $1.3 Billion in First Month*, CNBC (Dec. 9, 2024), https://www.cnbc.com/2024/12/09/tiktok-ban-cost-us-small-businesses-creators-billion-dollars-month.html [https://perma.cc/PY9S-RX2T]. This perspective often hinges on the widespread belief that platforms such as YouTube and Instagram could gain directly from the TikTok ban, given their ability to capture TikTok's significant user base. *See* Laura He, *Banning TikTok Would Hit China's Tech Ambitions and Deepen the Global Digital Divide*, CNN Bus. (Apr. 24, 2024), https://www.cnn.com/2024/04/24/tech/tiktok-ban-bytedance-split-the-world-further-intl-hnk/index.html [https://perma.cc/XPU4-APXB] ("A US ban, or a less powerful version of TikTok, would be a windfall for YouTube, Google, Instagram and other TikTok competitors, as many of its customers may jump ship.").

182. Meta's CPM rose by 10% following TikTok's temporary outage, while the share of advertisers running campaigns on Meta increased by 6 percentage points, indicating a shift of ad budgets under reduced platform competition. Dante Donati & Hortense Fong, *The Cost of Banning TikTok: Implications for Digital Advertising*

Its immediate effects would reverberate throughout the domestic digital advertising sector, reshaping the competitive landscape among incumbent platforms. Industry analysts projected that a potential ban would cause $6–8 billion in advertising spending to shift to domestic competitors such as Meta and Google.[183] Reports revealed that Google has been actively encouraging advertisers to allocate more resources to YouTube by emphasizing the potential ban of TikTok in the U.S.[184] Similarly, Meta reportedly engaged a consulting firm to orchestrate a nationwide public relations campaign targeting TikTok, aiming to portray the Chinese-owned company as "a danger to American children and society."[185]

3. TikTok

The United States is TikTok's largest market.[186] As such, the TikTok ban exposes the company to significant economic losses. In 2023 alone, TikTok generated approximately $16 billion in revenue from the United States market.[187] Although this amount represents only a modest fraction of ByteDance's total global revenue,[188] the impact is nonetheless significant. However, country-specific bans do not necessarily impede

3 (Colum. Bus. Sch. Rsch. Paper No. 5177746, 2025), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5177746. Meanwhile, researchers projected a 57% surge in ad spend on TikTok in early 2025, but TikTok later estimated a $1B monthly revenue loss for small businesses under a ban, underscoring its role as a low-cost, high-impact marketing channel for emerging market participants. *Id.* at 4–6.

183. Lloyd Lee, Lara O'Reilly & Kenneth Niemeyer, *Meta Could Rake in Billions in Ad Dollars if TikTok Is Banned*, Bus. Insider (Jan. 17, 2025), https://www.businessinsider.com/tiktok-us-ban-how-meta-benefits-google-instagram-youtube-ad-2025-1 [https://perma.cc/ZL3F-998F] ("Assuming TikTok could lose between 50% and 70% of ad revenues due to a ban, $6.17 billion to $8.64 billion of ad spending could need a new home."); Will Oremus, *Trump Got One Thing Right: Banning TikTok Would Help Meta (and Google)*, Wash. Post (Apr. 24, 2024), https://www.washingtonpost.com/technology/2024/04/24/tiktok-ban-benefits-meta-google/ [https://perma.cc/WFB3-J27X] ("The industry analyst eMarketer predicts that Meta could capture an estimated 22.5 to 27.5 percent of TikTok's U.S. ad revenue, bolstering the company's bottom line by more than $2 billion in 2025. It envisions Google capturing more like 15 to 20 percent.").

184. Hugh Langley, *Internal Document Shows Google Using Uncertainty over a TikTok Ban to Try to Win More Ad Dollars for YouTube*, Bus. Insider (May 8, 2024), https://www.businessinsider.com/google-youtube-advertising-spend-tiktok-ban-2024-5 [https://perma.cc/9FDU-RMBG].

185. *See, e.g.*, Bradford, *supra* note 1, at 171.

186. He, *supra* note 181.

187. *TikTok's U.S. Revenue Hits $16 Bln as Washington Threatens Ban, FT Reports*, Reuters (Mar. 15, 2024), https://www.reuters.com/technology/tiktoks-us-revenue-hits-16-bln-washington-threatens-ban-ft-reports-2024-03-15/ [https://perma.cc/A62X-XNDQ].

188. *Id.* (reporting TikTok generated $120 billion in global revenue in 2023).

TikTok's global growth; despite mounting regulatory barriers in the United States, TikTok's reach outside the United States has robustly expanded. Despite India's ban on TikTok in 2020, the platform's global user base nearly doubled within four years, fueled by explosive growth in Southeast Asia and Latin America.[189] As of early 2025, TikTok boasts over 1.6 billion monthly active users worldwide and is projected to reach over 2.3 billion by 2029.[190]

Yet, enforcing a strict prohibition on any post-sale connections between ByteDance and TikTok presents formidable challenges for TikTok, given that its employees have historically relied on ByteDance software in their operations.[191] Most importantly, ByteDance continues to own TikTok's core algorithm and underlying technical architecture, which adds another layer of complexity to their separation.[192] TikTok's experience with Project Texas already proved that it is difficult for U.S.-based teams to review modifications in real time as engineers in China routinely update the recommendation engine.[193] This challenge is exacerbated by the sheer costs involved: Estimates suggest that the construction and ongoing operation of Project Texas, which is structured primarily as a data localization scheme, required initial expenditures of approximately $1.5 billion, with annual operating costs projected between $700 million and $1 billion.[194] Nonetheless, TikTok has undertaken several measures to facilitate its post-sale separation from ByteDance. In addition to maintaining the costly Project Texas,

189. Andrew R. Chow, *Here's What Happened When India Banned TikTok in 2020*, TIME (Jan. 18, 2025), https://time.com/7208112/what-happened-when-india-banned-tiktok/ [https://perma.cc/2K8X-FZP5] ("Research shows that TikTok's userbase essentially doubled between 2020 and 2024. And the U.S. was not even the main driver of this uptick: Indonesia has the most TikTok users in the world. Brazil, Mexico, and Vietnam also have sizable audiences.").

190. Christina Newberry, *35 TikTok Stats Every Marketer Needs to Know in 2025*, HOOTSUITE (Feb. 5, 2025), https://blog.hootsuite.com/tiktok-stats/ [https://perma.cc/6ME4-6SFG].

191. *See, e.g.*, Maheshwari & McCabe, *supra* note 2.

192. *See, e.g.*, Fung, *supra* note 130 (noting that Chinese export controls may prevent the sale of TikTok's algorithm); Maheshwari & McCabe, *supra* note 2 (noting that the Chinese government stated it would not allow a sale of the algorithm); Hagstrom, *supra* note 6 ("[T]he Chinese government 'has made clear that it would not permit a divestment of the recommendation engine that is a key to the success of TikTok in the United States.'").

193. Georgia Wells, *TikTok Struggles to Protect U.S. Data from Its China Parent*, WALL ST. J. (Jan. 30, 2024), https://www.wsj.com/tech/tiktok-pledged-to-protect-u-s-data-1-5-billion-later-its-still-struggling-cbccf203 [https://perma.cc/GBY4-96QT].

194. Matt Perault & Samm Sacks, *Project Texas: The Details of TikTok's Plan to Remain Operational in the United States*, LAWFARE (Jan. 26, 2023), https://www.lawfaremedia.org/article/project-texas-the-details-of-tiktok-s-plan-to-remain-operational-in-the-united-states [https://perma.cc/TYP3-8UQS].

the company is preparing to launch a U.S.-specific version of the app, which would feature its own algorithm trained exclusively on American user data and supported by non-ByteDance data infrastructure.[195]

B. International Impact

1. International Investment in U.S. Technology

The TikTok ban could ripple through global tech investment channels, prompting companies to diversify away from U.S. markets in case of an abrupt, politically-driven restriction on foreign access to U.S.-based cloud or data services. For example, European policymakers increasingly view unilateral U.S. tech sanctions, whether directed at China or otherwise, as a signal of the United States' willingness to weaponize digital infrastructure.[196] Denmark's media companies are already actively seeking alternatives to U.S. technology products, driven by growing concerns that a sudden political decision made by President Trump could compel tech companies to cut off cloud services to European platforms.[197] Likewise, the Dutch government recently adopted a series of parliamentary motions advocating for, among other measures, the establishment of a nationally controlled cloud services platform to reduce reliance on U.S. technology.[198] In the long run, such unilateral bans risk deepening the splintering of the global internet.[199]

---

195. Krystal Hu, *Exclusive: TikTok Prepares US App with Its Own Algorithm and User Data*, Reuters (July 9, 2025), https://www.reuters.com/world/china/tiktok-prepares-us-app-with-its-own-algorithm-user-data-2025-07-09 [https://perma.cc/H83K-4U7M].

196. *See* Theodore Christakis, *When Governments Pull the Plug*, Lawfare (Sep. 29, 2025), https://www.lawfaremedia.org/article/when-governments-pull-the-plug [https://perma.cc/C642-EA4S] (noting that "European policymakers have been increasingly concerned about a U.S. "kill switch," despite reassurances from hyperscalers that digital services will be protected").

197. *See* Sarah Gotfredsen, *Is Europe Divorcing Big Tech?*, Colum. Journalism Rev. (June 5, 2025), https://www.cjr.org/the_media_today/europe-divorce-big-tech-trump-cloud-exit-plan.php [https://perma.cc/XY3B-8SL2] (noting how Danish concerns about the reliability of U.S. technology are driven by President Trump's perceived willingness to spontaneously "pull the plug" on foreign access to U.S. technology).

198. Sterling, *Dutch Parliament Calls for End to Dependence on US Software Companies*, Reuters (Mar. 20, 2025), https://www.reuters.com/world/europe/dutch-parliament-calls-end-reliance-us-software-2025-03-18 [https://perma.cc/DB7W-AJLN].

199. *See generally* Thomas J. Christensen, *Mutually Assured Disruption: Globalization, Security, and the Dangers of Decoupling*, World Pol. (2023) (arguing that government interventions to protect national security should be limited in scope so as to avoid fundamental damage to the complex economic interdependence between the United States and China); Jon Bateman, Carnegie Endowment for Int'l Peace, U.S.-China Technological "Decoupling": A Strategy and Policy Framework (2022) (noting that technological decoupling should not go too far, otherwise it may

2. U.S.-China Trade Relations

The Chinese government has made credible threats of reciprocal retaliation should the United States pursue a forced sale or outright ban of TikTok. In August 2020, amidst the first Trump Administration's efforts to compel a sale of TikTok, the Chinese government revised its export control regulations, which classify a range of technologies as sensitive, to include those resembling TikTok's personalized information recommendation services.[200] Prior to PAFACA's passage, China's Ministry of Commerce reaffirmed its stance against any forced sale of TikTok by leveraging export controls that would prevent its separation from ByteDance.[201] The Chinese government has since vowed to implement "all necessary measures" to protect its interests in light of PAFACA.[202]

In addition to export restrictions, China has retaliated broadly against American companies in light of a possible TikTok ban. On September 19, 2020, a month after the United States announced bans on TikTok and WeChat, China's Ministry of Commerce unveiled details of its long-anticipated "Unreliable Entity List," an official tool to penalize foreign companies deemed harmful to China's national interests.[203] While the list did not formally designate specific firms, Chinese authorities indicated that potential measures could include investigations and operation restrictions targeting U.S. technology companies such as Apple, Cisco, and Qualcomm.[204] Just days before the United States enacted PAFACA in 2024, China's Cyberspace Administration ordered

undermine America's own innovation base, supply chain flexibility, and international cooperation).

200. *See* He, *supra* note 2.

201. *See id.*

202. *See id.*; He, *supra* note 181.

