Politics and Governance
2025 • Volume 13 • Article 10361
https://doi.org/10.17645/pag.10361

cogitatio

ARTICLE

Open Access Journal

A Geopolitical Economy Analysis of China and India's Approaches to Transnational Data Governance

Yujia He [1] and Ka Zeng [2]

[1] Patterson School of Diplomacy and International Commerce, University of Kentucky, USA
[2] Department of Political Science, University of Massachusetts Amherst, USA

Correspondence: Yujia He (yujia.he@uky.edu)

Submitted: 18 March 2025 **Accepted:** 10 July 2025 **Published:** 10 September 2025

Issue: This article is part of the issue "The Geopolitics of Transnational Data Governance" edited by Xinchuchu Gao (University of Lincoln) and Xuechen Chen (Northeastern University London), fully open access at https://doi.org/10.17645/pag.i437

Abstract

Recent literature on the behavior of rising powers in digital trade and data governance highlights their discourses of data sovereignty and desire to preserve domestic policy autonomy. This article contributes to the literature by employing a political economy lens that shifts the focus from the nation-state/inter-state framework towards the dynamics of state–capital relations, allowing for a more historical and contextual understanding of the geopolitics of data governance in emerging economies. Using China and India—two of the largest emerging economies—as comparative cases, and drawing on secondary data from government documents and other sources, the article argues that the interplay between the state's interests in promoting security and development objectives and the commercial interests of domestic firms, global Big Tech companies, and transnational capital in data commercialization and market expansion has shaped the two countries' respective trajectory of data governance over the past three decades. These developments are deeply embedded in each country's distinctive political economic and geopolitical contexts. As a result, key policy developments in digital governance that might appear to be driven primarily by geopolitics may instead have deeper roots in evolving state–business relations.

Keywords

China; data governance; economic interests; geopolitics; India; rising powers

1. Introduction

With the rapid pace of digital transformation across the Global South, an increasing number of emerging economies, especially the BRICS (Brazil, Russia, India, China, and South Africa), have developed their distinct

approaches to transnational data governance based on the notion of "data sovereignty" (Belli et al., 2024). As the cyberspace becomes less Western-centric, rising powers also call for more representation in global digital trade and data governance (He & Zeng, 2024). Policymakers and academics have contested the existing US-centric multistakeholder governance model, arguing that it privileges the interests of the private sector and reinforces the dominance of the incumbent powers (Arsène, 2016). There is considerable speculation about whether the ascendence of these emerging digital economies may generate further tensions in this "post-liberal order" (Barrinha & Renard, 2020, p.749), and whether transnational data governance as an emerging arena of geopolitical tensions may threaten "international coordination in the global data economy" (Arner et al., 2022, p.623).

Much of the recent international relations literature discussing the behavior of rising powers in transnational data governance highlights their discourses of sovereignty and desire to preserve domestic policy autonomy (Adonis, 2019). It is certainly useful, and should be commended, to "bring the state back in" to the discussion of global internet governance (Drezner, 2004, p. 477), an approach that could mitigate the epistemological focus on technical design negotiations in earlier literature (DeNardis, 2009). However, by contrasting the positions of emerging powers with those of the US, this framing risks overlooking the historical contexts of domestic tech industry development and the dialectical relationship between the state and transnational capital and tech companies.

This article adds to the literature by employing a (geo)political economy lens that shifts from either the dominant state-centric/inter-state framework or the earlier focus on technical design and administration of networked technologies, towards the local dynamics of state–firm relations. While not seeking to minimize the importance of inter-state power competition, this study contends that political economic forces, specifically the dynamic relations between the state and capital (both domestic and international), are important in shaping emerging economies' evolving approaches to data governance, behind the often-used buzzword of data sovereignty. The study seeks to answer the following research question: How have the interactions between state interests and the interests of domestic and international capital influenced the rising powers' approach to transnational data governance under evolving global geopolitics?

