

RESEARCH ARTICLE

Arbitrage of the TikTok ban: The conundrum of the U.S.–China data war

Qingxiu Bu^{1,2} 

¹School of Law, Politics and Sociology, University of Sussex, Brighton, UK and ²Institute for Advanced Studies, UM6P, Ben Guerir, Morocco
Email: q.bu@sussex.ac.uk

(Received 5 August 2025; revised 18 March 2026; accepted 20 April 2026)

Abstract

Data privacy and protection are inextricably intertwined, whereas the former often slides into a national security concern. Amid geopolitical tensions, the U.S. aims to preserve TikTok's independence and prevent its use in cognitive warfare. The landmark case presents potentially groundbreaking trade-offs for the Committee on Foreign Investment in the United States and the balance between data privacy and national security. The TikTok ban can be seen as a Catch-22 situation, presenting a Hobson's choice for both the U.S. and China in the ongoing data war. The U.S. faces national security concerns regarding Chinese influence over the app's data and its potential use for surveillance and propaganda. Conversely, banning TikTok risks setting a precedent for censorship and digital platform manipulation, undermining the U.S.'s long-standing commitment to free speech and open markets. The dilemma lies in whether to prioritize national security over the principles of free expression and open trade or to accept the risks posed by adversary-owned platforms operating in the U.S. This decision underscores rising tensions as the two powers grapple with data governance, digital sovereignty and geopolitical rivalry – an outcome that will shape global data governance and the technological landscape for years to come. A paradox emerges as China's ideological aims and the U.S.'s technical concerns converge on a cutting-edge global challenge, that is, cognitive warfare in shaping global discourse and public opinion. This study examines how these conflicting forces shape TikTok's quest to become a global platform, delving into the root causes of these tensions and exploring strategies to address the associated challenges.

Keywords: arbitrage; data war; national security; data governance; cognitive warfare; TikTok

1. Introduction

Artificial intelligence (AI) could enable foreign adversaries to manipulate data that could be leveraged in future military conflicts or diplomatic disputes (Gordon, 2021). Data access has become a new battlefield in terms of national security. The subject of data could be susceptible to blackmail or become a national security vulnerability (Creemers, 2022). China's rapid AI advancements are playing a pivotal role in the current geopolitical competition (Zúñiga et al., 2024). Emerging as a focal point in the U.S.–China rivalry for technological supremacy, TikTok's success relies on an algorithm that gathers personal data to predict user preferences (Bradford, 2023). U.S. concerns center on whether the Chinese government can access this data or influence censorship decisions. TikTok presents the U.S. with a unique tension between economic openness and data control, fueled by national

security concerns over cross-border dataflows in an evolving geopolitical landscape. The primary issue is whether cross-border dataflows should remain unrestricted or be subject to national data localization requirements. A related question is whether the U.S. initiative poses risks to democratic values and freedom of expression, thereby undermining its role as a proponent of internet freedom. It further raises the question as to whether the congressional framework aligns with free speech principles and sufficiently safeguards TikTok's procedural and substantive rights. In response to these challenges, this study proceeds as follows.

Section 2 examines the perspectives of both China and the U.S. on data security in the context of escalating geopolitical tensions. This section examines China's efforts to enhance its data security, aimed at strengthening domestic control while extending its international influence. Additionally, it investigates the Chinese Communist Party's (CCP) global propaganda strategy, focusing on an approach to discourse power, which leverages incremental manipulation of information through platforms like TikTok. **Section 3** analyzes how the Protecting Americans from Foreign Adversarial Applications Act (PAFACAA 2024) addresses legal barriers within the existing regulatory framework, positioning it as a *lex specialis* in U.S. national security law tailored to data governance. Although the U.S. has explained how its measures differ from other countries' restrictions on digital dataflows, the Act raises valid concerns about whether it could undermine U.S. leadership in advocating for an open internet and minimal regulation. This section explores whether imposing similar restrictions on Chinese online media would be a reasonable measure in the interest of reciprocity. **Section 4** analyzes the Supreme Court's decision and explores the rationale behind the judgment. Instead of directly addressing whether the PAFACAA 2024 aligns with constitutional principles, especially the procedural and substantive rights of private economic entities, the Supreme Court focused primarily on its implications for cognitive warfare and national security. **Section 5** delves into potential solutions, building on the insights discussed earlier to propose pathways that are more just, equitable and fair. Specifically, it emphasizes the importance of multinational companies (MNCs) navigating the contrasting strategies of duality within two distinct governance models. The study concludes with a tentative assessment, emphasizing the need for further research grounded in innovative theoretical frameworks and empirical evidence in future stages of inquiry.

2. Legitimacy: regulatory and statutory foundations at the intersection of dataflows and national security

The U.S. closely scrutinizes foreign acquisitions of domestic businesses that handle sensitive personally identifiable information (PII) of U.S. citizens, driven by heightened security and privacy concerns. However, the existing legal framework has proven insufficient to address the complex security risks posed by TikTok's Chinese ownership. Moreover, the legal justification for invoking *the* International Emergency Economic Powers Act (IEEPA 1977) to restrict data trade on national security grounds remains uncertain. A primary concern for the Committee on Foreign Investment in the United States (CFIUS) continues to be mitigating the risk of Chinese government access to U.S. user data.

2.1 A theory of intelligence espionage in China's approach: balancing privacy and national security

Privacy concerns frequently intersect with and escalate into national security issues (Fry, 2015). As long as digital platforms collect sensitive personal data, the risk of foreign adversaries accessing it persists. TikTok poses a national security threat due to the potential for the Chinese government to compel access to that data for propaganda and espionage purposes, despite TikTok's assurances to the contrary. The U.S. views TikTok's data collection practices through the lens of the CCP's strategic objectives, perceiving the potential PII process as a substantial security threat. Chinese law requires all companies, including ByteDance, to assist with intelligence activities, blurring the line between

the private sector and state surveillance (Creemers, 2022). This effectively merges data privacy with national security, making it plausible that social media apps like TikTok must grant the state access to user information.¹

2.1.1 *Espionage risks under the Chinese legal system: a statutory analysis of data protection, cybersecurity and personal information*

China exercises extensive surveillance within its borders and has broad authority to access company-held data at its discretion (Feldstein, 2019). Under various laws, often justified on broadly defined national security grounds, the Chinese government has the authority to request information from companies operating within its jurisdiction (Biancotti, 2019). Cybersecurity review with a heavy emphasis on data security becomes a new norm, especially for those deemed as critical information infrastructure (CII) operators. China's Cybersecurity Law (CSL 2017) aims to safeguard cyber sovereignty and secure essential data, reflecting its stance on national control over internet governance and reinforcing its online censorship system. The nation's first comprehensive cybercity law imposes strict limitations on the free flow of data, significantly restricting cross-border transfers of information, even when such transfers are routine and essential for normal business operations (Jones et al., 2024). It mandates data localization as a measure to enhance cybersecurity, requiring foreign companies like Apple and Amazon to store Chinese user data in China (CSL 2017).² The Data Security Law (DSL 2021) strengthens systematic control over cross-border data transfers to safeguard national security.³ It prohibits companies from transferring "core state data" to foreign judicial or law enforcement agencies without prior approval from Chinese regulators.⁴ The law introduces enhanced oversight of data sharing and imposes severe penalties for violations of cross-border data transfer regulations. Offenders face fines of up to ¥10 million (£1 million) and may have their operating licenses revoked.⁵ The DSL 2021 serves as a cornerstone for the development of China's digital economy, providing a robust legal foundation for enforcing stringent data security requirements. It plays a critical role in standardizing dataflows by requiring companies to classify data based on its significance to national security. Notably, China has been increasingly concerned about the potential national security risks posed by the transfer of personal data outside its borders. As one of the toughest privacy legislations, the Personal Data Protection Law (PDPL 2021) provides that data collectors establish a specialized agency within China or designate a representative to oversee cross-border dataflows.⁶ With extraterritorial effect, storing data overseas does not exempt a firm from complying with the PDPL 2021, as the law imposes statutory obligations for privacy risk mitigation and security assessments during data transfers.⁷ Furthermore, China's broad National Intelligence Law (NIL 2017) contains sweeping language that requires companies to comply with intelligence gathering operations, if requested (Nicas et al., 2019). The NIL 2017 confers enforcement agencies with broad powers over companies, individuals and the data they produce,⁸ which requires that: "any organisation or citizen shall support, assist and cooperate with national intelligence efforts."⁹ As such, Chinese intelligence could exploit users' personal information.

Comprehensive legislation has established a robust legal framework for data security and privacy, reflecting the country's efforts to strengthen regulatory oversight in its tech sector. TikTok is alleged to threaten national security through its collection of users' personal data and content censorship

¹ Cybersecurity Law 2017 Arts 37, 38.

² China Cybersecurity Law (CSL 2017) Art. 31.

³ DSL 2021 Art. 8.

⁴ DSL 2021 Art. 36.

⁵ DSL 2021 Art. 46.

⁶ PDPL 2021 Art. 38 (2).

⁷ PDPL 2021 Art. 40.

⁸ China National Intelligence Law Art. 14.

⁹ China National Intelligence Law Art. 7.

practices. These laws grant the Chinese government broad authority to compel companies to provide access to TikTok's data, fueling concerns that it could obtain a vast repository of sensitive information on U.S. citizens. Meanwhile, these laws impose few constraints on government access to personal data. China's expansive view of national security often blurs the boundaries of an individual entity's obligation to assist the government in accessing data, raising a valid yet difficult question: where should the line be drawn? The gray area under these legislations creates a risk that sensitive data held by TikTok could be transferred to Chinese authorities. There is a deep-seated concern that TikTok, owned by ByteDance and subject to the country's strict intelligence and security laws, could be used for espionage, posing a significant threat to U.S. national security by potentially granting intelligence agencies access to user data (Lewis, 2024).