203. Rebecca Kagan, *Fight Escalates over TikTok and WeChat, China Unveils "Unreliable Entity List" and JAIC Hosts AI Partnership for Defense*, Ctr. for Sec. & Emerging Tech. (Sep. 30, 2020), https://cset.georgetown.edu/newsletter/fight-escalates-over-tiktok-and-wechat-china-unveils-unreliable-entity-list-and-jaic-hosts-ai-partnership-for-defense/ [https://perma.cc/YFD8-PJZ8].

204. Bu Kekao Shiti Qingdan Guiding (不可靠实体清单规定) [Provisions on the Unreliable Entity List] (promulgated by the Ministry of Commerce, Sep. 19, 2020, effective Sep. 19, 2020) art. 10 (authorizing measures such as restricting import and export activities, restricting investment, restricting entry and residence of personnel, imposing fines, and other necessary restrictions); *China Ready to Put Apple, Other U.S. Companies in 'Unreliable Entity List' – Global Times*, Reuters (May 15, 2020), https://www.reuters.com/article/technology/china-ready-to-put-apple-other-us-companies-in-unreliable-entity-list-glo-idUSKBN22R22K/ [https://perma.cc/LDW8-7ZC8].

Apple to remove WhatsApp, Threads, Telegram, and Signal from its Chinese App Store, citing national security concerns.[205]

The forced sale of TikTok is not the first instance of forced transfer of technology in the trade relationship between the United States and China. From the American perspective, China has long required U.S. companies to transfer technology and intellectual property to Chinese entities through investment regulations and administrative approval procedures, in a practice known as forced technology transfer.[206] This practice is one of the most contentious issues in U.S.-China trade relations and represents how these two countries use their power to advance national interests by depriving foreign companies of their property rights.[207] PAFACA, on the other hand, reverses these roles as the United States attempts to force Chinese entities to transfer their property to American companies.

However, banning a globally popular foreign app sets a dangerous precedent for economic nationalism in the United States that contradicts the government's open-door investment policy.[208] The Department of Commerce historically promotes the United States as having a predictable regulatory environment to attract foreign direct investment ("FDI").[209] Abrupt bans, like the one threatened against TikTok, reinforce the growing perception that the United States is shifting from being a guarantor of global commerce to a regulator prioritizing

---

205. Natasha Lomas, *Apple Pulls WhatsApp, Threads from China App Store Following State Order*, TechCrunch (Apr. 19, 2024), https://techcrunch.com/2024/04/19/threads-whatsapp-removed-from-china-app-store [https://perma.cc/3GB5-VEHG].

206. Jyh-An Lee, *Forced Technology Transfer in the Case of China*, 26 B.U. J. Sci. & Tech. L. 324, 328–32 (2020).

207. *Id.* at 326–28. *See generally* Peter Lee, *An Organizational Theory of International Technology Transfer*, 108 Minn. L. Rev. 71, 128–30 (2023) (analyzing how China is alleged to use mandatory joint venture rules to facilitate domestic companies' acquisition of data from foreign investors from an organizational theory perspective); Alan O. Sykes, *The Law and Economics of "Forced" Technology Transfer and Its Implications for Trade and Investment Policy (and the U.S.–China Trade War)*, 13 J. Legal Analysis 127, 127–30 (2021) (approaching the forced technology transfer issue from the view of World Trade Organization regulations); Peter K. Yu, *The U.S.-China Forced Technology Transfer Dispute*, 52 Seton Hall L. Rev. 1003, 1003–07 (2022) (introducing the forced technology transfer debate under the Agreement on Trade-Related Aspects of Intellectual Property Rights).

208. *See* 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 [https://perma.cc/TW5B-XW29] ("The proposed ban reinforces a growing belief that America is no longer the leading guarantor of global business, but rather a potential threat to it — a notion that is profoundly reshaping the world economy and threatening American businesses.").

209. *See* U.S. Council of Econ. Advisers, Foreign Direct Investment in the United States 4 (2013) ("This appropriate IP regime is just one example of the stable and predictable regulatory environment that the United States has on offer.").

national security concerns.[210] For instance, Singapore-based Broadcom, a semiconductor company, is not a "hostile state enterprise" in the traditional sense, but the United States blocked its attempted acquisition of Qualcomm because of concerns that the acquisition would weaken Qualcomm's competitiveness in 5G, ceding technological leadership to Chinese firms like Huawei.[211] The United States' intervention expanded the scope of CFIUS's review and marked a shift in the Committee's orientation: Even when an acquiring firm is not Chinese, the potential for an acquisition to erode U.S. technological competitiveness vis-à-vis China may be treated as sufficient grounds for national security concerns.[212] The tightening of the U.S. investment environment for national security reasons may discourage future high-tech FDI inflows to the United States.[213]

3. Global Internet Architecture

The TikTok ban also erodes the United States' commitment to an open and interconnected internet.[214] Historically, a truly borderless internet has long been undermined by government interventions,

---

210. *See* Courtney Fingar, *TikTok Bill Marks a Shift in the U.S.' Foreign Investment Policy*, FORBES (Apr. 25, 2024), https://www.forbes.com/sites/courtneyfingar/2024/04/25/tiktok-law-signals-a-shift-in-us-foreign-investment-stance/ [https://perma.cc/L8ZB-BCPB] ("More broadly, the TikTok order underscores ongoing shifts in U.S. foreign investment policy, particularly with regard to technology and data security from foreign entities.").

211. Michael Leiter, Ivan Schlager & Donald Vieira, *Broadcom's Blocked Acquisition of Qualcomm*, HARV. L. SCH. F. ON CORP. GOVERNANCE (Apr. 3, 2018), https://corpgov.law.harvard.edu/2018/04/03/broadcoms-blocked-acquisition-of-qualcomm/ [https://perma.cc/5JZB-7TMH] (discussing the complex corporate history and jurisdictional identity of Broadcom in the context of U.S. national security reviews).

212. *Id.* (analyzing an "unprecedented" presidential order, marking the first pre-acquisition agreement block in CFIUS history, signaling an expanded scope of China-related concerns that reaches even non-Chinese firms with Chinese ties).

213. See Kristen E. Eichensehr & Cathy Hwang, *National Security Creep in Corporate Transactions*, 123 COLUM. L. REV. 549, 560–78 (2023) (quoting Secretary of State Antony Blinken describing "sharper investment screening measures to defend companies and countries against Beijing's efforts to gain access to sensitive technologies, data, or critical infrastructure" and describing the global adoption of such measures including in the United Kingdom, EU, and Australia); Soha AbdurRahman, *POV: Balancing Foreign Activity and National Security Through the Lens of TikTok*, 2021 U. ILL. J. L., TECH. & POL'Y 363, 373–74 (2021) (suggesting that "[t]he mere mention of a CFIUS investigation regarding a company can hurt the business's ability to complete a deal or gain investments").

214. It is worth mentioning that scholars commonly adopt a more tempered view. While they stop short of condemning the ban with cyber utopianism and acknowledge that the neoliberal vision of a borderless internet is, in many respects, historically obsolete, they nonetheless question the adequacy of sweeping, security-driven prohibitions as a regulatory response. *See* Sitaraman, *supra* note 10, at 1090–100 (cautioning that a national security technocrat model risks underestimating systemic

from the United States' early assertion of control over root servers,[215] to the commercialization of the internet's network infrastructure.[216] With the passage of PAFACA, "balkanization" of the internet appears inevitable.[217] The law signals that the United States, which has historically advocated for a free internet without borders, is now building an isolated local internet.[218] The TikTok ban could "set a terrible precedent for liberal democracy in the digital age," as it may pose "a greater threat to our status as a free and democratic nation than any form of Chinese influence on TikTok ever could be."[219] TikTok and ByteDance similarly claimed that the divesture stipulated by PAFACA "would disconnect Americans from the rest of the global community on a platform devoted to shared content—an outcome fundamentally at odds with the Constitution's commitment to both free speech and individual liberty."[220] These statements reflect concerns that measures like the TikTok ban risk supplying authoritarian regimes with rhetorical ammunition to dismiss U.S. criticism that they themselves suppress speech platforms deemed politically or ideologically objectionable.[221]

---

and latent dangers, including the intelligence and market-power consequences of large-scale data outflows).

215. Jack Goldsmith & Tim Wu, Who Controls the Internet? Illusions of a Borderless World 170–71 (2006) (describing the United States' control of the physical root server for the domain name system).

216. Barry M. Leiner et al., *A Brief History of the Internet*, Arxiv (1999), https://arxiv.org/abs/cs/9901011 [https://perma.cc/9GAF-PWB4].

217. "Balkanization" of the internet is defined as the disaggregation of a "'network of networks' into an amalgam of networks, with varying degrees of accessibility to other networks." Rob Frieden, *Without Public Peer: The Potential Regulatory and Universal Service Consequences of Internet Balkanizatio*n, Va. J.L. & Tech., Fall 1998, at 2. The internet will be fragmented into territorially bounded networks, where governments impose sovereignty-based restrictions on data flows and platforms.

218. *See, e.g.*, Bradford, *supra* note 1, at 152, 169, 171 (indicating that the TikTok ban undermines the core values of the American market-driven model while inadvertently strengthening the Chinese state-driven approach, in which government intervention in tech companies' applications is commonplace); He*, supra* note 181 (commenting that the TikTok ban "would further deepen the divide between two digital worlds centered around the rival economic superpowers").

219. Milton Mueller, *Banning TikTok: A Self-Inflicted Wound on Liberal Democracy,* Tech Pol'y (Sep. 12, 2024), https://www.techpolicy.press/banning-tiktok-a-self-inflicted-wound-on-liberal-democracy [https://perma.cc/6STC-S868] ("It's a shame that the Justice Department has lost confidence in our media governance model and is borrowing policies from China.").

220. *See* Petition for Review, *supra* note 82, at 3.

221. *See, e.g.*, Nick Frisch & Dan Wang, *The End of TikTok Is a Propaganda Win for Beijing*, N.Y. Times (May 14, 2024), https://www.nytimes.com/2024/05/14/opinion/tiktok-sale-ban-legislation-congress-china.html [https://perma.cc/G5NT-N4ZD] ("America's moral authority on maintaining open internet platforms will look very different if it bans TikTok. After years of enduring American sermonizing about free speech and open trade, autocrats would now be able to cite Washington's own example

Nevertheless, some acknowledge that, although such a ban could be perceived as a belligerent departure from America's longstanding commitment to an open internet,[222] this move is justified as a tit-for-tat reciprocity strategy toward China's "net nationalism" which blocks foreign content from the domestic market.[223] In this light, the United States' regulation of TikTok on national security grounds should be understood against a backdrop of China's institutional and legal environment.

III. Moving from the Physical Layer to the Content Layer: Free Speech and Judicial Deference in *TikTok v. Garland*

On January 17, 2025, the Supreme Court unanimously upheld the constitutionality of PAFACA in *TikTok v. Garland*.[224] In doing so, the Court held that PAFACA is a content-neutral regulation and therefore applied intermediate, rather than strict, scrutiny to the law. In its subsequent analysis, the Court showed significant deference to congressional and executive assessments of TikTok's national security risks. It accepted the government's predictive judgments about the risks posed by TikTok's data transfer practices, despite the absence of concrete evidence of such data transfers to the Chinese government.[225]

The Supreme Court's ruling in *TikTok v. Garland* creates two tensions that are not fully resolved in the Court's opinion. The first is a content-neutrality paradox: If PAFACA is justified by concerns that TikTok enables the Chinese government to influence American public discourse, then the part of the TikTok ban concerning Chinese content manipulation cannot be content-neutral, as it targets a particular category of speech, that is, speech allegedly shaped by a foreign adversary. Under

---

when they interfere with speech platforms that displace them."); Kevin Collier, *A TikTok Ban Could Embolden Authoritarian Censorship, Experts Warn*, NBC News (Mar. 17, 2024), https://www.nbcnews.com/tech/tech-news/tiktok-ban-embolden-authoritarian-censorship-experts-warn-rcna143476 [https://perma.cc/F45A-TD2X] ("The proposed TikTok ban working its way through Congress could embolden authoritarian censorship abroad, experts warn, and shatter the United States' reputation as an international champion of free speech.").