The study argues that for large emerging economies such as China and India, the interests of the state in promoting security and development objectives, along with the commercial interests of platform companies and transnational capital in data commercialization and market expansion, conditioned by their respective geopolitical as well as domestic political economic contexts, have shaped their evolving approaches to data governance. As digital platforms become infrastructuralized and transnational while amassing vast amounts of citizen data, both states have also considered data as assets with economic and strategic value and developed regulations against the background of shifting global geopolitical dynamics. Regulations concerning cross-border data remain in flux, with nuances, flexibilities, and even scale-backs in policy formation and implementation.

2. The Geopolitical Economy of Data Governance

2.1. Understanding Transnational Data Governance in Emerging Economies: The Limitations of a State-Centric Approach

Extant literature on data governance tends to focus on technical design and network administration, distinct national or supranational approaches to data governance, and patterns of global governance. One strand of the literature focuses on data standards, architecture, infrastructure, interoperability, privacy protection, and anonymization techniques and how they may affect compliance with data governance rules such as the European Union's (EU's) General Data Protection Regulation (GDPR; Khatri & Brown, 2010; Mishra, 2021; Purtova, 2018). As Tang (2022b) pointed out, the earlier mainstream internet governance scholarship focused on technical architectures and protocols, concerns which were in part driven by the dominant multistakeholder governance approach (DeNardis, 2009).

Another stream of the literature highlights distinct national approaches to data governance, showing a broad contrast between the emerging economies' data governance approaches and those of the incumbent Western powers. Large emerging economies, especially the BRICS, have pursued "digital sovereignty" or, specifically regarding data governance, "data sovereignty," as fundamental elements of their digital transformation (Belli et al., 2024). The concept of "digital sovereignty" has emerged as a political buzzword invoked in diverse narratives, policy discourses, and governance practices across multiple countries and regions (Pohle et al., 2024). Generally, it refers to "calls for a stronger role for the state, for strategic autonomy and digital borders," shown in national initiatives "aimed to regain control over strategic data, such as policies of data localization or reshaping of the architecture of connectivity," and its various discourses and practices represent a "condensation and materialization of these new geopolitics of data flows" (Glasze et al., 2023, p. 920). In contrast, the US government has long pursued a market-driven approach to data governance, protecting cross-border data flow, preventing data localization and web blocking, ensuring digital security, and facilitating internet services (Fefer, 2020). While the EU similarly encourages cross-border data flows, its emphasis on the protection of personal data and privacy, and increasing concerns about economic competitiveness, strategic autonomy, and technological sovereignty, have contributed to a rising EU digital sovereignty discourse that allows limited exceptions to free flows (Falkner et al., 2024; Farrand & Carrapico, 2022; Floridi, 2020). Barrinha and Renard (2020, p.758) noted that there is a fundamental divide between countries that "defend the principle of cyber sovereignty and the need to maintain public order in the cyberspace" and those that champion "an open and free internet," reflecting broader tensions within a contested and shifting "post-liberal order." O'Hara and Hall (2018, pp. 6–9) similarly argued that the geopolitics of internet governance should be understood as an uneasy coexistence and competition between the "European bourgeois internet," the "Chinese and Russian authoritarian internet," and the "American commercial internet."

This division can also be found in discussions of global internet governance. Scholars have emphasized that the US, as the center of global digital capitalism and economic networks, holds structural power, which in turn solidifies the power asymmetry of the global communications networks. This allows the US to weaponize such "interdependence" for extraterritorial surveillance and sanctions as coercive tools at times of confrontation (Farrell & Newman, 2019). Nonetheless, the US dominance in global communications and the US-centric multistakeholder governance model have generated many grievances and contestations, on