2.1.2 *Paradoxical thoughts behind the legislative approaches*

The concept of “data sovereignty” views the open, interoperable and free internet as a threat, offering a theoretical foundation for certain countries to influence global data governance platforms and advocate for a more closed, authoritarian-friendly model (Belli & Jiang, 2024). The European Union (EU) seeks sovereignty by prioritizing control over data and reducing reliance on foreign suppliers (Ryan et al., 2024), culminating in the adoption of the General Data Protection Regulation (GDPR) in 2018.¹⁰ The EU's approach reflects a more protectionist stance on internet governance, grounded in the principles of data protection and safeguarding the digital single market (Ryan et al., 2024). The PDPL 2021 draws inspiration from the GDPR and shares similar principles in its rationale for adoption. This tactic may coincidentally fall within the EU's conceptualization of technological sovereignty threats (Farrand et al., 2024). Unlike the EU, which emphasizes technological sovereignty and data protection to shield its digital market from U.S. dominance, the U.S. takes a market-driven approach to data governance, prioritizing the socioeconomic benefits of data economies (Roberts et al., 2021). The EU's approach is less focused on targeting specific firms, even those linked to geopolitical rivals (Balfour et al., 2024). Instead, it adopts a less politicized, rights-based framework for regulation, as exemplified by the 2022 Digital Services Act (Milne et al., 2024).

The implementation of data laws in China and the EU diverges significantly, reflecting their different approaches to balancing state power and individual rights (Li & Chen, 2024). Chinese law lacks clear limits on the information the government can access. The DSL 2021 and PDPL 2021 are designed to restrict data transfers to foreign countries, requiring all cross-border data transfers to be submitted to the Cyberspace Administration of China (CAC) for approval. These laws give the Chinese government expanded control over data, underscoring its growing emphasis on regulating cross-border dataflows, especially when national security is involved. With a politically motivated strategy for assertive control, this comprehensive legal framework has broad extraterritorial implications. For example, the PDPL 2021 specifies that certain processing activities, even if conducted entirely offshore, remain subject to its jurisdiction.¹¹ Given that the extraterritorial impact of the PDPL 2021 has yet to be fully tested, there remains limited clarity on how to apply data export regulations in this context. The extent to which large internet firms will be affected by the new laws on data and algorithms is still uncertain, making it increasingly difficult for them to navigate the evolving data governance landscape. Tech giants will need to adapt their operational models and adjust their level of autonomy to comply with these regulations. In theory, stringent limits on data collection and processing materially constrain AI development, a constraint particularly acute in the EU (King & Meinhardt, 2024). While for China, it is challenging to strike a balance between limiting Chinese tech giants' ability to process data and effectively managing cross-border dataflows.

¹⁰The EU General Data Protection Regulation (GDPR) went into effect on 25 May 2018, replacing the Data Protection Directive 95/46/EC.

¹¹PDPL 2021 Art. 3 (2).

2.2 The U.S. inadequate legal and regulatory framework for addressing challenges posed by dataflows from adversary-state-controlled companies

The primary concern in the U.S. is that the Chinese government could access TikTok's data and potentially exploit it for espionage or blackmail (Gertz, 2020). In response to emerging geopolitical challenges, the U.S. foreign investment screening framework has been strengthened through reforms under the Foreign Investment Risk Review Modernization Act (FIRRMA 2018), integrated within the Defense Production Act (DPA).¹² The CFIUS has heightened its scrutiny of critical technologies involving sensitive personal data. Paving the way for broader economic security measures, the FIRRMA 2018 strengthens the alignment between CFIUS's mandate and cyber-related national security risks, particularly concerning access to sensitive data. Building on this, the PAFACAA 2024 removes legal constraints, enabling the U.S. government to take actions previously prohibited to safeguard digital economic security. Key measures include reviewing TikTok's algorithm, restricting CCP access to platform data and imposing oversight on the app's dataflows.

2.2.1 Evolving legal frameworks addressing dataflow challenges

The IEEPA 1977 grants the President broad authority to address national security emergencies,¹³ empowering them to impose wide-ranging restrictions in response to any "unusual and extraordinary threat" originating, in whole or in part, outside the U.S. and posing a risk to national security.¹⁴ The president is authorized to implement a wide range of restrictive measures, including the power to "suspend or prohibit any covered transaction" if "credible evidence ... leads the President to believe that the foreign interest exercising control may take actions that threaten to impair national security."¹⁵ For instance, in March 2020, Trump ordered Beijing Shiji Information Technology to divest all interests in StayNTouch.¹⁶ In addition, CFIUS has long been concerned with the extent to which information can be collected and exploited by foreign intelligence for manipulation purposes.

In 2018, Congress emphasized the need to scrutinize foreign companies investing in the U.S. that "maintain or collect sensitive personal data of U.S. citizens that may be exploited in a manner that threatens national security" (Reinsch et al., 2020). The FIRRMA 2018, which came into effect on 13 February 2020, provides that any transaction that allows a foreign investor access to sensitive personal data is subject to CFIUS review.¹⁷ The law significantly expanded CFIUS jurisdiction to cover transactions granting foreign actors' access to sensitive data,¹⁸ including PII of U.S. citizens.¹⁹ It strengthens the review process, reinforcing the consensus that CFIUS oversight should remain focused solely on national security concerns.

As such, any transactions involved in critical technologies, critical infrastructure or sensitive personal data are subject to CFIUS review.²⁰ The CFIUS has been aggressive in intervening in cases involving potentially sensitive U.S. data, driven by concerns over the perceived threat of Chinese state access (Reinsch et al., 2020). When a national security concern arises, CFIUS often requires the divestiture of the affected U.S. businesses. In January 2018, CFIUS vetoed China's Ant Financial's \$1.2 billion bid to acquire MoneyGram over concerns that the Chinese government would gain access to U.S. citizens' financial records (Rudegeair & O'Keeffe, 2018). In March 2019, CFIUS ordered Kunlun

¹²DPA 50 USC 55, §4565.

¹³50 USC 35.

¹⁴IEEPA 1977 §1701(a).

¹⁵50 U.S.C. § 4565(d)(4) (50 U.S.C. app. 2170 (1988)).

¹⁶White House, "Order Regarding the Acquisition of Stayntouch, Inc. by Beijing Shiji Information Technology Co., Ltd." (6 March 2020) <https://www.whitehouse.gov/presidential-actions/order-regarding-acquisition-stayntouch-inc-beijing-shiji-information-technology-co-ltd/>.

¹⁷FIRRMA 2018 s1706.

¹⁸50 U.S.C. § 4565(a)(4)(B)(iii), (a)(4)(D)(i).

¹⁹31 C.F.R. § 800.211.

²⁰U.S. Department of the Treasury, "Proposed CFIUS Regulations to Implement FIRRMA" (17 September 2019).

<<https://home.treasury.gov/system/files/206/Proposed-FIRRMA-Regulations-FACT-SHEET.pdf>>.

Tech to divest Grindr over fears about access to personal data for potential blackmail (Marquardt et al., 2019). The forced divestiture serves as a stark reminder that CFIUS is committed to safeguarding the personal data of U.S. citizens (Gao, 2023). When a transaction was prohibited, the foreign acquirer was either barred from purchasing the assets in the U.S. or required to divest them to an approved buyer. These cases carry significant potential implications for platform-based data and transactions across various sectors.

2.2.2 The executive's attempt to ban TikTok

The case of TikTok highlights one of the known risks of CFIUS review: although filing for review of an acquisition is voluntary, CFIUS retains the authority to conduct a review post-closing if no filing is made (Marquardt, 2020). Some factors to be considered include the strategic value of data protection (Bateman & Lyu, 2019). Such reviews may result in divestiture of interests in the acquired business. CFIUS has broad authority that allows it to intervene even after a merger has been consummated (Lederman, 2020). ByteDance's acquisition of Musical.ly has been the subject of CFIUS review as a non-notified transaction since November 2019 (Walshe & Tan, 2020). TikTok's failure to proactively address and report security concerns left it vulnerable to forced divestment as those concerns intensified alongside its rapid growth (Chorzempa, 2020).

Trump threatened to ban TikTok under the authority of the IEEPA 1977.²¹ Under Executive Order (EO 13873), the provision of information technology goods and services to the U.S. is prohibited if the providers are "subject to the jurisdiction or direction of a foreign adversary" and if the transaction "poses an unacceptable risk to the national security of the United States or the security and safety of U.S. persons."²² On 6 August 2020, Trump issued EO 13942 to sever TikTok from the U.S. digital infrastructure by mandating its Chinese owners to sell the popular app²³ that collects or maintains sensitive information.²⁴ The EO claimed that TikTok potentially "allow[s] China to track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage."²⁵ The EOs sought to prohibit transactions involving components produced by "foreign adversaries" that pose risks to U.S. national security (Ferek, 2019). CFIUS statutes do not establish substantive standards or allow judicial review of presidential actions deemed "appropriate to suspend or prohibit any covered transaction that threatens to impair the national security of the United States."²⁶ While the law states such actions are not subject to judicial review,²⁷ case law has, to some extent, limited the practical impact of this provision.²⁸

TikTok has responded to the law by filing lawsuits and successfully resisting attempted bans, with federal courts consistently blocking Trump's proposed ban on the grounds that the information shared on TikTok does not qualify as a "thing of value."²⁹ In June 2021, Biden issued EO 14034, rescinding the ban on TikTok.³⁰

None of the judicial institutions mentioned above have established clear jurisprudence to address the risks of foreign adversaries' data manipulation that threatens national security. Existing legal authorities appear inadequate for managing cross-border dataflows, making it particularly difficult

²¹ 50 U.S.C. 1701 et seq.

²² Executive Office of the President, "Securing the Information and Communications Technology and Services Supply Chain" (Washington DC, White House, Executive Order 13873, 15 May 2019).

²³ Executive Order No. 13942, 85 Fed. Reg. 48637 (6 August 2020).

²⁴ Defense Production Act of 1950 §721.

²⁵ White House, "Executive Order on Addressing the Threat Posed by TikTok" (6 August 2020).

<<https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/>>.

²⁶ 50 U.S.C. § 4565.

²⁷ 50 U.S.C. §4565(e).

²⁸ *Ralls Corp. v. Comm. on Foreign Inv. in the United States*, 758 F.3d 296 (D.C. Cir. 2014).