222. Tim Wu, *A TikTok Ban is Overdue*, N.Y. Times (Aug. 18, 2020), https://www.nytimes.com/2020/08/18/opinion/tiktok-wechat-ban-trump.html [https://perma.cc/7ZCK-W4NC].

223. *See id*. ("Were almost any country other than China involved, Mr. Trump's demands would be indefensible. But the threatened bans on TikTok and WeChat, whatever their motivations, can also be seen as an overdue response, a tit for tat, in a long battle for the soul of the internet.").

224. TikTok Inc. v. Garland, 604 U.S. 56 (2025) (per curiam).

225. *See infra* Sections III.B.2 and III.B.3.

conventional First Amendment doctrine, that framing would trigger strict scrutiny.[226] Yet if PAFACA is truly content-neutral, as the Court maintains, then the asserted national security interest becomes harder to sustain because the government can no longer rely on China's purported capacity to manipulate TikTok's content as a justification for the ban.

The second tension concerns judicial deference. National security determinations are volatile political judgments[227] that mirror changing political understandings of what constitutes a national security threat. Across the twentieth and twenty-first centuries, the objects that trigger deference have expanded from wartime military decisions,[228] to Cold War ideological subversion,[229] to post-9/11 terrorism,[230] and now to digital infrastructure, data flows, and algorithmic recommendation systems. The logic of foreign affairs exceptionalism has migrated into these new technological domains as they have developed,[231] with courts applying familiar deference frameworks to these new forms of risk. *TikTok v. Garland* marks the newest stage in this evolution: The Court embraced predictive judgments surrounding national security concerns without demanding substantial evidence, extending deference into a domain where the technology is uncertain and the harms are speculative and often undetectable.

This Section also explains that the judiciary's deference to national security assessments in *TikTok v. Garland* is not unprecedented by comparing the TikTok ban and the Huawei sanction. Both share a common origin in the companies' entanglement with foreign ownership and national security concerns, yet both also exhibit an expanding tendency of courts to defer to governmental forecasts of risk even in the absence of concrete evidence, where regulators are acting preemptively against potential vulnerabilities. However, TikTok's role as a speech infrastructure operating on the content layer introduces a new dimension—unlike hardware systems that sit at the physical layer, TikTok mediates expressive activity directly at the content layer. Therefore, *TikTok v. Garland* marks a further step in this evolution;

226. *Garland*, 604 U.S. at 70.

227. *See infra* Sections III.B.2 and III.B.3.

228. *See*, *e.g.*, Korematsu v. United States, 323 U.S. 214, 224 (1944) (Frankfurter, J., concurring) (reasoning that the validity of actions under the war power must be judged "wholly in the context of war").

229. *See* Dennis v. United States, 341 U.S. 494, 509 (1951) (deferring to the assessment that communist advocacy posed a danger to national security in the absence of an imminent threat); *infra* note 259 and accompanying text.

230. *See* Ziglar v. Abbasi, 582 U.S. 120, 142 (2017) (noting that judicial intervention in the government's post-9/11 response would inappropriately require "inquiry into sensitive issues of national security").

231. *See infra* Section III.A.2.

it illustrates how the Supreme Court extended its judicial deference doctrine from cases involving physical infrastructure to those involving digital platforms, where expressive interests are far more direct and constitutionally charged.

A. The Doctrinal Evolution of Free Speech and National Security

1. Categorizing Free Speech: Content-Based and Content-Neutral Regulation

A proper assessment of PAFACA's constitutionality requires situating TikTok and ByteDance's arguments within the established First Amendment framework. The First Amendment prohibits laws "abridging the freedom of speech."[232] While this protection is broad, it is not absolute.[233]

First Amendment doctrine distinguishes between content-based and content-neutral regulations.[234] A law is content-based if it applies to speech because of the message conveyed.[235] In *Reed v. Town of Gilbert*, the Supreme Court reaffirmed that such laws are presumptively invalid and generally subject to strict scrutiny.[236] In its analysis of content-based restrictions, the Court categorizes speech as either low-value or high-value: While categories deemed "low-value," such as obscenity, defamation, fighting words, or commercial speech, are subject to categorical balancing, high-value speech is treated as core expression and receives the highest level of constitutional protection.[237]

Content-based laws targeting high-value speech are subject to strict scrutiny, which requires the government to demonstrate both that it is pursuing a compelling interest and that the regulation is narrowly tailored to directly advance that interest by the least restrictive means

---

232. U.S. CONST. amend. I.

233. *See, e.g.*, Schenck v. United States, 249 U.S. 47, 52 (1919) (articulating the "clear and present danger" test); Brandenburg v. Ohio, 395 U.S. 444, 447–48 (1969) (holding that speech may be proscribed if it is "directed to inciting or producing imminent lawless action and is likely to incite or produce such action"); Chaplinsky v. New Hampshire, 315 U.S. 568, 571–72 (1942) (recognizing "fighting words" as unprotected speech); Miller v. California, 413 U.S. 15, 23 (1973) (holding that obscenity is not protected under the First Amendment).

234. R. George Wright, *Content-Based and Content-Neutral Regulation of Speech: The Limitations of a Common Distinction*, 60 U. MIA. L. REV. 333, 333 (2006) (characterizing the distinction between regulations that are content-based or content-neutral as "central to contemporary free speech law").

235. *Id.*

236. Reed v. Town of Gilbert, 576 U.S. 155, 163 (2015).

237. Geoffrey R. Stone, *Content-Neutral Restrictions*, 54 U. CHI. L. REV. 46, 47 n.4 (1987).

available.[238] The Court has emphasized that even in the presence of important governmental concerns, the state may not burden substantially more speech than is necessary to achieve its objectives.[239]

National security, though often invoked as a compelling interest, does not exempt the government from these constitutional requirements. Earlier cases relied on formulations such as the "clear and present danger" test,[240] but modern doctrine, most prominently articulated in *Brandenburg v. Ohio*, requires evidence that speech is directed toward inciting imminent lawless action and is likely to produce such action.[241] In contexts involving classified information or intelligence assessments, courts have often deferred to the executive's factual judgments,[242] but scholars have consistently warned that national security rationales are especially susceptible to overreach and thus warrant heightened judicial vigilance.[243]

Content-neutral restrictions, by contrast, regulate expression without reference to specific ideas, viewpoints, or subject matter. Examples of content-neutral restrictions include laws that require the use of city-provided sound systems to control volume,[244] that prohibit camping in a particular park,[245] or that forbid the destruction of draft cards.[246] These restrictions are reviewed under intermediate scrutiny if they are genuine "time, place, or manner" restrictions that are narrowly

238. *Reed*, 576 U.S. at 163.

239. *See* Ashcroft v. ACLU, 542 U.S. 656, 666 (2004) (striking down the Child Online Protection Act because the government had not shown that its restriction on speech was the least restrictive means of furthering its compelling interest).

240. Schenck v. United States, 249 U.S. 47, 52 (1919) ("The question in every case is whether the words used are used in such circumstances and are of such a nature as to create a clear and present danger that they will bring about the substantive evils that Congress has a right to prevent.").

241. Brandenburg v. Ohio, 395 U.S. 444, 447–48 (1969) (addressing incitement and national security cases involving classified information or espionage, which are generally governed by more deferential standards).

242. *See, e.g.*, Dep't of the Navy v. Egan, 484 U.S. 518, 529 (1988) (upholding the Executive Branch's authority to grant or deny security clearances based on its expertise in protecting classified information).

243. Robert M. Chesney, *National Security Fact Deference*, 95 Va. L. Rev. 1361, 1365, 1434 (2009) (observing that judicial deference to executive factual judgments in national security cases is poorly understood, inconsistently applied, and can have a dispositive impact, thereby exacerbating uncertainty about the judiciary's checking role); Shirin Sinnar, *A Label Covering a "Multitude of Sins": The Harm of National Security Deference*, 136 Harv. L. Rev. F. 59, 59 (2022) (contending that judicial deference encourages national security agencies' overreach and "insulat[es] national security abuses from meaningful judicial review").

244. Ward v. Rock Against Racism, 491 U.S. 781, 787 (1989).

245. Clark v. Cmty. for Creative Non-Violence, 468 U.S. 288, 289 (1984).

246. United States v. O'Brien, 391 U.S. 367, 369–70 (1968).

tailored to serve significant governmental interests.[247] Intermediate scrutiny allows a wide range of outcomes and leaves the government with substantially more regulatory space than is available under strict scrutiny.[248] At its most deferential application, content-neutral restrictions are sustained on the ground that they do not implicate First Amendment concerns or that they are merely "reasonable."[249] More frequently, however, courts uphold such restrictions only when they serve a substantial governmental interest and do not unreasonably limit alternative channels of communication.[250]

2. Explaining Judicial Deference through Foreign Affairs Exceptionalism

National security has long been treated as a domain in which the Executive Branch enjoys substantial discretion.[251] This tradition of judicial restraint has, over time, evolved into a broader, and "generally more relaxed," jurisprudential stance on foreign affairs, also known as foreign affairs exceptionalism.[252] Proponents of exceptionalism contend that contemporary constitutional practice allows the government to operate under looser constitutional constraints abroad than at home,[253] a

247. *Ward*, 491 U.S. at 791.

248. Ashutosh Bhagwat, *The Test that Ate Everything: Intermediate Scrutiny in First Amendment Jurisprudence*, 2007 U. ILL. L. REV. 783, 785 (2007) (noting that intermediate scrutiny "has attained central importance in the overall structure of free speech law").

249. *Clark*, 468 U.S. at 297 (holding that the prohibition on overnight camping in the National Mall was a reasonable regulation of the use of public space rather than a direct restriction on expressive content); *O'Brien*, 391 U.S. at 381–82 (explaining that the prohibition on burning draft cards was aimed at maintaining the effective functioning of the Selective Service system, rather than suppressing expression, and thus constituted a content-neutral regulation not subject to strict scrutiny).

250. City of Renton v. Playtime Theatres, Inc., 475 U.S. 41, 48–50 (1986) (treating an ordinance targeting a specific type of content as a content-neutral "secondary effect" regulation and holding that it served a substantial governmental interest in preserving community order and left open adequate alternative locations for expression).

251. *See* Chesney, *supra* note 243, at 1362–63 (observing that, in national security litigation, courts frequently comply with executive branch demands for deference to its factual judgments, shielding executive actions from substantive oversight); Eichensehr & Hwang, *supra* note 213, at 587 (highlighting that "[t]he Supreme Court has been particularly deferential in circumstances where predictive judgments about national security are involved").

252. Curtis A. Bradley, *A New American Foreign Affairs Law?*, 70 U. COLO. L. REV. 1089, 1096 (1999).

253. *See, e.g.*, *id.* ("Foreign affairs exceptionalism is the view that the federal government's foreign affairs powers are subject to different, and generally more relaxed, set of constitutional constraints than those that govern its domestic powers."); Ganesh Sitaraman & Ingrid Wuerth, *The Normalization of Foreign Relations Law*, 128 HARV. L. REV. 1897, 1902 (2015) ("Foreign relations exceptionalism [is] the belief that legal issues arising from foreign relations are functionally, doctrinally, and even methodologically distinct from those arising in domestic policy."). *See generally* Carlos

distinction sometimes justified by the executive's functional advantages, such as expertise, information control, secrecy, and flexibility.[254]

By contrast, Harold Koh argues that exceptionalism is normatively misguided: While the executive's functional strengths have indeed drawn decision-making authority toward it, these advantages are in part self-reinforcing.[255] Courts have been denied the resources, such as judicial training, skilled clerks, strong amicus input, robust scholarship, and an updated Restatement of Foreign Relations Law, that would enable them to engage more capably in foreign affairs and national security issues, making deference a consequence of neglect rather than necessity.[256]

Although framed as longstanding judicial tradition, national security deference and foreign affairs exceptionalism are not static. What counts as a national security threat has undergone successive waves of expansion, each broadening the scope of deference.[257] During the Cold War, national security was largely synonymous with military vulnerability and ideological subversion, and deference was invoked to shield decisions restricting communist speech.[258] After 9/11, national security broadened to encompass counterterrorism, with the Supreme Court permitting some judicial review but ultimately accepting that extraordinary measures were constitutionally permissible in the face of anticipatory harms.[259] Since 9/11, the Court has "nearly always

---

M. Vázquez, *The Abiding Exceptionalism of Foreign Relations Doctrine*, 128 HARV. L. REV. F. 305 (2015).

254. Harold Hongju Koh, *The 21st Century National Security Constitution*, 91 GEO. WASH. L. REV. 1391, 1409 (2023); Daniel Abebe & Eric A. Posner, *The Flaws of Foreign Affairs Legalism*, 51 VA. J. INT'L L. 507, 509 (2011) ("Secrecy, speed, and decisiveness are at a premium, and these are characteristics of the executive, not of the courts.").