the ground that the resultant global governance institutions prioritize the interests of the private sector, allow limited inclusion in participation, threaten the domestic policy autonomy of developing states, and sustain the dominance of the Western powers (Arsène, 2016; Jongen & Scholte, 2022). Research on the EU often highlights the so-called "Brussels effect," through which the EU leverages firms' desire to access its internal market to exert regulatory influence, resulting in the potential de jure or de facto harmonization of regulatory standards globally (Bradford, 2020). However, some question the long-term feasibility of the EU's regulatory influence and its ability to maintain digital sovereignty (Calderaro & Blumfelde, 2022). As geopolitical tensions rise among major powers, some scholars bemoan that data governance has become a "wicked problem" and that differing approaches among countries may threaten "international coordination in the global data economy" (Arner et al., 2022, p. 623) or even fragment the internet (Polatin-Reuben & Wright, 2014).

Recent international relations literature discussing data governance in relation to geopolitics often adopts a realist perspective, portraying states as engaged in a power struggle for status and influence within a competitive inter-state system. While some scholars also explore alternative dimensions of digital sovereignty such as citizens' empowerment against the tech sector (e.g., Mügge, 2024), or contest the state boundary-based thinking (Chander & Sun, 2023), the external dimension, characterized by a "state-centered and security-politics narrative" (Adonis, 2019), has gained prominence in discussions of the BRICS economies' approaches (O'Hara & Hall, 2018; Rosenbach & Mansted, 2019; Zinovieva & Shitkov, 2023). This state-centric focus mitigated the earlier tech-deterministic epistemological approaches that had rendered "the issue of state and sovereignty obsolete and irrelevant" (Tang, 2022b, p. 2399), calling attention to how internet governance rules are made and the power dynamics among nation states amidst geopolitical tensions.

However, perhaps unintentionally, by contrasting the data governance approaches of rising powers with those of the incumbent powers (notably the US) and emphasizing the latter's liberalization stance, this state-centric framing implicitly reinforces the earlier imagination of the internet as an open commons guided by market incentives with minimal government intervention (Lessig, 1998). As critical scholars of communications have argued, such an imagination overlooks the reality of the internet's Cold War origins, Washington's historically active role in shaping information and communication technology policies and practices in the developing world, and its long-armed control over American information and communication technology firms' international operations (Aouragh & Chakravartty, 2016; Cartwright, 2020).

Moreover, the state-centric and security-politics focus, while avoiding technical determinism, risks swinging the pendulum too far, giving inadequate attention to the roles of firms and their engagement with various players in policymaking and implementation, and the practices of data governance arising from these interactions. Major digital platform companies may assume the role of "ambassadors" of their home countries (Carr, 2016). However, for homegrown platforms in emerging economies like China and India, their relationships with domestic and foreign government entities, international tech firms, and transnational capital often involve a complex mix of collaboration and contestation (Shen, 2016; Thomas, 2019).

Notably, how data governance in emerging economies is influenced by the dialectical relations between the state and businesses remains largely underexplored. As Belli et al. (2024) argue, the simple division of liberal and non-liberal states can overlook the multi-faceted concerns for data sovereignty and the "complex 'datafied' global value chains dominated by financialized transnational companies headquartered in central

economies." Data regulations in emerging economies are often shaped by a combination of security, regulatory, economic, and technical considerations. These include safeguarding national security against emerging threats, protecting citizen rights, shielding public and private services from cybersecurity and privacy risks, ensuring domestic regulatory or legal compliance, promoting local industry and innovation development with global linkages, and fostering strategic autonomy to build digital capabilities independent of external actors (Belli et al., 2024; X. Chen & Gao, 2024; Foster & Azmeh, 2020; He & Zeng, 2024; Jiang, 2024). Our study extends the literature by emphasizing how the dynamic and evolving transnational data governance approaches of emerging economies are shaped not only by national security concerns driven by geopolitics but also by domestic political economy considerations.