²⁹ *TikTok v. Trump*, 507 F. Supp. 3d 92, 98 (D.D.C. 2020); *TikTok Inc. v. Trump*, No. 2:20-cv-7672 (C.D. Cal. filed 24 August 2020).

³⁰ Executive Order No. 14034, 86 Fed. Reg. 31,423 (9 June 2021).

to formulate effective law and policy responses. U.S. policymakers must develop a comprehensive framework to address data security tied to cross-border dataflows (Harrell, 2025). Striking a balance between the benefits of open dataflows and the imperative of national security remains a major challenge within the limitations of current U.S. legal protections (Gao, 2023).

3. The PAFACAA 2024: the divest-or-ban law against TikTok

The PAFACAA 2024 in question targets “foreign adversary-controlled applications” (FACA) and compels ByteDance to either sell TikTok to a qualified buyer or effectively cease its operations in the U.S.³¹ Amid legislative efforts to address national security threats, particularly concerning dataflows to China, the U.S. faces a distinct tension between economic openness and data control in the *TikTok* case. Concerns over ByteDance and the potential misuse of personal data by the Chinese government have raised significant national security challenges (Horowitz & Check, 2022). TikTok’s inability to fully assure independence from Chinese government influence has prompted legislative and executive efforts to mitigate risks. The law marks a pivotal development in the evolution of U.S. economic security law and establishes a specialized statutory framework, serving as *lex specialis* within the U.S. digital economy (Dimitropoulos, 2022).

3.1 A statutory milestone in the escalation of U.S.–China dataflow disputes

TikTok faces an unprecedented challenge with the enactment of the PAFACAA 2024, a law passed by the U.S. Congress in April 2024 to curb China’s access to sensitive American data. Its “divest-or-ban” provision specifically targets FACA, including ByteDance and its subsidiary, TikTok.³² Under the Act, ByteDance must either divest its stake in TikTok or face operational restrictions. The law mandates that an American entity take control to ensure compliance with U.S. laws and regulations, prohibiting access to TikTok unless it is sold to a U.S. company.

3.1.1 Unprecedented legislative approach to target an individual firm

With an unusual approach of addressing an individual firm’s data breaches, the PAFACAA 2024 aims to dismantle legal constraints shaped by earlier TikTok litigation. It reflects a strategic effort by U.S. policymakers to bypass existing economic security laws and confront ongoing national security concerns more directly. Given Trump’s efforts to ban the app were rejected in court,³³ the Act empowers the U.S. government to intervene when data is at risk of exposure to an adversary, allowing actions previously precluded in pursuit of economic security objectives in the digital domain. The law presents a new approach through forced divestiture, which represents the culmination of hardline efforts to contain TikTok. The move represents a significant step in the evolution of U.S. economic security law. To some extent, it paves the way for the U.S. to take economic security actions by removing certain legal constraints. A fundamental issue arises as to whether the regime designed by Congress itself complies with, *inter alia*, the freedom of speech and the procedural and substantive guarantees of the rights of private economic actors. Banning TikTok would mark a significant step toward decoupling and could provoke retaliation. It would push the two nations with the greatest influence over global data governance onto increasingly divergent paths, fostering the simultaneous rise of competing Chinese and Western technology ecosystems (Kennedy, 2024).

3.1.2 Enforceable viability

Divestiture has ostensibly become a viable solution, enabling the app to remain part of America’s digital ecosystem while safeguarding democratic values and free speech (Chander & Haochen Sun, 2023).

³¹ PAFACAA 2024 s3.

³² PAFACA s 2(g)(3)(A).

³³ *TikTok Inc. v. Trump*, 507 F. Supp. 3d 92 (D.D.C. 2020).

The legislation seeks to ban the distribution of “FACA” within the U.S., unless the app is sold within six months to a buyer approved by the U.S. president.³⁴ The PAFACAA 2024 imposes a 270-day deadline for ByteDance to divest its U.S. operations by 19 January 2025, or face a full shutdown.³⁵ To enforce the TikTok ban, ByteDance must relinquish all control over TikTok and its algorithms. The law requires TikTok to be sold to an American entity, prohibiting access to the app unless this condition is met. Thus, the PAFACAA 2024 separates the concept of qualified divestiture from the underlying transaction, while also enabling government-encouraged relinquishment of private assets beyond the scope of 50 U.S.C. § 4565. In theory, the Act has a wide scope, encompassing any foreign application that poses national security risks similar to those linked to TikTok. This provides policymakers with a more actionable framework to safeguard America’s digital landscape from adversary nations aiming to undermine its core values. Regarding potential buyers, there is no guarantee that a private equity firm or investor could navigate the political hurdles involved in such a deal, aside from the potential antitrust review.

China has asserted its authority over sensitive exports and accused the U.S. of politically motivated interference, citing exaggerated national security concerns as justification (Atkinson, 2024). The Ministry of Commerce (MOFCOM)’s regulation effectively requires government approval for any sale of TikTok’s recommendation algorithm to a foreign entity.³⁶ For the sake of argument, China would be willing to sacrifice TikTok if it still serves its strategic interests, arguing that the ban has reinforced the Chinese government’s routine censorship practices and its strong stance on data sovereignty (Xing & Li, 2024). The legislative efforts targeting TikTok are emblematic of broader issues in global digital politics and the challenge of balancing national security with free speech (Gray, 2021). The ban sheds light on how the U.S. views data security in the context of rising geopolitical tensions (Duffy, 2025). It has become a template for the U.S. to apply against other Chinese-owned technology companies, such as DeepSeek. As such, the arbitrage and strategic dynamics implicated in the TikTok case hinge not on corporate interests or broader human rights considerations, but predominantly on national security concerns.

3.2 *The divest-or-ban law: deeply rooted contributing factors*

The U.S. ordered ByteDance to divest TikTok, aiming to balance constitutional rights with national security. The divest-or-ban law grants broad authority to ban foreign-owned apps over data security concerns. When American data risks exposure to adversaries, the PAFACAA 2024 enables action against FACA.³⁷ While introducing forced divestiture as a new tactic, the law marks the peak of efforts to curb TikTok (Sitaraman, 2022). The ban also raises concerns about how the actions might contradict the U.S.’s commitment to an open internet and weaken its global advocacy for internet freedom.

3.2.1 *Ideological clashes between national security interests and First Amendment rights*

Intensifying geopolitical tensions are polarizing the world, as divergent values and political ideologies drive growing policy fragmentation between the two largest economies. The TikTok ban reflects a volatile mix of genuine national security concerns and the political appeal of a tough stance on China (Clausius, 2022). The U.S. views China from a potential “responsible stakeholder” to a “strategic rival” (Czin, 2007). The Beijing Model crashes into those in market-based democracies, that is, online freedom, privacy and free international markets. China’s doctrine of digital sovereignty asserts a seemingly legitimate mandate: Chinese firms are required to comply with any government demands

³⁴ PAFACA s2(g)(3)(B).

³⁵ PAFACA s2(a)(2).

³⁶ MOFCOM, *Catalogue of Technologies Prohibited or Restricted from Export* (Beijing, 29 August 2020) Art. 15.

³⁷ PAFACA s 2(g)(3)(A).

for data access (Voss, 2024). Individual entities have limited options when facing orders from China's authoritarian government.

Although it may not be readily perceived as a thinly veiled form of xenophobia, much of the case against TikTok is built on paradoxical claims of harm (Feldstein, 2023). Nevertheless, the U.S. must address the risks associated with TikTok's deep technological ties to an adversary government, regardless of its specific level of complicity (Lavoy, 2024). The concern remains theoretically valid, given China's record of leveraging user data, even though concrete evidence supporting claims that TikTok poses a national security threat is lacking (Rinaldo, 2024). TikTok does have the legal capacity to transmit data to China, but it remains uncertain how much information may actually be shared. A conspiracy theory fuels a weaponized narrative focused on identity, which could be exploited under Chinese legal obligations.³⁸ This suggests that the Chinese government could pressure ByteDance to hand over U.S. user data or manipulate TikTok's algorithm, posing a potential national security risk. Amid rising geopolitical tensions, the U.S. Department of Justice (DoJ) has argued that the Chinese government could force TikTok to aid China's intelligence, law enforcement and national security operations. TikTok has yet to prove a clear separation from its Chinese parent company, fueling fears that sensitive user data could be accessed by the Chinese government. The core issue is balancing First Amendment protections with pressing national security concerns and the judiciary's deference to Congress and the executive branch (Horowitz & Check, 2022). The U.S. aims to leverage digital technologies and American data in ways that raise significant national security risks, even as it confronts the rise of authoritarian control (Brock, 2024). TikTok must address potential national security risks tied to its platform, while the U.S. must balance economic openness with data security.

3.2.2 *Disruptive driving force in cognitive warfare: reshape global discourse and influence public opinion*

The CCP sees data as a critical asset to integrate market advantage, national power and strategic influence (Kokas, 2022). Amid the global integration of the digital economy, a state may impose its values on others that do not share them (Sitaraman, 2022). The pervasiveness of social platforms and the depth of user information they collect make them very powerful tools for both espionage and manipulation of public opinion (Biancotti, 2019). Occupying a dominant position, TikTok symbolizes the challenge that a rising China poses to American hegemony (Pearson et al., 2022). The platform emerged as a significant challenge to Western dominance in shaping global discourse and influencing public opinion (Fu & Dirks, 2024). The platform holds significant power to shape democratic discourse, providing authoritarians with a potent tool to promote their governance models (Feldstein, 2023). TikTok wields substantial influence in the U.S., shaping public opinion and controlling information flow (Schleffer & Miller, 2021). Its sophisticated algorithms raise concerns that the platform could be used as a tool for disseminating Chinese propaganda (Schleffer & Miller, 2021). In this vein, China has arguably leveraged propaganda and covert influence tactics to promote its authoritarian model and diminish the appeal of open societies (Diamond, 2024). By offering an alternative voice in the arena of public opinion, TikTok has inadvertently weakened the traditional monopoly on information, disrupting the dynamics of public opinion warfare. It furthers China's geopolitical aims by supporting the CCP's narrative control, promoting values that contrast with the U.S. and amplifying narratives divergent from mainstream American views (Fu & Dirks, 2024). A potential concern is that China could manipulate TikTok's algorithms, potentially leading to uncontrollable public opinion dynamics in the U.S., especially during critical situations (Gray, 2021). TikTok's benefits are overshadowed by the rise of authoritarian digital discourse (Guggenberger, 2023). The U.S. cannot risk its use in advancing China's geostrategic goals (Gao, 2023). A paradoxical shift is occurring as China's previous ideological focus and the U.S.'s technical concerns converge on a shared emphasis: cognitive warfare in shaping global discourse and public opinion (Fu & Dirks, 2024).