255. Koh, *supra* note 254, at 1409.

256. *Id*. ("Some scholars have simply asserted that, unlike past judges, modern federal judges are just too ignorant to decide foreign affairs cases. But again, this is a self-fulfilling prophecy.").

257. *See* OFF. OF DIR. OF NAT'L INTEL., VISION 2015: A GLOBALLY NETWORKED AND INTEGRATED INTELLIGENCE ENTERPRISE 4 (2008) (observing that "the list of national security . . . concerns" must expand "to include infectious diseases, science and technology surprises, financial contagions, economic competition, environmental issues, energy interdependence and security, cyber attacks, threats to global commerce, and transnational crime"). *See generally*, Lisa A. Rich, *New Technology and Old Law: Rethinking National Security*, 2 TEX. A&M L. REV. 581 (2015) (exploring how law should respond to or expand to address new national security challenges).

258. *See* Dennis v. United States, 341 U.S. 494, 509, 516–17 (1951) (upholding convictions under the Smith Act and deferring to Congress's assessment that communist advocacy posed a sufficient danger to national security, despite the absence of any imminent threat).

259. *See* Holder v. Humanitarian L. Project, 561 U.S. 1, 4 (2010) ("The parties agree that the Government's interest in combating terrorism is an urgent objective of the highest order.").

deferred to the executive branch when the latter invokes national security."[260] By the late 2010s, national security evolved further—towards election interference and disinformation, as evinced by the government's regulation of foreign influence operations on platforms like Facebook and X.[261] The TikTok content ban marks the newest shift. National security is now concerned with both harmful content as well as the content distribution architecture itself, including data transfer, cloud storage, and algorithmic recommendation. The judicial restraint stemming from national security interests and foreign affairs exceptionalism remains the same, but the object of such actions has shifted from missiles to metadata, from pamphlets to recommendation systems.

While courts may, in practice, accept the executive's expanding definition of national security and quietly expand the deference they apply to such cases,[262] it does not necessarily follow that courts *should* invariably accord deference to the executive. To the contrary, such excessive judicial deference to national security concerns carries the risk of backfiring.[263] There are generally two possible options for courts to avoid such backfiring. First, courts may conclude that the definition of national security has been overly stretched to include even contexts far removed from traditional national security issues, such as dating apps, and thus courts may choose to adopt a more skeptical stance across all national security cases.[264] In such cases, claims of national security receive more rigorous judicial scrutiny, thereby undermining the very deferential treatment the executive sought to secure.[265] Alternatively, courts may move toward a bifurcated approach where they extend

260. Sinnar, *supra* note 243, at 69 (2022) (noting a tendency towards deference despite a few instances where the Court ruled against the government detention of post-9/11 terrorism suspects).

261. Exec. Order No. 13,848, 83 Fed. Reg. 46843 (Sep. 12, 2018) (characterizing unauthorized access of election and campaign data as constituting "an unusual and extraordinary threat to the national security and foreign policy of the United States").

262. *See* Eichensehr & Hwang, *supra* note 213, at 587 (highlighting that "[j]udges rely on functional justifications for such national security fact deference, including the executive's expertise (and the court's comparative lack expertise) . . . and the executive's access to additional sources of information").

263. *Id.* at 595 (naming the two possible judicial responses as "the constriction possibility" and "the bifurcation possibility").

264. *Id.* at 585 ("[E]ver-broader claims about what falls within the ambit of national security, particularly the economically focused claims at issue in national security creep, cause judges to become more skeptical of and less deferential to executive branch national security assertions across the board, even on more traditional national security–related issues like terrorism or war powers.").

265. *Id.* at 595 (summarizing how the constriction possibility "prompt[s] normalization in the form of decreased deference").

little deference to economic or non-traditional security claims, such as investment screening or data governance, while maintaining, or even strengthening, deference in traditional domains like military affairs, defense, and counterterrorism.[266]

Critics of exceptionalism argue that foreign affairs exceptionalism has largely receded since the end of the Cold War as foreign relations law has "normalized"—courts increasingly treat foreign affairs as ordinary policy questions rather than as exceptional domains warranting heightened deference.[267] Exceptionalists concede some normalization but maintain that deference remains entrenched in lower court practice.[268] Indeed, the core logic of foreign affairs exceptionalism continues to shape judicial behavior in subtle but durable ways. In a recent article, Professor Mark Jia noted a New York trial court decision that treated China's legal system as systemically unjust, thereby precluding recognition of any Chinese judgment in the state.[269] The trial court accorded the State Department's country reports an exceptional and determinative weight at the motion to dismiss stage, well beyond their ordinary evidentiary role,[270] exemplifying how such entrenched deference continues to operate in lower courts.

B. Understanding TikTok from the Perspectives of Free Speech and National Security

Given that TikTok is fundamentally a platform for user expression, a significant critique of PAFACA is its potential to suppress free

266. *Id.* at 591.

267. Sitaraman & Wuerth, *supra* note 253, at 1903 (2015) ("In *Zivotofsky v. Clinton* and *Bond v. United States* (*Bond I*) . . . the Court rejected the exceptionalist approach and declared the issues in those cases as suitable for adjudication."); Harlan Grant Cohen, *Formalism and Distrust: Foreign Affairs Law in the Roberts Court*, 83 Geo. Wash. L. Rev. 380, 384–87 (2015) (noting the Court's shift in attitude from deference towards distrust of the executive branch in the realm of foreign affairs).

268. Sitaraman & Wuerth, *supra* note 253, at 1949–74 (noting that, despite the Supreme Court's trend toward normalization and the waning of exceptionalism, exceptionalism remains "unfinished business" in lower courts).

269. Mark Jia, *American Law in the New Global Conflict*, 99 N.Y.U. L. Rev. 636, 702–03 (2024) (describing how a judge, who was asked to determine whether China's courts were impartial enough for New York courts to recognize their judgments, "held for the first time in state or federal law that a Chinese judgment could not be enforced because China's system was systemically unfair").

270. *Id.* at 703 (pointing out that the court held that "the State Department's country reports, which assess the human rights conditions of foreign countries, constituted 'conclusive documentary evidence' that could end a case at the dismissal stage of litigation").

speech.[271] Critics of PAFACA contend that national security concerns alone cannot justify restrictions on freedom of expression.[272] They assert that the government bears the burden of demonstrating the necessity of such restrictions, a burden they argue that has not been adequately met with regard to PAFACA.[273] In its lawsuit challenging PAFACA's constitutionality, TikTok contended that "[t]he statements of congressional committees and individual Members of Congress during the hasty, closed-door legislative process preceding the Act's enactment confirm that there is at most speculation, not 'evidence,' as the First Amendment requires."[274] TikTok and ByteDance further argued that, if the law was upheld, it could empower the government to invoke national security concerns to compel the owners of other platforms, including news sites, to either divest or face closure.[275] The TikTok users who filed a parallel lawsuit claimed that PAFACA "bans an entire medium of communication and all the speech communicated through that medium, even though, at the very least, the vast majority of that speech is protected."[276] Additionally, they argued that the law prevents them from creating and sharing expressive material through their chosen publisher, as well as from viewing content from other users.[277]

The TikTok ban indeed falls within the analytical framework of free speech, though the Supreme Court ultimately declined to ground its *TikTok v. Garland* analysis in the full protections of the First Amendment through two maneuvers in their reasoning. First, by treating PAFACA as content-neutral, the Court applied only intermediate rather than strict scrutiny to assess the restriction. Second, under intermediate scrutiny,

---

271. *See, e.g.*, Allyn, *supra* note 17; Fung, *supra* note 130; Maheshwari & McCabe, *supra* note 133.

272. *See, e.g.*, Gorski & Toomey, *supra* note 174 ("The law at issue gives the president unprecedented power to shut down Americans' speech and access to information under the guise of protecting national security."); Jennifer Huddleston, *US Wants to Ban TikTok, but First Amendment Demands Stronger Case on National Security*, CATO INST. (Mar. 20, 2024), https://www.cato.org/commentary/us-wants-ban-tiktok-first-amendment-demands-stronger-case-national-security [https://perma.cc/A89B-5UE6] (arguing the government has not provided sufficient evidence that their national security concerns alone justify restricting First Amendment-protected expression).

273. *Id.*

274. Petition for Review, *supra* note 82, at 41.

275. *See id.* at 50 ("The government 'cannot claim' that banning some types of foreign owned applications is 'necessary' to prevent espionage and propaganda 'while at the same time' allowing other types of platforms and applications that may 'create the same problem.'").

276. Petition for Review and Complaint for Declaratory and Injunctive Relief at 29, Firebaugh v. Garland, 122 F.4th 930 (D.C. Cir. 2024) (No. 24-1130), 2024 WL 2190747 at *29.

277. *Id.* at *1.

the Court accepted the government's predictive judgments of TikTok's national security risks, lowering the evidentiary burden by not requiring concrete proof of harm.

1. The Content-Neutrality Paradox

At the core of the Supreme Court's reasoning in *TikTok v. Garland* lies an exploration of PAFACA's nature and the distinction between content-based and content-neutral restrictions.[278] In its elaboration on why PAFACA does not regulate particular speech, the Court's reasoning can be understood as proceeding in three steps. First, it emphasizes that the statue "do[es] not target particular speech based upon its content," but instead directs its restrictions at TikTok as an entity.[279] Second, unlike the law in *Holder v. Humanitarian Law Project*, which singled out expression that served a particular function, the Court rejects the possibility that the Act regulates speech based on its "function or purpose."[280] Third, the Court concludes that the Act does not "impose a restriction, penalty, or burden by reason of content on TikTok," relying on the observation that "petitioners cannot avoid or mitigate" the statute's effects by altering their speech.[281]

The D.C. District Court's opinion introduced a nuanced framing of whether the TikTok ban is a speech restriction. It emphasized that the Chinese government's ability to manipulate public discourse on TikTok to serve its own ends "is at odds with free speech fundamentals."[282] This view suggests that restricting a foreign actor's capacity to manipulate communicative platforms may be understood as a vindication of maintaining free expression rather than as a suppression of speech. This rationale is particularly salient in national security contexts, where covert foreign influence over the U.S. information environment has been treated as a threat to the integrity of public discourse itself.[283]

However, both the D.C. District Court's opinion and the Supreme Court's framing of PAFACA as content-neutral creates a

278. TikTok Inc. v. Garland, 604 U.S. 56, 73 (2025) (per curiam) (noting that "requiring divestiture for the purpose of preventing a foreign adversary from accessing the sensitive data of 170 million U. S. TikTok users is not 'a subtle means of exercising a content preference").
279. *Id.*
280. *Id.*
281. *Id.*
282. TikTok Inc. v. Garland, 122 F.4th 930, 958 (D.C. Cir. 2024).
283. Alan Z. Rozenshtein, *What if Free Speech Means Banning TikTok?*, ATLANTIC (Dec. 12, 2024), https://www.theatlantic.com/ideas/archive/2024/12/tiktok-ban-free-speech/680976/ [https://perma.cc/D4X5-PFFE] ("[T]he anti-distortion rationale lives on in national-security cases.").

content-neutrality paradox, which emerges in two steps. First, as the government's case rests on evidence that the Chinese government has in fact manipulated TikTok's content through the platform's algorithmic recommendations, the law cannot plausibly be content-neutral. By targeting China's "covert content manipulation,"[284] the Act becomes content- and viewpoint-based, which should trigger strict scrutiny. Second, if the government abandons the content-based claims of potential Chinese content manipulation, resting its case solely on the risks associated with the identity of TikTok's foreign ownership and the potential data surveillance scheme, then PAFACA's logic begins to weaken. Without the premise of content manipulation or data exploitation, it becomes unclear why TikTok's ownership structure alone creates a harm that distinguishes it from other foreign owned, or even domestically owned, companies. The paradox, then, is that the government invokes content-based concerns to justify its action while insisting on content-neutral treatment to survive constitutional review.