2.2. Towards a Historical, Contextualized (Geo)Political Economy Lens

To overcome the limitations of the state-centric/inter-state framework dominant in recent literature, this study adopts an approach frequently utilized by political economy scholars of information that treats the cyberspace as "layered, varied and evolving" and as "a socio-technical and ultimately geopolitical environment" (Hong & Goodnight, 2020). This perspective "highlights the need to understand the historical contexts and dialectical relations" involved in "the enabling and conditioning of actors in policy processes" (Tang, 2022b). Instead of treating the internet as a boundless, frictionless open commons, critical political economy scholars view it as a space fraught with tensions and contradictions. Therefore, the subjectivity of various actors within and beyond the state and the power dynamics among them in rule-making are important considerations (Mosco, 2009).

As this study illustrates, the development of data governance approaches in both China and India is influenced by the dynamic interplay between the governing authority, the domestic tech platforms, private capital, and international tech firms and transnational capital. This relationship is deeply rooted in the unique historical development of digital industries and local socioeconomic contexts. In both cases, we are interested in key turning points in each country's data governance regime as our dependent variable, with business–state interactions serving as the main independent variable. While the specific pathways linking the two diverged somewhat in the two countries, our analysis underscores the similarities in how external pressures were filtered through the domestic political economic landscape as interest groups in each country navigate the respective institutional setting to mold the policy outcome.

In this vein, this study contributes to the emerging political economy literature on the evolving digital landscape in emerging economies against the backdrop of geopolitical tensions (W. Chen, 2022; Grover et al., 2024; Kumar & Thussu, 2023; Lei, 2023; Schroeder, 2022; Shen & He, 2022; Tang, 2022b). As Qiu et al. (2022, p. 2335) proposed:

> A novel geopolitical approach analyzes 'Chinese internets' as internally diverse and externally border-crossing; as both public (governmental and non-governmental) and private (e.g., corporate); as discursive and policy entanglements beyond the dichotomy of multistakeholderism and multilateralism; and as global, regional, and local formations that are connected to, but not entirely constrained by, their national counterparts.

Similarly, this study treats the geopolitics of data regulations in emerging economies as an evolving and dynamic process that involves public and private players both internally and externally, with the state's key

policy responses to heightened external risks underpinned by such two-way interactions. Analytically, this historical, contextualized approach to explaining changes in transnational data governance based on the dialectical relations between state institutions, private platforms, and capital resonates with L. Zhang and Chen's (2022, p.1454) call for a "regional and historical approach" that helps to "deprovincialize platform studies and extend its analytical relevance beyond the Euro-American focus or the disciplinary boundaries."

This study additionally echoes the call for a "geopolitical economy" research agenda in international relations, moving beyond "geopolitical fetishism" and the narrow strategic or security-centric focus common in policy analysis (Jayasuriya, 2021). As Wijaya and Jayasuriya (2024, p. 2139) argue, one of the most significant developments in international political economy in the past few years has been "the emergence of a new business class in emerging markets with international connections." These emerging market multinationals "seek to shape new projects of globalization which are often, confusingly, seen as new forms of statism" (Wijaya & Jayasuriya, 2024, pp. 2139–2140). This study's analysis similarly highlights how emerging economies' regulatory approaches to data governance have in part been influenced by the logic of capitalist accumulation by private companies. Domestic private digital platforms have grown with both the help of international capital and technology partners in a domestic policy environment that enables market expansion and the gathering of user-generated data. Having built "ecosystems" that straddle domestic public and private services, these homegrown platform companies are also internationalizing (J. Y. Chen & Qiu, 2019; Shen & He, 2022). In response, emerging economies' governments, through digital policy and data regulations, seek to facilitate the firms' capitalist accumulation, while also guarding against possible risks to political stability, including those brought by their international linkages. Meanwhile, the interplay among various domestic and international players, and the realignment of actors in the accumulation process are deeply influenced by each country's domestic political, socioeconomic, and geopolitical circumstances, leading to varied data governance approaches. Consequently, key policy developments in both countries' approaches to data governance that may, at first glance, be attributed to geopolitical tensions may instead need to be placed in the context of evolving state–business relations in their domestic political economy.