³⁸National Intelligence Law Art. 7; National Security Law Art. 77; Cybersecurity Law Art. 28.

3.3 Far-reaching implications of the PAFACAA 2024

The situation intensified with the PAFACAA 2024, which effectively treats TikTok as an *alter ego* of the Chinese government and the CCP. A key question is whether dataflows should remain unrestricted across borders or be localized within national boundaries. Paradoxically, it remains unclear whether the U.S. is embracing a governance model it once criticized, as it struggles to balance economic openness with the imperative of ensuring data security.

3.3.1 *Paradoxical reciprocal asymmetry: is the U.S. losing the moral high ground or simply copying China's playbook?*

Banning social media access is a defining trait of authoritarian regimes (Ding, 2020). China, in its pursuit of global dominance, strategically leverages private companies to expand its influence while effectively barring U.S. tech firms from its market (Friedberg, 2022). Through its “Great Firewall,” platforms like Facebook, X and Google are routinely blocked, leaving over a billion Chinese netizens without access to these services (Yang, 2024). Viewing the open internet as a threat to CCP authority, the Chinese government has promoted a concept of data sovereignty that prioritizes state control over dataflows (Harrell, 2025). Exemplified by TikTok, China's exosystemic strategy harnesses vast personal data to accelerate its AI capabilities, while disproportionately advancing its digital economy. The model, advocating strong national internet control while extending global influence, is facing growing international scrutiny (Bateman, 2022). The TikTok case, to some extent, reflects a blurring of U.S. values and marks China's success in cognitive warfare (Bernot et al., 2024). This approach would place the U.S. in a paradoxical position, adopting the very internet sovereignty tactics it has long criticized China for, raising fundamental questions about the limits of state control. Without clear evidence of a genuine threat, the U.S. risks building its own version of the Great Firewall, echoing China's censorship model and weakening its credibility as a global champion of internet freedom (Schleffer & Miller, 2021). As a result, America's moral authority in advocating for an open internet has been significantly compromised.

The TikTok ban reflects the core principles of an authoritarian regime. These actions seem to offer justification for such systems, sparking concerns about a potential global ripple effect. One disturbing consequence is that authoritarian regimes may use national security as a pretext to suppress free speech, citing the TikTok case as justification, even as they face ongoing criticism for their own censorship and trade restrictions (Pearson et al., 2022). China has already pointed to the U.S.'s handling of TikTok as evidence of “double standards” on freedom of expression (Chander & Haochen Sun, 2023). The forced sale of TikTok will render protests against China's blocking of Western social media platforms hypocritical. The passage of PAFACAA 2024 could be strategically exploited by China to shift the narrative and highlight perceived U.S. hypocrisy on internet governance. China would capitalize on the valuable propaganda asset, effectively challenging the U.S.'s advocacy for a free digital market. Furthermore, China has introduced measures mirroring the PAFACAA 2024, further reinforcing its own digital barriers, a move that underscores the ongoing cycle of regulatory escalation (Tilley et al., 2024). The TikTok ban, by potentially infringing on constitutionally protected speech, risks setting a far-reaching precedent – one that authoritarian regimes could invoke to justify protectionist policies and legitimize their own censorship of online expression (Schleffer & Miller, 2021).

A more complex inquiry arises as to whether matching China's tactics would compromise fundamental American values. Despite the ostensible notion of reciprocity, considering that platforms like Facebook, Snap, X and Instagram are banned in China, the root cause is a deeply ingrained security-driven mindset. Entrenched within a pan-security trap, this mentality has accelerated the push toward an absolute security state (Feldstein, 2023). This approach could undermine a state's ability to accurately assess and contextualize threats. To effectively compete with China, the U.S. must adopt balanced policies that safeguard national security while upholding core American values (Lettow, 2021). A reaction needs to be measured and consistent with the values of individual freedom

and the rule of law (Lewis, 2024). Only time will reveal the extent to which the geo-economic shift in the global economic order will spill over into the global information society (Gray, 2021).

3.3.2 PAFACAA 2024's departure from the U.S. traditional stance on unrestricted dataflow

The enactment of the PAFACAA 2024 raises a pivotal question: do actions against TikTok contradict the U.S.'s stance in favor of an open internet? The U.S. has previously positioned itself as the champion of an open internet, advocating for minimal regulation and the unrestricted global flow of digital data across borders (Jones, 2023). The U.S. has long advocated for the free flow of data, leveraging its extensive jurisdictional reach. It seeks to mitigate risks through a review of TikTok's algorithm, restricting CCP access to platform data and requiring oversight of the app's dataflows (Gray, 2021). The CFIUS alleged that TikTok presents a risk to U.S. data security and sought action to prevent it from accessing U.S. users' data. The DoJ has argued that any infringement on TikTok users' First Amendment rights is superseded by the government's interest in preserving national security (Huddleston, 2024). On 28 February 2024, the U.S. issued an EO and a proposed DoJ rule restricting the cross-border transfer of sensitive data, marking the first use of national security grounds to limit U.S. dataflows to China. The order introduced a broader framework for regulating such transfers.³⁹ The EO created a broader approach to regulating dataflows. Such a move would, *prima facie*, undermine its case for advocating a free and interoperable internet. TikTok has countered the move by filing a lawsuit to challenge the law, asserting that banning the app would infringe on its First Amendment right to free speech.⁴⁰ The U.S. argues that a rigid commitment to fully open dataflows could hinder efforts to manage data-related risks (Broadbent, 2023). The PAFACAA 2024 represents a targeted initiative to bolster the U.S. economic security framework by addressing ongoing security concerns related to TikTok and overcoming legal obstacles from previous litigation. If the PAFACAA 2024's constitutionality were upheld in court, the U.S. executive branch would gain greater authority to take decisive action against FACAs.

4. Supreme Court's decision on TikTok ban

The Supreme Court has upheld the constitutionality of the TikTok ban. The one-day effect of the solution reflects the strategic manoeuvres and leverage employed by the two powers (Duffy, 2025). The Court's decision has profound implications for the resilience of the global internet ecosystem. Since the PAFACAA 2024 was upheld by the Supreme Court, the U.S. now has the authority to ban other apps, such as RedNote and DeepSeek, under the same national security justifications.⁴¹ The core concern lies in social media platforms' potential involvement in China's censorship apparatus and the urgent need to prevent Chinese cognitive influence over content manipulation (Schleffer & Miller, 2021). It is worth examining whether the move would pose serious risks to democracy and freedom of speech and undermine the U.S.'s position as a promoter of internet freedom.

4.1 The Supreme Court's balance of national security and the override of constitutional protections

TikTok seems to have conflated national security imperatives with free speech values. It has been alleged to be censoring politically sensitive narratives, a practice that poses a significant risk to the values upheld by the U.S. (Brannon, 2019). For the sake of argument, an outright ban on the app would require a strong legal foundation, particularly given First Amendment concerns. Justifying the TikTok ban on privacy grounds would tread into uncharted constitutional territory, raising novel

³⁹ White House, "Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern" (Washington DC, 28 February 2024).

⁴⁰ *TikTok v Merrick Garland* 604 U.S. (2025).

⁴¹ PAFACAA 2024 s2(g)(1); Decoupling America's Artificial Intelligence Capabilities from China Act of 2025.

legal questions about the limits of government action on the basis of data protection (Horowitz & Check, 2022).

The nine Supreme Court justices unanimously ruled that the ban was consistent with the U.S. Constitution, holding that the PAFACAA 2024 targets corporate control rather than protected speech. They focused heavily on congressional authority to safeguard national security interests, steering clear of addressing the free speech implications.⁴² The Court implied that any infringement on TikTok users' First Amendment rights is superseded by the government's interest in preserving national security (Huddleston, 2024). A key legal question is whether the framework established by Congress aligns with freedom of speech and upholds TikTok's procedural and substantive rights. Since the law serves the compelling interest of national security, it remains valid under the "strict scrutiny" standard.⁴³ The Supreme Court has sidestepped the complex free speech debate, focusing instead on data protection, surveillance and propaganda risks. It has also yet to clarify whether foreign companies and individuals are entitled to First Amendment protections under the U.S. Constitution (Marien, 2025). Given the pivotal role of free speech in public discourse, a vague interpretation of constitutional tensions risks leaving critical debates inadequately unresolved.

4.2 *Poste Supreme Court judgment: manoeuvres and leverages*

The Supreme Court ruled against TikTok on 17 January 2025, rejecting the company's First Amendment challenge to the PAFACAA 2024 that effectively banned it starting on 19 January.⁴⁴ As such, all three branches of the U.S. government have endorsed the view that TikTok poses a national security threat. Following this decision, TikTok's swift resumption of operations after a brief ban has undermined the credibility of the national security rationale and heightened the perception that political motives and posturing are driving the decision-making process (Duffy, 2025).

Trump invoked enforcement while the PAFACAA 2024 was already in effect, efficiently bypassing its procedural framework. Although the law penalizes app stores for distributing or updating TikTok content, it remained in force for less than a day, specifically, on 19 January 2025.⁴⁵ Circumventing a Congressional act upheld by the Supreme Court would be an extraordinary act of legal defiance. Trump's EO may face legal challenges questioning whether he has the authority to suspend the enforcement of a federal law. The PAFACAA 2024 provides that the president may grant a one-time 90-day extension to the ban, provided he certifies to Congress that a "qualified divestiture" is in progress and can be completed within that period.⁴⁶ The law permits an extension only if there are indications of progress in negotiations to sell TikTok's U.S. operations to a non-Chinese owner.⁴⁷ Trump has postponed the implementation of the PAFACAA 2024 on TikTok more than once. However, such an extension would be legally invalid under the law since no divestment process is currently in progress, unless a "qualified divestiture" is in progress and can be completed within that period (Chander & Schwartz, 2024).