PAFACA itself references its target as TikTok's content recommendation: In defining the scope of a "qualified divestiture," the statute authorizes the President to prohibit any arrangement that would allow continued "cooperation with respect to the operation of a content recommendation algorithm or an agreement with respect to data sharing."[285] The statute contains two distinct strands of concern—one aimed at data exploitation and another aimed at algorithmic manipulation. While the former addresses data exploitation or surveillance concerns in a manner generally indifferent to its meaning, the part targeting cooperation over the operation of a content recommendation algorithm implicates how expressive materials are curated and disseminated. At least this part of PAFACA therefore operates in a content-based manner. Additionally, PAFACA imposes a divestiture requirement that applies to TikTok and its parent company, ByteDance. This requirement is thus a speaker-specific regulation targeting TikTok and other "foreign

284. *Garland*, 604 U.S. at 67 (mentioning the D.C. Circuit's finding that "the Government's national security justifications—countering China's data collection and covert content manipulation efforts—were compelling" yet framing the risk from TikTok's recommendation algorithm exclusively in terms of the algorithm's reliance on U.S. user data for training and the difficulties of monitoring data flows). *But see id.* at 81 (Gorsuch, J. concurring) (cautioning that the government's asserted interest in preventing "covert content manipulation" is dangerously elastic and should not be judicially endorsed).

285. Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, div. H, § 2(g)(6)(B), 138 Stat. 955, 959 (2024).

adversary controlled" apps, and not other social media platforms, based on who controls them,[286] which should trigger strict scrutiny.[287]

However, the Court treats the government's two stated national security concerns as if they are functionally indistinguishable, folding algorithmic recommendation practices into a broader data security frame.[288] In other words, it applies a content-neutral classification by selective attention to the statute's components of data security while ignoring components of content manipulation. By doing so, the Court is able to characterize PAFACA as content-neutral rather than content-based.

The broader consequence of this interpretation is more troubling. If algorithmic recommendation can be recharacterized as merely an extension of data exploitation whenever national security concerns are invoked, then future regulations targeting expressive platforms may similarly evade strict scrutiny. Other platforms whose communicative architecture depends on algorithmic ranking could be regulated under a content-neutral framework applying intermediate scrutiny, so long as the government frames its concerns in terms of "data flows," "algorithmic risk," or "foreign exploitation."

The choice of standard is critical. Under strict scrutiny, the government must show that a restriction is narrowly tailored to a compelling interest and that no less restrictive alternative would suffice.[289] In such cases, courts have overturned many laws that restrict speech, including a federal law that restricted citizens' "right to receive" mailed communist propaganda from a foreign adversary because it imposed a burden with a "deterrent effect" on free speech.[290] By contrast, intermediate scrutiny allows the government considerably

286. *Id.* § 2(g)(3)(A)(ii), 138 Stat. at 958–59.

287. Citizens United v. FEC, 558 U.S. 310, 340 (2010) ("Prohibited, too, are restrictions distinguishing among different speakers, allowing speech by some but not others."); Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 659 (1994) (confirming that speaker-based regulation itself often suffices to trigger First Amendment review because "[r]egulations that discriminate among media, or among different speakers within a single medium, often present serious First Amendment concerns").

288. *Garland*, 604 U.S. at 79–80 (relying on concerns about data collection practices to justify regulating TikTok's recommendation algorithm).

289. *See, e.g.*, United States v. Playboy Ent. Grp., 529 U.S. 803, 813 (2000) ("If a less restrictive alternative would serve the Government's purpose, the legislature must use that alternative."); Ashcroft v. ACLU, 542 U.S. 656, 665 (2004) ("A statute that 'effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another . . . is unacceptable if less restrictive alternatives would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve.'" (quoting Reno v. ACLU, 521 U.S. 844, 874 (1997))).

290. Lamont v. Postmaster Gen., 381 U.S. 301, 307 (1965).

more leeway.[291] The government need only show that the law furthers an important interest unrelated to speech suppression and does not burden substantially more speech than is necessary to serve that interest.[292] By treating the statute as content-neutral, the Court sidestepped the higher bar of strict scrutiny, allowing the government more discretion to address pro-China content and speech on TikTok.

2. National Security Under the Strict Scrutiny Scenario

The Court draws a distinction between the content-neutral approach and the content-based approach by invoking the government's national security concerns. TikTok's ownership by a company from a designated foreign adversary, the platform's capacity to collect sensitive data from U.S. users, and the resulting national security implications together create a distinct regulatory profile in the Court's mind.[293] Under this view, PAFACA's divestiture mandate addresses infrastructural risks arising from the platform's foreign ownership rather than from the platform's speech or expressive content.

National security, while unquestionably a compelling interest, does not guarantee that the government would prevail under strict scrutiny. The difficulty lies in the requirement of narrow tailoring. In *United States v. Robel*, the Court invalidated a Cold War–era statute that barred all members of the Communist Party from employment in defense facilities.[294] Although the government invoked national security as its justification, the Court concluded that such a sweeping prohibition was not narrowly tailored because it indiscriminately excluded individuals from entire sectors of employment without considering less restrictive alternatives. Even in *Holder v. Humanitarian Law Project*, where the Court acknowledged the government's interest in preventing terrorism as compelling and ultimately upheld the statute at issue,[295] the Court

---

291. Bhagwat, *supra* note 248.

292. *Garland*, 604 U.S. at 70 ("Under that standard, we will sustain a content-neutral law if it advances important governmental interests unrelated to the suppression of free speech and does not burden substantially more speech than necessary to further those interests.").

293. *Id.* at 72 ("The Government also supports the challenged provisions with a content-neutral justification: preventing China from collecting vast amounts of sensitive data from 170 million U. S. TikTok users.").

294. United States v. Robel, 389 U.S. 258, 262–68 (1967).

295. *Id.* at 266 (contending that part of the law "contains the fatal defect of overbreadth because it seeks to bar employment both for association which may be proscribed and for association which may not be proscribed consistently with First Amendment rights"); Holder v. Humanitarian L. Project, 561 U.S. 1, 4 (2010) (noting both the plaintiff and the defendant "agree that the Government's interest in combating terrorism is an urgent objective of the highest order").

conceded that it "must [apply] a more demanding standard" than intermediate scrutiny.[296]

These precedents cast doubt on the constitutionality of the TikTok ban if reviewed under strict scrutiny: A blanket ban on an entire expressive platform like TikTok appears excessively broad, as it imposes a burden on millions of speakers and listeners alike, regardless of whether their activity poses any national security risk. Similarly, in *Marland v. Trump*, a challenge by TikTok users to one of President Trump's TikTok executive orders in his first term, the district court drew from *City of Ladue v. Gilleo* to observe that "even if the Commerce Identification were a content-neutral regulation, this would not render it immune from First Amendment scrutiny . . . 'Although prohibitions foreclosing entire media may be completely free of content or viewpoint discrimination, the danger they pose to the freedom of speech is readily apparent—by eliminating a common means of speaking, such measures can suppress too much speech.'"[297] Therefore, as PAFACA forecloses an entire medium of communication, such broad coverage of speech makes it difficult to argue that the Act is narrowly tailored to the asserted national security threat under strict scrutiny.

This analysis illustrates that national security can be a compelling interest, but it does not automatically override First Amendment protections, especially under strict scrutiny. If strict scrutiny was applied to PAFACA, the government's burden becomes far more difficult to sustain. It would need to show that divestiture, or platform removal, is narrowly tailored to an actual risk of foreign manipulation, and that no less speech-restrictive alternative could address that risk. There is no sufficient evidence to presume that the government deliberately framed its regulation as content-neutral to evade strict scrutiny; however, if PAFACA were subject to strict scrutiny, the government would bear a significantly heavier burden. By contrast, under intermediate scrutiny, the Act stood a far better chance of surviving constitutional review, which, indeed, it did.

3. The Extent of Judicial Deference

While the Supreme Court accepted the government's national security justification under intermediate scrutiny,[298] the more difficult

296. *Id.*

297. Marland v. Trump, 498 F. Supp. 3d 624, 638 n.6 (E.D. Pa. 2020) (quoting City of Ladue v. Gilleo, 512 U.S. 43, 55 (1994)).

298. *Garland*, 604 U.S. at 72 ("The Government also supports the challenged provisions with a content-neutral justification: preventing China from collecting vast amounts of sensitive data from 170 million U. S. TikTok users.").

question is whether even intermediate scrutiny permits reliance on "predictive judgments" in the absence of demonstrated evidence,[299] and, if so, what threshold of proof such reliance should demand. This issue was left largely unexamined in *TikTok v. Garland*.

The Court relied on the government's predictive judgments about anticipated future national security harms not yet supported by concrete or observable evidence.[300] The Court treated Congress's predictive judgments as sufficiently plausible to justify the enactment of PAFACA, "afford[ing] the Government's informed judgment substantial respect here" and dismissing TikTok's claim that the government's data-related concerns were speculative.[301] It pointed to evidence of the Chinese government's efforts to obtain data on U.S. persons,[302] as well as to suspicions that China could have access to the locations and contact information of federal employees and contractors, allowing China to conduct corporate espionage.[303] It is notable that the Court deferred to the government's judgments based only on publicly available information and required no production of classified intelligence.[304] In other words, even unclassified assertions of national security risk were deemed sufficient to justify predictive judgments of national security concerns. On the strength of these disclosures, Justice Gorsuch, in his concurrence, concluded that the government's national security concern was not merely speculative.[305]

---

299. Scholars have variously described this phenomenon with terms such as "threat inflation," "preemptive regulation," or "predictive judgments," highlighting the tendency to legislate against unseen or speculative risks in the name of national security. *See, e.g.*, Eichensehr & Hwang, *supra* note 213, at 587 (calling the phenomenon "predictive judgment"); Adam Thierer, *Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle*, 14 MINN. J. L., SCI. & TECH. 309, 317–31 (2013) (discussing how "threat inflation" fosters anticipatory restrictions based on predictive assessments of risk). In this Article, we adopt the Court's own terminology in the *TikTok Inc. v. Garland* decision, which framed the government's reasoning in terms of "predictive judgment." 604 U.S. at 75.

300. *See, e.g.*, Lewis, *supra* note 31 ("[TikTok] could be used for espionage purposes, to identify targets for recruitment, but again, there is no evidence that China has done this."); *Garland*, 604 U.S. at 85 (Gorsuch, J., concurring) (stating that "[w]hether this law will succeed in achieving its ends, I do not know," and noting a lack of "certainty . . . about the arguments and record before us").

301. *Garland*, 604 U.S. at 75 (majority opinion).

302. *Id.* ("China has engaged in extensive and years-long efforts to accumulate structured datasets, in particular on U.S. persons, to support its intelligence and counterintelligence operations.").

303. *Id.* at 74–75.

304. *Id.* at 74 n.3 ("Our holding and analysis are based on the public record, without reference to the classified evidence the Government filed below.").