3. Methodology

This study employs a qualitative and comparative case study approach that enables an in-depth exploration of emerging economies' evolving approaches to data governance (Ragin & Becker, 1992). Specifically, it addresses the question of how the state's interests in national development agendas and the domestic and transnational private capital's business interests interact to shape government regulations concerning data governance amidst changing global information geopolitics. Such an approach provides valuable insights into not only broad patterns but also variations across cases, therefore contributing to more nuanced explanations of how data governance regimes have evolved in different national contexts. China and India were chosen as the case studies as they are the two largest emerging economies in terms of both the size of their economy and the number of internet users (World Bank, 2024). Qualitative data were collected through a systematic review of scholarly literature, news articles, official documents and government policies, and speeches by government officials and business leaders, to allow for in-depth analysis and systematic comparison of regulatory developments over the past three decades. Data analysis was performed concurrently with data collection to compare the findings against the initial propositions derived from the literature review.

4. The Case of China

This section traces the geopolitical economy of China's data governance development, emphasizing the mediating role of the dialectical relationships between the Chinese state and capital.

4.1. Early Developments in State–Business Relations in Digital Governance: 1990s–Early 2010s

In the early years of its digital economy development from the 1990s until the late 2000s, the Chinese state's approach to internet governance simultaneously emphasized the potential of digital connectivity to facilitate knowledge transfer, trade and economic development, domestic capacity development through joint ventures, and the preservation of national sovereignty and political stability through information control but pluralization of online discourses (Han, 2018; Shen, 2016; Tang, 2022b). Such a permissive policy environment enabled the expansion of Western technology companies such as IBM, Microsoft, Dell, Cisco, Amazon, and Google in the Chinese market, often in partnership with Chinese businesses in the form of joint ventures. China was a latecomer to data governance, with only three domestic regulations over data concerning ID card data, information security protection, and medical data confidentiality by 2010 (Sacks et al., 2019). Moreover, coordination among ministries, even at the central level, was limited (Shen, 2016).

With the rise of new technologies such as cloud computing and the government's shift towards high-tech development in economic planning in the late 2000s and early 2010s, the Chinese government sought to provide a favorable policy environment to promote the development of the digital sector as one of the pillars of the national economy. The State Council named next-generation computing as one of the "strategic emerging industries" in 2010, with significant implications for economic growth and the structural upgrading of the economy, followed by a series of official documents and policies from the relevant government ministries (State Council of the People's Republic of China, 2010). Meanwhile, domestic tech companies such as Baidu, Alibaba, and Tencent (collectively known as BAT) had sprung up as strong rivals to global tech firms in the Chinese market, bolstered by the financial backing of transnational venture capital and the expertise of senior executives with prior experience in Western tech firms (Shen, 2019).

4.2. The Snowden Revelation as a Catalyst for Change: Rising Data Regulations in the 2010s

Notably, China's data governance regulations took a sharp upturn in 2013 (Sacks et al., 2019) in response to Edward Snowden's revelation of the US government's global surveillance networks which, by reinforcing concerns about data security and information geopolitics, provided renewed impetus for the Chinese government to reform internet governance and emphasize data localization. Chinese official media expressed concerns that the operation of eight US technology companies—Apple, Cisco, Google, IBM, Intel, Oracle, Qualcomm, and Microsoft—in the Chinese market may enhance the ability of the US National Security Agency to influence the Chinese government, military, businesses, and academic institutions (Tang, 2022b). The central government subsequently created the Central Leading Group for Cyberspace Affairs and the Cyberspace Administration of China (CAC) in February 2014 to strengthen oversight of China's internet security and the implementation of its internet governance strategy. The CAC took over the responsibilities of the joint task forces under the State Council for safeguarding the strategic importance of China's information industry. A flurry of policies was created in the next few years, including the Internet Plus policy, which systemically planned the development of digital infrastructure and industrial ecosystem, and the