At its core, the issue centers on the national security risks associated with ByteDance's ownership of TikTok. The primary rationale behind the PAFACAA 2024 legislation is to safeguard data security and prevent manipulation of access by the CCP. Largely owned by global investors, ByteDance, the parent company of TikTok, owns 39 percent of the shares. When the shares held by American stakeholders are aggregated, U.S. capital will make up 50 percent. As such, the key to success lies in strict operational separation, legal enforcement and transparency. This framework seeks to balance

⁴²*TikTok v Merrick Garland* 604 U.S._ (2025) 19.

⁴³*TikTok v Merrick Garland* 604 U.S._ (2025) 3.

⁴⁴*TikTok v Merrick Garland* 604 U.S._ (2025).

⁴⁵PAFACAA 2024 s2 (a).

⁴⁶PAFACAA 2024 s5.

⁴⁷PAFACAA 2024 s3(c)(2).

ByteDance's interests with U.S. national security concerns while also establishing trust and compliance mechanisms. The framework permits ByteDance to maintain control over its core asset, the algorithm, while subjecting user data to U.S. oversight. ByteDance's control over the algorithm may raise concerns in the U.S., particularly the fear that it could be used to promote content that aligns with the interests of the Chinese government. Given this equity structure, it is unlikely that the U.S. will interfere with the algorithms, which are crucial to national security. A more complex unresolved issue concerns whether the proposed shareholding structure affects the CCP's golden shares. This also highlights ByteDance's effective use of TikTok's immense popularity to amplify political pressure. In this context, the U.S.'s maximum pressure strategy has fallen short of achieving its intended goals.

5. New thinking: breaking the deadlock for a long-term, equitable governance framework

The extent of Chinese ownership and current legal access to U.S. data raise potential national security concerns. The current international regime was not designed for a world of data and AI. Digital technologies allow foreign powers to hack CII, conduct cyber-espionage and manipulate social media (Rodrik, 2020). Owing to asymmetry in governance standards, some countries may suffer from the operations of foreign companies from jurisdictions with underdeveloped regulatory frameworks. A strategic response to these challenges is to promote greater international coordination and create global governance rules (Meltzer, 2019). A transnational regulatory framework could produce new standards and enforcement mechanisms. One of the challenges is that authoritarian and democratic countries may not be able to reach agreement on certain ideological and geopolitical issues, such as privacy and digital sovereignty.

5.1 American data privacy and protection act

The U.S. lacks robust data privacy laws to protect consumers from having their personal information acquired by foreign adversaries, as existing regulations are fragmented and outdated. The PAFACAA 2024 would only partially address the associated national security risks (Sitaraman, 2022). The most effective approach would be for Congress to pass comprehensive privacy legislation that regulates the collection and misuse of online personal and commercial data. This legislation should apply not only to current apps like TikTok but also to future digital platforms with potential security or privacy risks (Sitaraman, 2022). Given the lack of overarching digital privacy standards, a targeted ban or divestiture of TikTok is unlikely to bring about significant improvements in data governance. Other tech behemoths also transfer sensitive data across borders, including with entities located within China. A record 72 percent of Americans support increased government regulation on how companies handle their data (McClain et al., 2023). While the Illinois Biometric Information Privacy Act imposes strict penalties for data collection without consent,⁴⁸ a comprehensive federal privacy law could standardize compliance requirements. Such a law would set clear baseline rules to prevent companies from exploiting algorithms for control and influence. It should regulate algorithm use by large data holders and mandate transparency, requiring entities to disclose in their privacy policies whether covered data may be accessible to China. This approach would enhance transparency within software supply chains and impose restrictions when adversarial technologies pose significant national security risks. The case of *TikTok* sends a delicate message that a Chinese company following China's orders to threaten U.S. security will impair its access to the U.S. market. By limiting the misuse of Americans' personal data, concerns about Chinese authorities leveraging TikTok for surveillance could be substantially mitigated.

All Chinese-owned tech platforms face increased scrutiny amid fears that the CCP could access sensitive American user data or pressure these platforms to enforce censorship internationally (Chorzempa, 2020). The crackdown on DiDi showed CAC's tough restrictions on dataflow, which

⁴⁸Illinois Biometric Information Privacy Act s20.

echo similar concerns that drive Western regulators to reconsider their own data governance landscape (Zhai, 2023). The TikTok ban could serve as a touchstone for transitioning to a stricter data security oversight regime, potentially reshaping the landscape in which tech giants operate and expand their businesses across borders. The tension between the U.S. and China highlights the increasing intersection of geopolitics and technology, as both nations advance competing visions for the global digital economy while striving to expand their influence in the digital era (Liu & Miao, 2024). The outcome of this conflict will decide whether Chinese firms retain access to the U.S. stock markets, the world's largest and most liquid investment capital source and whether TikTok will be treated similarly to Western tech giants. A more pragmatic approach could involve leveraging TikTok's interest in pursuing an IPO, which would enable its current owners to legally capitalize on the company's success (Milhaupt & Puchniak, 2025). The IPO could provide a mechanism for CFIUS to mitigate risks, as it explicitly prioritizes data security as a central component of its investment screening process (Korn et al., 2024). This includes key measures such as monitoring dataflows, imposing conditions on where personal data can be stored, determining who can access it and regulating how it can be used (Lewis, 2024).

5.2 *Catch-22 vis-à-vis Hobson's choice*

These cases illustrate a classic Catch-22, compelling both the U.S. and China into a Hobson's choice amid the intensifying data war (Bradford, 2024). On one side, the two powers grapple with national security concerns regarding adversaries' control of their data and its potential use for surveillance and propaganda. On the other hand, banning the platform risks setting a troubling precedent for manipulating digital ecosystems, potentially undermining the free speech and open market principles the U.S. has long upheld (Feldstein, 2023). This struggle to balance national security with free expression highlights the complex tensions shaping the future of the digital landscape (Dearing, 2020). The dilemma lies in choosing between prioritizing national security at the expense of free expression and open trade or accepting the risks of allowing an adversary-owned platform to operate within the U.S. (Kello, 2021). This decision highlights the escalating tensions as the U.S. and China navigate the pressing issues of data governance, digital sovereignty and geopolitical rivals. Its outcome will likely set the course for global data governance and influence the broader technological landscape for years ahead (Graham et al., 2024).

5.3 *Navigating catalysts for a more balanced and equitable global data governance framework*

U.S. national security requires a nuanced approach that balances protecting strategic interests with safeguarding American values.⁴⁹ As seen in the TikTok ban, both the U.S. and China are developing their own regulatory standards and shaping distinct national security narratives. It is worth concerning that the ecosystem that cultivated a vibrant tech sector could be broken, because of the geopolitical tension and both the U.S. and China's unpredictable policies. A viable global governance framework must navigate and balance these regulatory diversities.

5.3.1 *Applications for accession to the CPTPP and DEPA as catalysts for China's transformation*

Promisingly, China is expected to implement changes prompted by the provisions on Free Cross-Border Data Flow⁵⁰ and the Prohibition on Data Localization Requirements⁵¹ outlined in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). Notably, these

⁴⁹“2019 Report to Congress of the U.S.-China Economic and Security Review Commission.” (116th Congress 1st Session, Washington DC, USCC, November 2019).

<<https://www.uscc.gov/sites/default/files/2019-11/2019%20Executive%20Summary.pdf>>.

⁵⁰CPTPP Art. 14.11.

⁵¹CPTPP Art. 14.13.

provisions are mandatory prerequisites for China's accession to the CPTPP as part of its application process. Restrictions on dataflows or localization are generally permissible when they serve legitimate public policy objectives, such as protecting national security or privacy, and are considered necessary and proportionate.⁵² Similar provisions to ensure free cross-border flows and the prohibition of data localization are provided under the Digital Economy Partnership Agreement (DEPA).⁵³ To meet the accession criteria for the CPTPP and DEPA, China will need to allow free cross-border dataflow and revoke data localization requirements. These transformations could pave the way for reciprocal actions, such as the potential lifting of bans on U.S. social media platforms like X.

5.3.2 *Prevent a race toward protectionist measures in cross-border dataflows*

The TikTok ban has set a precedent for other governments to adopt similar protectionist measures. Meanwhile, firms face ongoing uncertainty about the legality of U.S.–EU dataflows after the European Court of Justice invalidated the Privacy Shield and Safe Harbor agreements due to concerns over U.S. government surveillance (Murphy, 2022). Even close allies have raised concerns about the fragmented nature of U.S. data governance. Meanwhile, escalating U.S.–China measures, including sweeping bans, threaten to further fracture the global internet. From a macro level, the renewed U.S.–China Science and Technology Agreement (STA) signals a positive approach, historically playing a crucial role in fostering cooperation on bilateral and global challenges. The updated agreement includes provisions emphasizing data reciprocity, encouraging both countries to share data openly to advance mutual interests (Gilbert & Mallapaty, 2024). However, concerns persist regarding China's stringent data localization policies (Creemers, 2022). It remains uncertain whether the ongoing debate over cross-border dataflow will lead to a more equitable governance framework.

5.4 *Tech firms' contrasting strategies of duality under different governance models*

In an era of intensified geo-economic competition, MNCs struggle to shield themselves from broader geopolitical conflicts, even as CFIUS remains an impartial body focused solely on national security, not economic protectionism (Horowitz & Check, 2022). This is especially challenging when operating across the U.S.–China divide (Gertz & Evers, 2020). Additionally, the multinationals must proactively consider alleviation of any perceived risk to U.S. national security. To mitigate potential legal risks, MNCs should thoroughly assess all relevant legal and regulatory challenges in both contrasting social, legal and political environments.