305. *Id.* at 83–84 (Gorsuch, J., concurring in judgment) (acknowledging that "assessing exactly what a foreign adversary may do in the future implicates 'delicate' and 'complex' judgments about foreign affairs and requires 'large elements of

Judicial deference without concrete evidence of national security risks is hardly a novelty in American constitutional practice. *Korematsu v. United States* is a notable instance in which the Supreme Court accepted governmental assertions of national security necessity without evidentiary support, namely the lack of evidence of actual disloyalty from Japanese Americans during World War II.[306] The Court's reasoning in this case was closely shaped by the highly sensitive political environment in which it was decided and reflects wartime political psychology: The attack on Pearl Harbor triggered sustained fear of Japanese advances in the Pacific theater, newspapers and state officials circulated claims of "fifth-column" activity, and mass internment was widely recast as a matter of "military necessity."[307] Although Justice Murphy in his dissent made clear that the courts had been presented with no factual record on which to base the exclusion order,[308] the majority opinion nonetheless accepted the military's judgment, concluding that the Court could not reject the judgment of the military authorities and of Congress as unfounded.[309]

Deference to national security concerns based on predictions about what could occur in the future, rather than on demonstrated harm, is also not new.[310] Two decades ago, in *Turner Broadcasting System, Inc. v. FCC*, the Supreme Court articulated a posture of judicial restraint toward congressional predictive judgments.[311] There, the Court emphasized that it was not the role of the judiciary to reweigh conflicting legislative evidence or substitute its own factual conclusions.[312] Instead, it limited its review to whether the legislature's judgment was "reasonable and supported by substantial evidence in the record before

---

prophecy[,]'" but that "the record the government has amassed in these cases after years of study supplies compelling reason for concern").

306. 323 U.S. 214, 223–24 (1944).

307. Patricia Miye Wakida, *How a Public Media Campaign Led to Japanese Incarceration During WWII*, PBS (Sep. 23, 2021), https://www.pbs.org/wgbh/americanexperience/features/citizen-hearst-japanese-incarceration [https://perma.cc/JPP9-4AT2] ("The U.S. government claimed that the possibility of sabotage, espionage and fifth-column activity made the removal of Japanese Americans a military necessity.").

308. *Korematsu*, 323 U.S. at 236 (Murphy, J., dissenting) ("[N]o reliable evidence is cited to show that such individuals were generally disloyal.").

309. *Id.* at 218 (majority opinion).

310. *See* Eichensehr & Hwang, *supra* note 213, at 587 (highlighting that "[t]he Supreme Court has been particularly deferential in circumstances where *predictive* judgments about national security are involved").

311. 520 U.S. 180, 196 (1997) ("We owe Congress' findings an additional measure of deference out of respect for its authority to exercise the legislative power.").

312. *Id.* at 199 ("The Constitution gives to Congress the role of weighing conflicting evidence in the legislative process."); *id.* at 211 ("[W]e are not to 'reweigh the evidence *de novo*, or to replace Congress' factual predictions with our own.'").

Congress."[313] This deferential standard enables Congress to legislate in complex policy domains, such as media regulation, without the burden of conclusive proof.

TikTok v. Garland both echoes and extends this view. First, citing a previous iteration of the *Turner* case, the Court observed that "[s]ound policymaking often requires legislators to forecast future events . . . based on deductions and inferences for which complete empirical support may be unavailable."[314] The Court then pointed to the record's reference to China's long-term efforts to acquire data on U.S. persons to support its intelligence operations as sufficient factual grounding.[315] That reference, though generally about the Chinese government and not directly tied to TikTok, was deemed adequate to sustain the congressional judgment.[316] While the *Turner* framework originally demanded a record of "substantial evidence"[317] to justify speech restrictions, the *Garland* Court instead embraced the more deferential posture that later defined the doctrine's subsequent evolution. The Court in *Garland* insists that its decision rests entirely on the public record,[318] even where the underlying assessments are necessarily predictive in nature.[319] This logic opens the door to a new mode of predictive judgment and preemptive regulation in which the government is not asked to demonstrate actual misuse of data or direct foreign coercion, but rather is permitted to legislate based on what adversaries *might* do or what platforms *could* enable. In a world where most foreign actors engage in intelligence gathering activities, the line between justified concern and generalized suspicion becomes increasingly difficult to draw.

The Court's broad deference to the government's national security justifications reveals a deeper anxiety about technological uncertainty or even judicial incapacity in evaluating the risks posed by algorithmic systems. The perceived threat from TikTok remains latent or unseen and lies beyond the current scope of detection. As the Court acknowledges, "[t]he Government has further noted the difficulties associated with

313. *Id.* at 211.
314. TikTok Inc. v. Garland, 604 U.S. 56, 75 (2025) (per curiam) (quoting Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 665 (1994)).
315. *Id.*
316. *Id.*
317. *Id.*
318. *Id.* at 74 n.3 ("Our holding and analysis are based on the public record, without reference to the classified evidence the Government filed below.").
319. *Id.* at 74–75 (pointing to Chinese intelligence activities as justification without specific evidence that those activites were conclusively conducted on TikTok).

monitoring data sharing between ByteDance Ltd. and TikTok Inc."[320] This inability to verify whether structural separation is genuine becomes, paradoxically, a reason to demand ever more stringent forms of decoupling, justified by national security.

This posture also extends the view articulated in *Holder v. Humanitarian Law Project* ("*HLP*"). In *HLP*, the Supreme Court allowed the government to prohibit Americans from providing advocacy and legal guidance to foreign terrorist groups on the ground that such speech might indirectly advance hostile foreign interests.[321] Although TikTok, unlike the plaintiffs in *HLP*, is not engaged in activities linked to terrorism or violence, the Court nonetheless invoked the same analytical caution: "We are mindful that this law arises in a context in which national security and foreign policy concerns arise in connection with efforts to confront evolving threats in an area where information can be difficult to obtain and the impact of certain conduct difficult to assess."[322] The D.C. Circuit similarly deferred to Congress's national security rationale, pointing out that policymaking often requires anticipating future risks without complete empirical evidence.[323] This holding signals the broadening reach of national security deference, extending judicial restraint from counterterrorism to the structural regulation of expressive platforms.

It is worth observing that the Court's deference to national security interests reflects a priori, and often volatile, understandings of threats that are shaped by broader political dynamics and public sentiment.[324] The national security concerns surrounding TikTok were not initially judicially accepted. In *Marland v. Trump*, the district court noted that the government described the potential risks as hypothetical and stated that ByteDance's ties to the Chinese government "could potentially be leveraged" or that the Chinese government could "compel TikTok

320. *Id.* at 80.

321. Holder v. Humanitarian L. Project, 561 U.S. 1, 36 (2010).

322. *Garland*, 604 U.S. at 75 (quoting *Holder*, 561 U.S. at 34).

323. *See* TikTok Inc. v. Garland, 122 F.4th 930, 960 (D.C. Cir. 2024) ("The Congress was entitled to address the threat posed by TikTok directly and create a generally applicable framework, however imperfect, for future use. It would be inappropriate to 'punish' the Congress for attempting to address future national security threats by inferring an impermissible motive.").

324. *See* Marland v. Trump, 498 F. Supp. 3d 624, 633 n.2 (2020) (declining to engage with hypothetical national security harms, characterizing such inquiries as "impermissibly advisory," and citing *Chafin v. Chafin*, 568 U.S. 165, 172 (2013), to suggest that "[f]ederal courts may not . . . give 'opinion[s] advising what the law would be upon a hypothetical state of facts'").

to provide" access to user data.[325] The court found such conjectural language insufficient to substantiate a national security threat and concluded that the record did not support the government's asserted urgency in banning the application.[326] As this case shows, the factual basis of the government's national security concerns remained initially uncertain. PAFACA marked a decisive shift. Passed by Congress in 2024 with overwhelming bipartisan support, by a vote of 352 to 65 in the House and 79 to 18 in the Senate,[327] the Act reflected the increasingly bipartisan consensus on the technological and national-security issues presented by TikTok. After its passage, the national security threat once deemed speculative by courts was reconstituted almost as a political fact, one embraced by Congress, the executive branch, and public policy discourse as an accepted premise.

In summary, the Court's reasoning in *TikTok v. Garland* affirms that the TikTok ban implicates expressive rights but stops short of demanding strict scrutiny and a heightened evidentiary threshold. By accepting potential national security risks as sufficient justification under intermediate scrutiny, the Court's upholding of PAFACA reflects significant deference to the legislature.

C. Same Recipe, Different Companies: From Huawei to TikTok

While the TikTok ban has acquired unusual visibility due to the platform's social media nature and the case's judicial escalation to the Supreme Court, it is far from the first time the United States has mobilized national security law to constrain a foreign adversary. PAFACA and the litigation over its constitutionality reflects recurring themes that have long structured American responses to foreign technology firms. First, judicial deference, a stance deeply rooted in national security concerns, continues to shield executive and legislative assessments from searching review. And second, use of predictive judgments in crafting regulation, an approach that was adopted in earlier restrictions against Chinese

325. *Id.* at 642; *see id.* at 630–31 ("President Trump identified a risk that the People's Republic of China (the 'PRC') and the Chinese Communist Party (the 'CCP') could use TikTok to access . . . Americans' personal information for blackmail, and conduct corporate espionage.").

326. *Id.* at 642 ("[T]he Government's own descriptions of the national security threat . . . are phrased in the hypothetical."); *id.* at 636–43 (finding plaintiffs have a likelihood of success on their IEEPA informational-materials exception claim and granting a preliminary injunction).

327. Lauren Peller et al., *House Passes Bill That Would Ban TikTok if Its Chinese Owners Don't Sell the Popular App*, ABC News (Mar. 13, 2024), https://abcnews.go.com/Politics/house-passes-bill-ban-tiktok-chinese-owners-sell/story?id=108077695 [https://perma.cc/5CZW-63RW] (House vote); S. Roll Call Vote 154, 118th Cong., 2d Sess., 170 Cong. Rec. S2992 (Apr. 23, 2024) (Senate vote).

hardware companies like Huawei, has since extended from the physical layer of infrastructure to the content layer of digital platforms.

1. Extending a Predictive Judgment Approach from Huawei to TikTok

The United States has long maintained systematic restrictions on foreign ownership, control, and influence across platform-like sectors, such as banking, communications, transportation, and energy.[328] Such restrictions are not limited to China.[329] Nevertheless, the legal and policy lineage of PAFACA can be traced to earlier executive and legislative actions targeting Chinese telecommunications companies, namely Huawei and ZTE. Both companies originally provided critical hardware for U.S. telecommunications infrastructure, including switches, routers, and other network components that constitute the physical backbone of wireless and 5G systems.[330]

As early as 2012, the U.S. House Intelligence Committee had flagged both Huawei and ZTE as potential vectors of foreign surveillance, urging federal and private actors to avoid engagement.[331] After a yearlong investigation, the Committee released a report alleging that both companies were implicated in economic espionage and "potential violations" of immigration, bribery, corruption, and copyright infringement laws.[332] Although the report provided no direct evidence that either Huawei or ZTE acted to compromise the security of American clients, it nonetheless concluded that "Huawei and ZTE cannot be trusted to be free of foreign state influence,"[333] given their close relationship to, and

328. *See* Sitaraman, *supra* note 10, at 1106–27 (2022) (detailing historic restrictions on foreign platforms).

329. *See, e.g.*, 50 U.S.C. § 4565 (authorizing presidential blocking of foreign acquisitions on national security grounds); Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), Pub. L. No. 115-232, 132 Stat. 2173 (expanding CFIUS review of critical technology and infrastructure); Defense Production Act of 1950, 50 U.S.C. §§ 4501 et seq. (prioritizing control over key resources in times of emergency); Merchant Marine (Jones) Act of 1920, 46 U.S.C. § 55102 (restricting foreign ownership in U.S. maritime transport).

330. *See generally* JILL C. GALLAGHER, CONG. RSCH. SERV., R47012, U.S. RESTRICTIONS ON HUAWEI TECHNOLOGIES: NATIONAL SECURITY, FOREIGN POLICY, AND ECONOMIC INTERESTS, at ii (2022) (discussing Huawei and ZTE's significant presence in global markets and the security risks their hardware presents for U.S. network infrastructure).