5.4.1 *Behind the façade of corporate purpose: supremacy of national security vis-à-vis doctrine of separate personality*

Corporate personality tests are growing increasingly inadequate for addressing the national security challenges posed by data-intensive operations in a rapidly de-globalizing world (Chivvis & Cuéllar, 2024). The TikTok case grows increasingly contentious amid rising U.S.–China geopolitical tensions, as China's political economy blurs the line between commercial enterprises and state influence, making it difficult for outsiders to differentiate between the two (Pearson et al., 2022). The security concerns persist as long as ByteDance retains control over the algorithm (Patnaik & Litan, 2023). Although global institutional investors like Blackstone and General Atlantic own 60 percent of ByteDance, the Chinese government's "golden share" theoretically gives it significant control over TikTok's algorithm, a key driver of the platform's influence and global reach.⁵⁴ TikTok continues to face scrutiny regarding China's role in its operations and decision-making (Yu & Liu, 2020). In this context, the principle of corporate separate legal entity appears to be overshadowed by concerns over data security risks associated with the platform.

⁵² CPTPP Art. 14.2.

⁵³ DEPA Art. 4.3 (2); Art. 4.3 (3); Art. 4.4 (2); Art. 4.4 (3).

⁵⁴ *TikTok v. Garland* (District of Columbia Circuit, United States Court of Appeals, 6 December 2024).

Despite efforts to distance itself, TikTok continues to face widespread perceptions that ByteDance remains closely linked to the Chinese government, even as it seeks to assert operational independence. The U.S. court did not rigidly apply the doctrine, but instead emphasized the “risk of a foreign adversary exploiting the corporate form.”⁵⁵ TikTok is widely seen as a potential instrument of malign Chinese state influence. It is the firm’s susceptibility to Chinese party-state influence that supersedes the doctrine of corporate personality (Bernot et al., 2024). The TikTok case highlights the limitations of traditional corporate law doctrines in addressing the concerns of policymakers who are increasingly focused on data security and geopolitical rivalry (Horowitz & Check, 2022). More nuanced frameworks are needed to assess *de facto* state influence effectively. TikTok has invoked the principle of “technological neutrality” in an attempt to sidestep transparency requests regarding its data collection, access and usage practices (Lala, 2024). The firm’s lack of transparency in data governance can be attributed to China’s authoritarian system and the broader geopolitical tensions surrounding the case, despite its algorithm’s goal of maintaining content neutrality (Bernot et al., 2024). To avoid muddling the issue, TikTok should take immediate action to establish a clearer, verifiable separation from ByteDance in order to make its claims of independence more credible (Gray, 2021).

5.4.2 Rule by law vis-à-vis rule of law

Seen as both a technological and geopolitical threat, TikTok finds itself increasingly caught between the pressures of its authoritarian government at home and growing hostility abroad (Bernot et al., 2024; Sitaraman, 2022). Tech firms operate within starkly different social, legal and political frameworks in China and the U.S. This duality manifests in their strategies for survival, shaped by the contrasting governance models (Bernot et al., 2024). The divergence in the firms’ strategies highlights the stark contrast between the Beijing Model and the New Washington Consensus. The former is characterized by *rule by law*, where the legal system functions as a tool for reinforcing centralized power rather than serving as an independent authority (Li, 2022). The latter operates under the *rule of law*, where governance is rooted in the principle of separation of powers and the law constrains executive authority (Kavanagh, 2016), which is exemplified by TikTok’s lawsuits against the U.S. government. The independence of the judiciary enables firms to challenge undue government impositions, reinforcing a more equitable relationship between businesses and the state (Levi, 2020).

In China, firms operate within an authoritarian system where the state wields substantial control. Government decision-making is highly discretionary, emphasizing authority over the rule of law (Ji, 2022). Noncompliance by platforms such as DiDi and ByteDance can lead to severe consequences, including hefty fines, operational restructuring or even shutdowns (Schleffer & Miller, 2021). As a result, firms must proactively prioritize regulatory compliance over autonomy, complying with government directives rather than depending on legal frameworks to protect their interests (Creemers, 2022). Shaped by a hierarchical relationship with the government and driven by compliance with state demands (Gray, 2021), ByteDance’s approach in China mirrors the strategies of other domestic tech giants, such as DiDi, where strict regulatory adherence is vital for survival within a tightly controlled system (Zhang, 2022). In the U.S., TikTok functions within a framework that promotes a more balanced relationship, supported by legal protections and procedural fairness (Lewis, 2024). When faced with bans and divestiture demands, it has leveraged the U.S. legal system by launching lawsuits to defend its market position (Ji, 2024). This approach not only defends legitimate rights but also exemplifies standard behavior in a rule-of-law society, where firms can challenge executive powers relying on impartial adjudication (Pollman, 2021).

TikTok’s legal challenges to U.S. government actions reflect its confidence in the independence of the American judicial system, an assurance that would be unviable under China’s tightly controlled regulatory regime.⁵⁶ This duality reflects not only the firms’ adaptive strategies but also serves as

⁵⁵ *TikTok v. Garland* (District of Columbia Circuit, United States Court of Appeals, 6 December 2024).

⁵⁶ *TikTok v Merrick Garland* 604 U.S._ (2025).

a lens to understand the divergences between rule-by-law and rule-of-law scenarios. As such, the “dual personas” exemplify the challenges MNCs face in navigating survival across vastly different governance paradigms (Doz & Prahalad, 1980). These contrasting approaches reveal not only the strategies of an MNC but also the deep-seated differences in how power and law shape the business landscape in China and the U.S.

6. Conclusion

The TikTok ban is a key episode in the broader U.S.–China tech rivalry, reflecting deep tensions over data governance and national security. This study examines the conflicting forces driving the ban and the challenges in resolving them. The U.S. has conventionally championed free dataflows through its long-arm jurisdiction, yet the TikTok ban, framed as a national security measure, mirrors China’s own restrictions on foreign platforms from a cognitive warfare perspective. Marking a strategic shift, the U.S. prioritizes data protection and counters China’s expanding soft power beyond traditional digital infrastructure controls. A central dilemma remains: how to balance sensible cross-border dataflows with security concerns. This tension between national security and data openness will shape the future digital landscape. The TikTok controversy highlights the broader struggle to reconcile security, data governance and freedom of speech, underscoring the need for the U.S. to strike a sustainable balance between economic openness and data control.

The regulatory approaches of both powers will critically influence the global data governance framework in the coming years. The TikTok case underscores the urgency for nuanced policymaking amid growing efforts to “de-risk” digital ecosystems. Simply banning TikTok does little to improve the information environment; real progress requires unified privacy and algorithmic standards for all tech giants. Broader reforms might include comprehensive national privacy legislation, greater transparency in software supply chains and targeted restrictions where Chinese technology poses genuine risks.

Addressing long-standing security concerns, the PAFACAA 2024 represents a deliberate effort by U.S. policymakers to bypass legal constraints from prior TikTok litigation and strengthen economic security laws. This move escalates the data governance standoff with China, carrying significant national security implications. While the global landscape is not purely zero-sum, the TikTok ban risks reinforcing the belief that conflict with China is inevitable. Against mounting concerns about China’s potential misuse of personal data, the TikTok case will set a crucial precedent for how the U.S. addresses security risks posed by adversary-owned social media platforms. Ultimately, TikTok’s legal battles highlight profound uncertainty over cross-border data transactions, with long-term implications still unfolding. The case may also become a blueprint for U.S. actions against other Chinese tech firms. As geopolitical tensions rise, the U.S. is expected to continue closely scrutinizing Chinese investments and mergers amid ongoing concerns over national security and data governance.

Acknowledgements. I am grateful to the Forum’s reviewers for their proactive and insightful feedback, which proved invaluable in bringing this paper to fruition. I also wish to express my sincere thanks to the College for Social Sciences and Humanities, UA Ruhr | Research Alliance, for its generous support throughout the writing process.

Competing interests. The author declares none.

References

- Atkinson, R. D. (2024, September 16). China is rapidly becoming a leading innovator in advanced industries. <https://itif.org/publications/2024/09/16/china-is-rapidly-becoming-a-leading-innovator-in-advanced-industries/>
- Balfour, R., Baroncelli, E., Bomassi, L., Csernatoni, R., Goldthau, A., Grevi, G., Hoeffler, C., Jones, E., Nair, P. P., Ülgen, S., & Youngs, R. (2024). *Geopolitics and Economic Statecraft in the European Union*. Carnegie Endowment for International Peace. <https://carnegieendowment.org/research/2024/11/geopolitics-and-economic-statecraft-in-the-european-union?lang=en>