331. Kim Zetter, *Report: Chinese Tech Firms Should Be Viewed with Suspicion, Barred from U.S. Networks*, WIRED (Oct. 8, 2012), https://www.wired.com/2012/10/chinese-telecoms-suspicious [https://perma.cc/8M37-352Z].

332. H.R. PERMANENT SELECT COMM. ON INTEL., 112TH CONG., INVESTIGATIVE REPORT ON THE U.S. NATIONAL SECURITY ISSUES POSED BY CHINESE TELECOMMUNICATIONS COMPANIES HUAWEI AND ZTE 34–35 (2012).

333. *Id.* at 45.

heavy financial funding from the Chinese government.[334] The report's rationale was that even a reasonable suspicion could justify scrutiny, on the grounds that surveillance technology embedded in hardware, such as routers and switches, is difficult to detect.[335] Subsequent enforcement culminated in the 2019 designation of Huawei to the Entity List under the Export Administration Regulations (EAR).[336] In 2021, Biden signed the Secure Equipment Act of 2021, which mandated the Federal Communications Commission ("FCC") to establish clear regulations stipulating that licenses will no longer be granted for any telecommunications equipment deemed to present an unacceptable risk to national security.[337] This Act represents a pivotal step in safeguarding the nation's communications infrastructure against potential threats. The FCC further tightened its oversight of Chinese telecommunications firms, culminating in orders such as FCC 22-84, which barred new equipment authorizations for Huawei, ZTE, and other companies deemed high-risk suppliers.[338]

The belief that reasonable suspicion alone suffices to justify restrictions on Chinese hardware companies laid the foundation for a broader U.S. regulation of Chinese digital platforms. The TikTok ban reflects this extension. While restrictions against Huawei and ZTE targeted the physical layer of network architecture, the TikTok ban represents a shift to the content layer, where the national security concerns lie in potential manipulation of data flows and information exposure. Both types of restrictions share the view that government intervention does not require demonstrated harm and that the mere plausibility of risk is sufficient to justify intervention.

---

334. Michael S. Schmidt, Keith Bradsher & Christine Hauser, *U.S. Panel Cites Risks in Chinese Equipment*, N.Y. Times (Oct. 8, 2012), https://www.nytimes.com/2012/10/09/us/us-panel-calls-huawei-and-zte-national-security-threat.html [https://perma.cc/4ACN-RG77].

335. Tom Simonite, *Why the United States Is So Afraid of Huawei*, MIT Tech. Rev. (Oct. 9, 2012), https://www.technologyreview.com/2012/10/09/85048/why-the-united-states-is-so-afraid-of-huawei/ [https://perma.cc/3KJK-HNPA].

336. Addition of Entities to the Entity List, 84 Fed. Reg. 22961 (May 21, 2019) (codified at 15 C.F.R. pt. 744). Placement on the Entity List is determined through an inter-agency review led by the Department of Commerce's End-User Review Committee. *Id.* The legal standard requires only "reasonable cause to believe, based on specific and articulable facts" that the entity poses national-security risks, including acting "contrary to the national security or foreign policy interests of the United States." *Id.*

337. Secure Equipment Act of 2021, 47 U.S.C. § 1601.

338. FCC, Report and Order, FCC 22-84, ET Docket No. 21-232, EA Docket No. 21-233 (Nov. 25, 2022).

2. *Extending Judicial Deference from Huawei to TikTok*

PAFACA marks a categorical expansion of national security concerns from the physical layer to the content layer.[339] But the broadening of national security restrictions on Chinese companies from hardware companies to internet platforms has encountered distinctive resistance. Unlike telecommunications hardware, the internet is both a conduit of and a participant in expressive activity. It is therefore embedded in a normative landscape shaped by long-standing commitments to openness, interoperability, and minimal state interference.[340] These ideological and cultural frames render structural restrictions on foreign internet platforms more politically and legally contestable than analogous measures in sectors whose functions are primarily technical or physical.

However, the shift also reflects a growing conviction within U.S. policy circles that such digital platforms, too, pose systemic risks, specifically through foreign access to user data and the potential for content manipulation at scale.[341] The regulatory instruments have evolved accordingly. Whereas export controls and entity list designations once targeted supply chains,[342] PAFACA operates by mandating app store removal, banning web hosting, and compelling corporate divestiture.[343] Yet, the underlying logic remains the same:

---

339. *See* Lawrence B. Solum & Minn Chung, *The Layers Principle: Internet Architecture and the Law*, 79 NOTRE DAME L. REV. 815, 847–49 (2004) (adopting Benkler's three-layer model of internet architecture, comprising a physical layer of infrastructure, a logical layer of protocols and software standards, and a content layer of data and communicative transactions).

340. *See* John Perry Barlow, *A Declaration of the Independence of Cyberspace*, 18 DUKE L. & TECH. REV. 5, 5 (2019) (originally published on Feb. 8, 1996) (describing cyberspace as "consist[ing] of transactions, relationships, and thought itself," a realm inherently committed to openness, free expression, and independence from state sovereignty); David Johnson & David Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1370 (1996) (describing how cyberspace lacks any territorial borders); Marjory S. Blumenthal & David D. Clark, *Rethinking the Design of the Internet: The End-to-End Arguments vs. the Brave New World*, 1 ACM TRANSACTIONS ON INTERNET TECH. 70, 74 (2001) (arguing that several end-to-end principles form the core of the "Internet philosophy": "freedom of action, user empowerment, end-user responsibility for actions undertaken, and lack of controls 'in' the Net that limit or regulate what users can do").

341. *See, e.g.*, Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, div. H, 138 Stat. 955, 956 (2024).

342. *See* sources cited *supra* note 329 (statutory authorities for restricting foreign ownership and supply chains); *see also* H.R. PERMANENT SELECT COMM. ON INTEL., *supra* note 332 (describing the threat that Huawei and ZTE pose to U.S. telecommunications infrastructure).

343. *See* Protecting Americans from Foreign Adversary Controlled Applications Act, div. H, 138 Stat. at 956.

The United States responds to the perceived entanglement of foreign ownership and national vulnerability with increasingly "anticipatory" forms of exclusion.[344] Furthermore, like the TikTok ban, restrictions on hardware from Huawei and ZTE are primarily designed to prevent the flow of sensitive data to foreign adversaries.[345] Therefore, regulations targeting both physical equipment and digital platforms originating from China are implemented to address the same concern about data transmission to Chinese authorities for potential espionage purposes.

Judicial deference to the legislative and executive branches in national security cases long predates the enactment of PAFACA or the legal controversies surrounding the TikTok ban.[346] Courts have consistently upheld the government's discretion to assess foreign threats without demanding granular disclosure of classified intelligence. This is evident in *Huawei v. FCC*, in which Huawei and ZTE challenged the FCC's designation of them as national security threats. The Fifth Circuit upheld the FCC's authority to restrict funding for equipment from companies posing national security risks.[347] Notably, while Huawei asserted that "the FCC lacks the relevant national security expertise,"[348] the Fifth Circuit ultimately upheld the FCC's authority to restrict federal subsidies based on national security concerns, as the FCC incorporated judgments from expert executive agencies and congressional mandates.[349]

What emerges from the Huawei, ZTE, and TikTok cases is a broader pattern: Courts are largely deferential to executive and legislative assessments of security threats, even when such assessments rest on evidence that is not fully disclosed or subject to examination in an adversarial proceeding. In *Huawei*, the FCC submitted a Classified Appendix as evidence of detailed justifications, yet it was unavailable to the plaintiffs.[350] Crucially, the court did not question the legitimacy

344. *See generally* Thierer, *supra* note 299, at 358–59 (introducing the concept of anticipatory regulation, which "attempts to deal with technological risk by controlling or curbing the uses of that technology").

345. BRADFORD, *supra* note 1, at 192–93.

346. *See supra* Section III.A.2.

347. Huawei Techs. USA, Inc. v. FCC, 2 F.4th 421, 443 (5th Cir. 2021) ("[A]s the agency contends, the authority it exercises under the rule closely resembles the kind of national security authority it has exercised for decades—limited, communications-focused judgment informed by expert agencies and deferential to their views.").

348. *Id.*

349. *Id.* ("That is, the FCC's judgments under the rule are informed by agencies with much more expertise than the FCC on these matters.").

350. FCC Response to Court Order at 15 n.5, Huawei Tech. USA, Inc. v. FCC, 2 F.4th 421 (5th Cir. 2020) (No. 19-60896) ("Respondents lodged the Classified Appendix that supported the Commission's initial designation of Huawei ex parte and in camera

or sufficiency of the appendix, nor did it require public elaboration.[351] Likewise, when asked to explain the precise nature of the national security threat posed by TikTok, the government invoked classification barriers, stating that the relevant materials could not be disclosed publicly.[352] This judicial deference is not unique to Huawei, ZTE, or TikTok. It reflects a consistent jurisprudential tradition. Courts, when confronted with inter-branch consensus on national security, typically decline to substitute their own risk assessments, even where the evidence remains abstract.

IV. Doctrinal Implications

This Section examines two doctrinal implications of the TikTok ban in terms of an ostensible narrowing of free speech and a seemingly expanded posture of judicial deference in cases invoking predictive national security risks. Both moves reflect the judiciary's attempt to accommodate the new national security risks associated with data security. But it should be cautioned that extending the *Garland* decision's logic beyond its context would risk normalizing broad governmental assertions of national security in contexts where exceptional circumstances, namely acute geopolitical tensions, are absent.

It highlights that judicial deference in response to a thinly supported national security interest may look different if we take into account how the medium of free expression has changed. The shift from printing culture to algorithmic distribution has changed how foreign adversaries can influence public discourse. A recommendation system that continuously shapes what content users interact with is a qualitatively different security risk than pamphlets, as pamphlets also do not allow for the collection of granular user data like digital platforms do. In this sense, the Court's expansion of its deference doctrine can be considered an adjustment to an escalated threat environment.

Nevertheless, while the inherent opacity of modern digital environments may make providing concrete evidence of actual data transfers or manipulations impractical, this technological complexity should

---

on or around June 9, 2020, to be transported to the Fifth Circuit's Clerk's Office through the Classified Information Security Officer to the Courts.").

351. *Huawei Techs. USA, Inc.*, 2 F.4th at 455 (demonstrating judicial deference by holding that the FCC "has the better argument" in its decision to employ a company-based prohibition, rather than a risk-based approach, without independently verifying the evidentiary sufficiency of the Classified Appendix or requiring the government to further substantiate its claims).

352. *See* TikTok Inc. v. Garland, 122 F.4th 930, 946 (D.C. Cir. 2024) ("Portions of the Government's brief and evidentiary submission were redacted because they contain classified information.").

not serve as a blank check for judicial deference. To avoid lapsing into an increasingly speculative posture, the judiciary should move towards a more rigorous framework by establishing standardized criteria for evaluating the legitimacy of national security risks. TikTok creates a quandary the doctrine has not previously confronted: Whether judicial deference should expand or contract as the risks grow more uncertain and speculative.

A. When an Expressive Platform Becomes Content-Neutral

TikTok is a distinct social media platform in two ways. First, it exemplifies the conventional internet ethos of an open platform where expression flows with minimal governmental constraints.[353] However, TikTok utilizes an algorithmic recommendation system that is subject to a foreign sovereign's control and thus is potentially susceptible to foreign influence. As such, the presumption of TikTok's openness collides with the very nature of its business model. The more the platform collects user data and uses algorithmic recommendation, the more room it leaves for the exercise of foreign influence and control.

If the U.S. government's intervention was confined to limit certain functions of TikTok's algorithm or data storage infrastructure, such regulation might have been more acceptable to the public and posed less constitutional concern.[354] However, PAFACA imposed a blanket ban on the platform.[355] Therefore, the issue the Supreme Court faced in *TikTok v. Garland* was whether the government was justified in sacrificing the platform's broad expressive function and any user-generated content not implicated by foreign influence in order to restrict TikTok's data collection and algorithmic recommendation systems, which may be subject to Chinese government influence. After all, a substantial amount

353. *See generally* Barlow, *supra* note 340 (describing cyberspace as a realm inherently committed to openness, free expression, and independence from state sovereignty).