- Bateman, J. (2022, April 25). "U.S.-China technological "decoupling": A strategy and policy framework. <https://carnegieendowment.org/research/2022/04/us-china-technological-decoupling-a-strategy-and-policy-framework?lang=en>
- Bateman, J., & Lyu, J. (2019, September 10) What is the U.S. ban on TikTok and wechat all about? <https://carnegieendowment.org/2020/08/25/what-is-u.s.-ban-on-tiktok-and-wechat-all-about-pub-82566>
- Belli, L., & Jiang, M. (Eds.). (2024). *Sovereignty in the BRICS Countries-How the Global South and Emerging Power Alliances Are Reshaping Digital Governance* (pp. 103–164). Cambridge University Press.
- Bernot, A., Cooney-O'Donoghue, D., & Mann, M. (2024). Governing Chinese technologies: TikTok, foreign interference, and technological sovereignty. *Internet Policy Review*, 13(1), 1–26. <https://doi.org/10.14763/2024.1.1741>.
- Biancotti, C. (2019, January 11). The growing popularity of Chinese social media outside China poses new risks in the west. <https://www.piiie.com/blogs/china-economic-watch/growing-popularity-chinese-social-media-outside-china-poses-new-risks>
- Bradford, A. (2023). *Digital Empires: The Global Battle to Regulate Technology* (pp. 183–220). Oxford University Press.
- Bradford, A. (2024). The false choice between digital regulation and innovation. *Northwestern University Law Review*, 119(2), 377–453. <https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1578&context=nulr>
- Brannon, V. C. (2019, March 27). Free speech and the regulation of social media content. <https://fas.org/sgp/crs/misc/R45650.pdf>
- Broadbent, M. (2023, December 11). USTR upends U.S. negotiating position on cross-border data flows. <https://www.csis.org/analysis/ustr-upends-us-negotiating-position-cross-border-data-flows>
- Brook, J. (2024, October 23). A new future for digital solidarity? Analyzing the United States international cyberspace & digital policy strategy. <https://www.csis.org/blogs/strategic-technologies-blog/new-future-digital-solidarity-analyzing-united-states>
- Chander, A., & Haochen Sun, H. (2023). Introduction: Sovereignty 2.0. In A. Chander & H. Sun (Eds.), *Data Sovereignty: From the Digital Silk Road to the Return of the State* (pp. 72–88). Oxford University Press.
- Chander, A., & Schwartz, P. (2024). The president's authority over cross-border data flows. *University of Pennsylvania Law Review*, 172(7), 1989–2052. <https://pennlawreview.com/2024/08/29/the-presidents-authority-over-cross-border-data-flows/>
- Chivvis, C. S., & Cuéllar, M. (2024, September 19). U.S.-China relations for the 2030s: Toward a realistic scenario for coexistence. <https://carnegieendowment.org/research/2024/10/us-china-relations-for-the-2030s-toward-a-realistic-scenario-for-coexistence?lang=en>
- Chorzempa, M. (2020, August 7). Trump's ban on WeChat and TikTok lacks clarity and will not solve our data security problems. <https://www.piiie.com/blogs/realtime-economic-issues-watch/trumps-ban-wechat-and-tiktok-lacks-clarity-and-will-not-solve>
- Clausius, M. (2022). The banning of TikTok, and the ban of foreign software for national security purposes. *Washington University Global Studies Law Review*, 21(2), 273–292. <https://journals.library.wustl.edu/globalstudies/article/id/8751/>
- Creemers, R. (2022). China's emerging data protection framework. *Journal of Cybersecurity*, 8(1), 1–12. <https://doi.org/10.1093/cybsec/tyac011>.
- Czin, J. (2007). Dragon-slayer or Panda-hugger? Chinese perspectives on "responsible stakeholder. *Diplomacy. Yale Journal of International Affairs*, 2(2), 100–112. <https://static1.squarespace.com/static/5d630d194bcc6a00018ff22b/t/697f581b79903005061f3672/1769553310749/YJIA+2.2.8.pdf>
- Dearing, C. K. (2020). Personal Information as an attack vector: Why privacy should be an operational dimension of U.S. National Security' *Journal of National Security Law & Policy*, 11(1), 351–401. https://nationalsecurity.law.georgetown.edu/wp-content/uploads/2020/04/Why_Privacy_Should_Be_an_Operational_Dimension_of_US_National_Security.pdf
- Diamond, L. (2024). How to end the democratic recession: The fight against autocracy needs a new playbook. *Foreign Affairs*, 103(6), 126–140. <https://www.foreignaffairs.com/world/how-end-democratic-recession-autocracy-larry-diamond>
- Dimitropoulos, G. (2022). Law and digital globalization. *University of Pennsylvania Journal of International Law*, 44(1), 41–110. <https://repository.law.upenn.edu/Documents/Detail/law-and-digital-globalization/89033>
- Ding, J. (2020, June 28). Social media: Threat to or tool of authoritarianism? *Harvard International Review*. <https://hir.harvard.edu/social-media-threat-to-or-tool-of-authoritarianism/>
- Doz, Y., & Prahalad, C. K. (1980). How MNCs cope with host government intervention. *Harvard Business Review*, 58(2), 149–157. <https://hbr.org/1980/03/how-mncs-cope-with-host-government-intervention>
- Duffy, K. (2025, January 17). Why the TikTok ban harms U.S. interests at home and abroad. <https://www.cfr.org/expert-brief/why-tiktok-ban-harms-us-interests-home-and-abroad>
- Farrand, B., Carrapico, H., & Turobov, A. (2024). The new geopolitics of EU cybersecurity: Security, economy and sovereignty. *International Affairs*, 100(6), 2379–2397. <https://doi.org/10.1093/ia/iaae231>.
- Feldstein, S. (2023, November 29). New digital dilemmas: Resisting autocrats, navigating geopolitics, confronting platforms. <https://carnegieendowment.org/research/2023/11/new-digital-dilemmas-resisting-autocrats-navigating-geopolitics-confronting-platforms?center=china&lang=en>

- Feldstein, S. (2019, September 17). The global expansion of ai surveillance. <https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847>
- Ferek, K. S. (2019, November 26). U.S. seeks to unwind business deals that pose telecommunications security threat. *The Wall Street Journal*. <https://www.wsj.com/articles/u-s-seeks-to-unwind-business-deals-that-pose-telecommunications-security-threat-11574782284?msockid=32487172acb3632920316625ad43621a>
- Friedberg, A. L. (2022). The growing rivalry between America and China and the future of globalization. *Texas National Security Review*, 5(1), 95–119. <https://doi.org/10.15781/b0sb-py52>.
- Fry, J. (2015). Privacy, predictability and internet surveillance in the U.S. and China: Better the devil you know? *University of Pennsylvania Journal of International Law*, 37(2), 419–501. <https://repository.law.upenn.edu/Documents/Detail/privacy-predictability-and-internet-surveillance-in-the-u-s-and-china-better-the-devil-you-know/88434>
- Fu, D., & Dirks, E. (2024, June 24). The TikTok debacle: Distinguishing between foreign influence and interference. <https://www.brookings.edu/articles/the-tiktok-debacle-distinguishing-between-foreign-influence-and-interference/>
- Gao, R. (2023). A battle of the big three? -Competing conceptualizations of personal data shaping transnational data flows. *Chinese Journal of International Law*, 22(4), 707–787. <https://doi.org/10.1093/chinesejil/jmad040>.
- Gertz, G. (2020, August 7). Why is the Trump administration banning TikTok and WeChat? *Brookings*.
- Gertz, G., & Evers, M. (2020). Geoeconomic competition: Will state capitalism win? *The Washington Quarterly*, 43(2), 117–136. <https://doi.org/10.1080/0163660X.2020.1770962>.
- Gilbert, G., & Mallapaty, S. (2024, December 13). US and China sign new science pact-but with severe restrictions *Nature News*
- Gordon, G. (2021). On the future perfect of artificial intelligence and war. *Journal of Conflict and Security Law*, 26(3), 577–593. <https://doi.org/10.1093/jcsl/krab013>.
- Graham, S., Mohammed, L. and Tucker, J. A. (2024, December 17). The case for open data access to Aid Tech regulation. <https://www.brookings.edu/articles/the-case-for-open-data-access-to-aid-tech-regulation/>
- Gray, J. E. (2021). The geopolitics of ‘platforms’: The TikTok challenge. *Internet Policy Review*, 10(2), 1–22. <https://doi.org/10.14763/2021.2.1557>.
- Guggenberger, N. (2023). Moderating Monopolies. *Berkeley Technology Law Journal*, 38(1), 119–172. <https://doi.org/10.15779/Z389K45T9Q>.
- Harrell, P. (2025, January 30). Managing the risks of China’s access to U.S. data and control of software and connected technology. <https://carnegieendowment.org/research/2025/01/managing-the-risks-of-chinas-access-to-us-data-and-control-of-software-and-connected-technology?lang=en>
- Horowitz, B., & Check, T. (2022). TikTok v. Trump and the uncertain future of national security-based restrictions on data trade. *Journal of National Security Law & Policy*, 13, 61–111. <https://nationalsecurity.law.georgetown.edu/journal/2022/12/16/tiktok-v-trump-and-the-uncertain-future-of-national-security-based-restrictions-on-data-trade/>
- Huddleston, J. (2024, March 20). US wants to ban TikTok, but first amendment demands stronger case on national security. <https://www.cato.org/commentary/us-wants-ban-tiktok-first-amendment-demands-stronger-case-national-security>
- Ji, L. (2024). *Negotiating Legality: Chinese Companies in the U.S. Legal System* (pp. 194–230). Cambridge University Press.
- Ji, W. (2022). *Towards the Rule of Law in China Social Diversification and the Power System* (pp. 138–256). Cambridge University Press.
- Jones, E. (2023). Digital disruption: Artificial Intelligence and international trade policy. *Oxford Review of Economic Policy*, 39(1), 70–84. <https://doi.org/10.1093/oxrep/grac049>.
- Jones, E., Kira, B., & Tavengerwei, R. (2024). Norm entrepreneurship in digital trade: The Singapore-led wave of digital trade agreements. *World Trade Review*, 23(2), 208–241. <https://doi.org/10.1017/S1474745624000089>.
- Kavanagh, A. (2016). The constitutional separation of powers. In D. Dyzenhaus & M. Thorburn (Eds.), *Philosophical Foundations of Constitutional Law* (pp. 221–239). Oxford University Press.
- Kello, L. (2021). Cyber legalism: Why it fails and what to do about it. *Journal of Cybersecurity*, 7(1), 1–15. <https://doi.org/10.1093/cybsec/tyab014>.
- Kennedy, S. (2024, November 20). Managing U.S.-China tensions over the global economic order’ security. <https://www.csis.org/analysis/managing-us-china-tensions-over-global-economic-order>
- King, J., & Meinhardt, C. (2024, February). Rethinking privacy in the AI era-policy provocations for a data-centric world. <https://hai.stanford.edu/sites/default/files/2024-02/White-Paper-Rethinking-Privacy-AI-Era.pdf>
- Kokas, A. (2022). *Social Media: The Algorithm as National Security Asset, Trafficking Data: How China Is Winning the Battle for Digital Sovereignty* (94–116). Oxford University Press.
- Korn, D., Denamiel, T., & Reinsch, W. A., (2024, August 16). Harmonising inbound investment screening. <https://www.csis.org/analysis/harmonizing-inbound-investment-screening>
- Lala, K. (2024). TikTok the tortfeasor: A Framework to discuss social-platform externalities and arguments favoring ex ante mitigations. *The University of Chicago Law Review*, 91(6), 1765–1808. <https://chicagounbound.uchicago.edu/ucirev/vol91/iss6/4>
- Lavoy, N. (2024, August 14). TikTok is a threat to national security, but not for the reason you think. <https://www.rand.org/pubs/commentary/2024/08/tiktok-is-a-threat-to-national-security-but-not-for.html>

- Lederman, I.** (2020). The right rights for the right people? The need for judicial protection of foreign investors. *Boston College Law Review*, 61(2), 703–747. <https://bclawreview.bc.edu/articles/186>
- Lettow, P.** (2021). U.S. national security strategy: Lessons learned. *Texas National Security Review*, 4(2), 117–154. <http://dx.doi.org/10.26153/tsw/13195>.
- Levi, D.** (2020). Protecting fair and impartial courts-reflections on judicial independence. *Judicature*, 104(2), 58–67. <https://judicature.duke.edu/articles/protecting-fair-and-impartial-courts-reflections-on-judicial-independence/>
- Lewis, J. A.** (2024, March 13). TikTok and national security. <https://www.csis.org/analysis/tiktok-and-national-security>
- Li, S.** (2022). *The Rise of China, Inc.-How the Chinese Communist Party Transformed China into a Giant Corporation* (pp 49–92). Cambridge University Press.
- Li, W., & Chen, J.** (2024). From Brussels effect to gravity assists: Understanding the evolution of the GDPR-inspired personal information protection law in China. *Computer Law & Security Review*, 54, 1–14. <https://doi.org/10.1016/j.clsr.2024.105994>.
- Liu, H., & Miao, C.** (2024). Digital geopolitics in a VUCA world: China encounters a new global order. *Global Policy*, 15(6), 67–83. <https://doi.org/10.1111/1758-5899.13435>.
- Marien, K.** (2025). TakeTok: Does a TikTok ban violate the takings clause? *University of Chicago Legal Forum*, 1, 515–550. <https://legal-forum.uchicago.edu/print-archive/taketok-does-tiktok-ban-violate-takings-clause>
- Marquardt, P. et al.** (2019, April 17). CFIUS and the unwinding of Kunlun's acquisition of Grindr. *The CLS Blue Sky Blog*. <https://clsbluesky.law.columbia.edu/2019/04/17/clearly-gottlieb-discusses-cfius-and-the-unwinding-of-kunluns-acquisition-of-grindr/>
- Marquardt, P.** (2020, August 24). TikTok: Familiar issues, unfamiliar responses. *Harvard Law School Forum on Corporate Governance*. <https://corpgov.law.harvard.edu/2020/08/24/tiktok-familiar-issues-unfamiliar-responses/>
- McClain, C., Faverio, M., Anderson, M., & Park, E.** (2023, October 18). How American view data privacy. <https://www.pewresearch.org/internet/2023/10/18/views-of-data-privacy-risks-personal-data-and-digital-privacy-laws/>
- Meltzer, J.** (2019). Governing Digital Trade. *World Trade Review*, 18(S1), 23–48. <https://doi.org/10.1017/S1474745618000502>.
- Milhaupt, C. J., & Puchniak, D.** (2025, January 3). TikTok's Identity Crisis: Corporate Personality in a De-Globalizing World. <https://corpgov.law.harvard.edu/2025/01/03/tiktoks-identity-crisis-corporate-personality-in-a-de-globalizing-world/>
- Murphy, M. H.** (2022). Assessing the Implications of Schrems II for EU–US Data Flow. *International and Comparative Law Quarterly*, 71(1), 245–262. <https://doi.org/10.1017/S0020589321000348>.
- Nicas, J., Milne, C., Hu, J. Z., & Khan, F.** (2019, November 1). TikTok said to be under national security review. *The New York Times*.
- Patnaik, S., & Litan, R. E.** (2023, May 11). tiktok shows why social media companies need more regulation. https://www.brookings.edu/wp-content/uploads/2023/05/20230511_CRM_PatnaikLitan_TikTok_FINAL.pdf
- Pearson, M., Rithmire, M., & Tsai, K. S.** (2022). China's party-state capitalism and international backlash: From interdependence to insecurity. *International Security*, 47(2), 135–176. https://doi.org/10.1162/isec_a_00447.
- Pollman, E.** (2021). The Supreme Court and the Pro-Business Paradox. *Harvard Law Review*, 135(1), 220–266. <https://harvardlawreview.org/print/vol-135/the-supreme-court-and-the-pro-business-paradox/>
- Reinsch, W. A., Caporal, J., Saumell, P., & Frymoyer, I.** (2020, September 2). TikTok is running out of time: Understanding the CFIUS decision and its implications. <https://www.csis.org/analysis/tiktok-running-out-time-understanding-cfius-decision-and-its-implications>
- Rinaldo, D.** (2024, October 24). Looking beyond TikTok: The risks of temu. <https://www.csis.org/analysis/looking-beyond-tiktok-risks-temu>
- Roberts, H., Cowls, J., Casolari, F., Morley, J., Taddeo, M., & Floridi, L.** (2021). Safeguarding European values with digital sovereignty: An analysis of statements and policies. *Internet Policy Review*, 10(3), 1–28. <https://doi.org/10.14763/2021.3.1575>.
- Rodrik, D.** (2020, September 8). The coming global technology fracture. *Project Syndicate*. <https://www.project-syndicate.org/commentary/making-global-trade-rules-fit-for-technology-by-dani-rodrik-2020-09>
- Rudegeair, P., & O'Keeffe, K.** (2018, January 3). U.S. Bars Merger of MoneyGram, China's Ant Financial. *The Wall Street Journal*. <https://www.wsj.com/articles/moneygram-and-ant-financial-halt-merger-deal-1514931496?msocid=32487172acb3632920316625ad43621a>
- Ryan, M., Gürtler, P., & Bogucki, A.** (2024). Will the real data sovereign please stand up? An EU policy response to sovereignty in data spaces. *International Journal of Law and Information Technology*, 32(1), 1–32. <https://doi.org/10.1093/ijlit/eaee006>.
- Schleffer, G., & Miller, B.** (2021). The political effects of social media platforms on different regime types. *Texas National Security Review*, 4(3), 77–103. <http://dx.doi.org/10.26153/tsw/13987>.
- Sitaraman, G.** (2022). The regulation of foreign platforms. *Stanford Law Review*, 74(5), 1073–1152. <https://www.stanfordlawreview.org/print/article/the-regulation-of-foreign-platforms/>
- Tilley, A., Lin, L., & Horwitz, J.** (2024, April 19). China orders apple to remove popular messaging apps. *The Wall Street Journal*. <https://www.wsj.com/tech/apple-removes-whatsapp-threads-from-china-app-store-on-government-orders-a0c02100?msocid=32487172acb3632920316625ad43621a>
- Voss, W. G.** (2024). China data flows and power in the era of Chinese big tech. *Northwestern Journal of International Law & Business*, 44(1), 1–68. <https://scholarlycommons.law.northwestern.edu/njilb/vol44/iss1/1>

- Walshe, T., & Tan, S. (2020, May 13) TikTok on the clock: A summary of CFIUS's Investigation into ByteDance. <https://www.csis.org/blogs/trustee-china-hand/tiktok-clock-summary-cfiuss-investigation-bytedance>
- Wang, J., Milne, C., Hu, J. Z., & Khan, F., (2024, April 8). Navigating Geopolitics in AI Governance. <https://oxgs.org/2024/04/08/oxgs-report-navigating-geopolitics-in-ai-governance/>
- Xing, J., & Li, M. (2024, April 11). The potential Chinese responses to a U.S. Ban on TikTok. <https://carnegieendowment.org/posts/2024/04/the-potential-chinese-responses-to-a-us-ban-on-tiktok?lang=en>
- Yang, Z. (2024, May 1). The depressing truth about TikTok's impending ban. *MIT Technology Review*. <https://www.technologyreview.com/2024/05/01/1091951/tiktok-ban-chinese-companies-political/>
- Yu, Y., & Liu, C. (2020, July 17). As US scrutiny mounts, is TikTok set to be the Next Huawei? *Nikkei Asian Review*. <https://asia.nikkei.com/economy/trade-war/as-us-scrutiny-mounts-is-tiktok-set-to-be-the-next-huawei>
- Zhai, K. (2023, March 6). China to Create New Top Regulator for Data Governance. *The Wall Street Journal*. <https://www.wsj.com/articles/china-to-create-new-top-regulator-for-data-governance-c9317233?msockid=32487172acb3632920316625ad43621a>
- Zhang, H. (2022). Agility over stability: China's great reversal in regulating the platform economy. *Harvard International Law Journal*, 63(2), 301–358. https://journals.law.harvard.edu/ilj/wp-content/uploads/sites/84/HLI203_crop-3.pdf
- Zúñiga, N., Datta Burton, S., Blancato, F., & Carr, M., (2024). The geopolitics of technology standards: Historical context for US, EU and Chinese approaches. *International Affairs*, 100(4), 1635–1652. <https://doi.org/10.1093/ia/iaae124>.

Qingxiu Bu has published widely in a variety of areas of law, many of which are themed around law and global challenges, with a particular focus on the development of legal infrastructures in transnational law and global governance. He has previously worked at Cardiff Law School, Cardiff University, and the School of Law, Queen's University Belfast, during which he taught Transnational Business Law at the Center of Transnational Legal Studies (CTLs), Georgetown University as Adjunct Professor. Qingxiu was appointed as Li Kashing Professor of Practice at the Faculty of Law, McGill University, in 2019. He has held visiting posts at various institutions, including Lund University, Tel Aviv University and the Max Planck Institute for Comparative and International Private Law in Germany. He also served as a Docent at the Institute of Global Law and Policy (IGLP), Harvard Law School. Over the years, Qingxiu has completed four projects funded, respectively, by the British Academy, the Department for Business, Energy & Industrial Strategy (BEIS), the Newton Fund and the British Council (PMI).