354. A familiar illustration comes from the federal response to Russian interference in the 2016 U.S. election. There, the government did not ban Facebook or Twitter as expressive platforms but, instead, sanctioned the specific actors and manipulative mechanisms that were believed to distort political discourse. *Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections*, U.S. DEP'T OF THE TREASURY (Mar. 15, 2018), https://home.treasury.gov/news/press-releases/sm0312 [https://perma.cc/CZ5T-QXQL] (sanctioning the Internet Research Agency and specific individuals for information warfare). Pew Research found that "75% of Americans say it's likely that Russia or other governments will try to influence 2020 election." Hannah Hartig, *75% of Americans Say It's Likely that Russia or Other Governments Will Try to Influence 2020 Election*, PEW RSCH. CTR. (Aug. 18, 2020), https://www.pewresearch.org/short-reads/2020/08/18/75-of-americans-say-its-likely-that-russia-or-other-governments-will-try-to-influence-2020-election/ [https://perma.cc/5C2D-PQ37].

355. *See* Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, div. H, § 2(a), 138 Stat. 955 (2024).

of content on TikTok is neither politically sensitive nor plausibly connected to foreign state manipulation,[356] from pet videos to cooking tutorials to personal diaries. Yet, under PAFACA's blanket ban, all of this content would be equally restricted. Unfortunately, in *Garland*, the Court drew on PAFACA's blanket ban approach to selectively frame the vast body of impacted non-political content on TikTok as evidence that the statute did not target specific viewpoints or subject matter.[357] TikTok's vast amounts of varied content became a constitutional cover for framing PAFACA as content-neutral even though PAFACA indeed targets a specific category of content, that is content presumed to be influenced by Chinese state.

The Court's selective framing carries significant implications for First Amendment doctrine. First, content-neutral restrictions have traditionally been confined to *time, place, or manner* regulations that narrow, but do not ban, expressive opportunities.[358] In prior cases dealing with content-neutral restrictions, the Court upheld regulations when they left open alternative channels of communication.[359] Even in *City of Renton v. Playtime Theatres*, where adult theaters were zoned away from certain locations, the regulation only limited the location of the adult theaters rather than eradicated the existence of adult theaters.[360] Under the content-neutral approach, PAFACA's attempt to either force divestiture or ban TikTok as an entire expressive platform does not leave open ample alternative channels of communication. Instead of regulating *how* speech is expressed, it eliminates an entire platform of expression.[361] The Court's upholding of PAFACA as content-neutral

356. Colleen McClain, Monica Anderson & Risa Gelles-Watnick, *How TikTok Users View, Experience the Platform*, Pew Rsch. Ctr. (June 12, 2024), https://www.pewresearch.org/internet/2024/06/12/how-tiktok-users-view-experience-the-platform [https://perma.cc/SH68-ZV8T] (suggesting that 95% of TikTok users indicate that "they go on the platform because it's entertaining").

357. *See* TikTok Inc. v. Garland, 604 U.S. 56, 73 (emphasizing a content-neutral justification for the law by pointing out it is "based on a content-neutral data collection interest").

358. Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989).

359. *Id.* at 802 (pointing out the restrictive guideline "leaves open ample alternative channels of communication" rather than banning any particular type of expression); Frisby v. Schultz, 487 U.S. 474, 488 (1988) (noting that the ordinance "also leaves open ample alternative channels of communication and is content-neutral").

360. City of Renton v. Playtime Theatres, Inc., 475 U.S. 41, 43 (1986). *Renton*'s classification as content-neutral has itself been questioned. *See* Reed v. Town of Gilbert, 576 U.S. 155, 184 (2015) (Kagan, J., concurring in judgment) (noting that *Renton* applied intermediate scrutiny to a zoning law that "facially distinguished among movie theaters based on content").

361. *See* Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, div. H, § 2(a), 138 Stat. 955 (2024).

normalizes such an extension, risking that content-neutral doctrine will migrate into speech that is traditionally more strictly regulated.

Second, the Court's selective framing functions as a doctrinal shortcut. Once a restriction is framed in terms of a predictive judgment that foreign adversaries may exercise influence over an expressive platform, courts may be inclined to treat it as content-neutral, allowing the government to circumvent the burden of strict scrutiny. Under this logic, the government could invoke the same rationale in future restrictions against platforms such as YouTube, Meta, or X, which under an expansive reading of the Court's rationale, could be characterized as presenting analogous structural risks.

TikTok's distinctiveness as a social media platform that is subject to the Chinese government's control and influence may render PAFACA and *Garland* less easily transferable to non-China-based platforms. But the Court's holding in *Garland* still risks the familiar danger of a "hard case making bad law,"[362] or an exceptional set of circumstances giving rise to doctrinal changes that have structural consequences that extend far beyond the dispute at hand. In the case of *Garland*, there was an exceptional circumstance in the form of a strong national security claim tied to geopolitical tensions between the United States and China. This exceptional circumstance provided justifications for finding a total ban of a social media platform to be content-neutral and for allowing the government to rely on predictive judgments of national security risks to satisfy its burden under intermediate scrutiny. This holding opens the door for lower courts or administrative agencies to sign off on government assertions of national security to justify restrictions in future cases without similarly exceptional circumstances that were present in TikTok's case.

B. When Predictive National Security Reasoning Expands

Although the Supreme Court has historically deferred to the legislative and executive branches in cases invoking national security,[363] such deference has not previously been extended to concerns about digital platforms or online expression. Similarly, the Supreme Court has not previously dealt with what level of predictive judgment, if any, is allowed to sustain national security concerns about digital platforms. TikTok's nature as an internet platform gives it a speech dimension that

362. Sepehr Shahshahani, *Hard Cases Make Bad Law? A Theoretical Investigation*, 51 J. LEGAL STUD. 135, 140 (2022) (explaining that "hard" in the maxim "hard cases make bad law" can be "a case that is not readily resolvable by reference to precedent or other authorities").

363. *See supra* Section III.A.2.

earlier national security cases did not confront, leaving open, at least in theory, a narrow space for judicial pushback in defense of speech interests. *Garland* marks the first time the Supreme Court has allowed the government to disable an entire expressive platform due to predictive national security concerns.

What appears at first glance to be an expanded form of judicial deference in *Garland* should not be understood as a sudden departure from First Amendment doctrine. Instead, *Garland* reflects an adjustment prompted by a transformation in the technological conditions that changed national security risks. The focus of national security concerns has shifted from discrete instances of ideological dissemination to continuous, large-scale information campaigns made possible by social media platforms powered by algorithmic recommendation systems. As the type of risk changes, the evidentiary and remedial baselines against which national security claims are evaluated shift too. Even decades ago, before the advent of technically complex data security issues, foreign affairs exceptionalists cautioned that judicial intervention into predictive judgments of national security would yield a "muddy and potentially destabilizing message produced by a group of non-experts."[364] In today's intricate digital ecosystem, where cyber-espionage and algorithmic influence are notoriously difficult to detect, the sheer difficulty of capturing concrete evidence in a "black box" environment has become a convenient justification for a posture of judicial deference. Therefore, the aggregated judicial deference to unsubstantiated national security risks can be seen as an accommodation to a new risk environment.

A useful point of comparison is *Lamont v. Postmaster General*. During the Cold War, Congress amended the Postal Act to require that any printed materials deemed "communist political propaganda" be detained by the post office unless the addressee affirmatively requested delivery.[365] The Supreme Court invalidated the law as unconstitutional.[366] But the information environment has changed dramatically since the 1960s. Compared to the occasional flow of printed propaganda through the mail, social media platforms powered by algorithmic recommendation systems exert influence with a reach and immediacy far exceeding the capacity of traditional mediums to traverse time and space.[367] The national security risks posed by such platforms are therefore regarded as far greater than those posed by the

364. Abebe & Posner, *supra* note 254, at 542.
365. Lamont v. Postmaster Gen., 381 U.S. 301, 305, 307 (1965).
366. *Id.* at 305.
367. *See* HAROLD A. INNIS, EMPIRE AND COMMUNICATIONS 26–27 (4th ed. 2007) (distinguishing media "that emphasize time," which are durable in character "such as

paper pamphlets of several decades ago.[368] The expanding application of judicial deference in national security contexts thus reflects a recalibration to evolving national security concerns. Although TikTok ultimately did not prevail, a hypothetical victory would have carried free speech implications arguably exceeding those in *Lamont*, because the national security stakes attached to algorithmic control have become materially greater than the circulation of paper pamphlets. In this regard, *Garland* is unlikely to be an endpoint or an exception to predictive national security reasoning being treated as sufficient to override the First Amendment interests of an expressive platform.

However, this technological shift should be viewed with caution. While providing substantive evidence of actual data transfer may be impractical in today's digital landscape, and the inherent opacity of the black box environment may explain the Court's posture, it does not mean the judicial process must remain entirely predictive or speculative. To move from the impasse, the judiciary could borrow wisdom from scholars currently challenging foreign affairs exceptionalism. Although beyond the scope of this Article, several scholars have proposed how courts can formalize their review of the executive's national security assertions.[369] Ultimately, we should recognize the role of technological sophistication in reshaping the modern national security landscape, but such complexity should not serve as a convenient excuse for blind judicial deference.

Conclusion

PAFACA is the first Act of the United States that could lead to a ban of a social media platform. The Supreme Court's decision in *Garland* upheld the Act by treating it as content-neutral and deferring

---

parchment, clay, and stone," and media "that emphasize space," which "are apt to be less durable and light in character, such as papyrus and paper").

368. *See generally* U.S. Gov't Accountability Off., GAO-22-104714, Information Environment: Opportunities and Threats to DOD's National Security Mission (2022) (arguing that the United States is facing new national security challenges as the world has shifted from an industrial age to an information age, which shapes people's perception in the cognitive dimension rather than simply the physical dimension).

369. *See generally* Deborah N. Pearlstein, *After Deference: Formalizing the Judicial Power for Foreign Relations Law*, 159 U. Pa. L. Rev. 783 (2011) (proposing that courts replace categorical deference with a dynamic equilibrium theory within which courts must inevitably operate to prevent the accrual of excessive power in any one branch); Chander & Schwartz, *supra* note 39 (calling for a National Security Constitution for Personal Data to check executive power through independent tribunal review that can test the government's specific claims of foreign threats and provide concrete evidence of risks).

to the government's predictive national security judgments. The judicial response to PAFACA thus shows that PAFACA's core concerns are not about technical safeguards to protect privacy. Instead, it reflects a broader geopolitical tension, an issue that TikTok's corporate compliance measures alone cannot resolve.

The title of this Article frames TikTok as an exception in a dual sense, and the Conclusion returns to that framing. *Garland* sits at the intersection of two exceptionalist traditions. Foreign affairs exceptionalism furnished the Court with a doctrinal basis for deference, shielding congressional and executive assessments from rigorous judicial review. At the same time, TikTok became an exception to internet exceptionalism — the longstanding presumption that expressive platforms should remain insulated from state control. When these two traditions collided, it was free speech that yielded to national security.

The analysis advanced here does not suggest that PAFACA marks a reversal of the United States' commitment to an open internet in favor of a cyber-sovereignty model. The two traditions have long coexisted within American practice—a rhetorical embrace of openness alongside enduring restrictions grounded in national sovereignty and security. What it does caution is that *Garland* should not be read as a general license. The decision rested on an exceptional confluence of factors: an identified foreign adversary, overwhelming legislative consensus, and a platform tethered to a rival state's legal system.

What PAFACA does represent, however, is an extension of the national security paradigm into the domain of digital content platforms. For the first time, legislation has moved beyond the regulation of physical infrastructure or supply chains to impose structural constraints on an expressive medium itself. But TikTok is unlikely to mark the endpoint or a rare exception to predictive national security judgments being deemed sufficient to outweigh the First Amendment interests at stake in expressive platforms. How courts negotiate this expanding frontier between expressive freedom and preemptive national security governance will continue to shape the future of platform regulation.