National Cyber Security Strategy, both in 2016, and numerous legal amendments and administrative regulations covering various aspects of internet governance. Market entry was tightened: For example, the Ministry of Industry and Information Technology revised the telecom business catalog in 2015 and identified cloud computing as a value-added service for which a pre-operation license would be required. The most notable legal development was the passage of the 2017 National Cybersecurity Law. Building on previous regulations, this law tightened data localization policies by requiring "critical information service providers" to store personal information or important data within the national border (Creemers et al., 2017).

4.3. Changing Power Dynamics in Chinese Tech Industry Development in the 2010s

The above policy changes contributed to shifting power dynamics and actor realignment in the capitalist accumulation of the Chinese tech industry. Transnational capital and Western tech firms were still important business partners in financing and joint projects with domestic platforms and venture capital (Tang, 2022a), and institutes such as Microsoft Research Asia were instrumental in producing talents who went on to work in Chinese tech firms and found startups. Yet with the industrial planning and localization policies, domestic platforms grew much more rapidly and became influential "ecosystem builders." Some local governments, eager to show alignment with the central government's agenda and willingness to support the local economy, also facilitated the market expansion of domestic tech firms through government contracts or public–private partnerships like Alibaba's Taobao Villages pilots in Zhejiang Province. The liberal and enabling environment for investment in the tech sector allowed Chinese homegrown platforms such as BAT and newcomers like ByteDance to acquire an enormous amount of economic power by expanding services beyond their core business to encompass almost all of Chinese users' online and offline activities, essentially achieving an infrastructural role in the Chinese society (Plantin & De Seta, 2019; Shen, 2021; Tang, 2019). This newly emerged platform capitalism, however, elevated the platforms' power and position vis-à-vis government officials (Su & Flew, 2020) and, in some cases, left regulators relatively powerless vis-à-vis corporate giants (Qiu, 2023). As Qiu (2023) argues, because of the rising power of China's tech giants, Beijing increasingly faced the dilemma of further liberalizing the domestic economy and promoting China's integration into the liberal international economic system on the one hand and maintaining the party-state's continued autonomy and leadership on the other.

Meanwhile, Chinese platforms started expanding internationally, resulting in record-high overseas investments by 2016 (He, 2024a). Some followed a deliberate "parallel platformization" approach to fit the divergent policy frameworks and platform ecosystems in China and abroad, such as ByteDance's video-sharing apps Douyin in China and TikTok overseas (Kaye et al., 2021). Nonetheless, similar to American platforms like Facebook and Google that came under increasing regulatory oversight both domestically and overseas, these Chinese infrastructuralized platforms' expansion in the global internet soon faced not just concerns about their dominating socioeconomic power and potential political leverage within China, but also their international operations and cross-border data flows. This was evidenced by new legal developments overseas that echoed the concerns of Chinese regulators (Wang & Gray, 2022). For example, the EU's GDPR, adopted in 2016, was a milestone legislation mandating data privacy of EU citizens for firms seeking access to the EU market, amplifying calls for the development of similar data protection laws in China. Rising geopolitical tensions further subjected these Chinese platforms to closer scrutiny from overseas regulators, notably the US.

4.4. Shifting State–Business Relations and Data Regulations Amidst Rising US–China Tensions and Internal Challenges

Once again, geopolitical tensions following the US–China trade war starting in 2017 provided the pretext for Beijing to engage in stricter regulations and to eventually crack down on domestic platforms since 2020. The US Trump administration used "national security" as justification to address China's trade practices, trade surplus with the US, and competitive challenges in high-technology development (Sun, 2019). In addition to imposing sanctions on Chinese telecom equipment providers Huawei and ZTE, Washington took a series of actions against Chinese platforms, including the proposed ban of TikTok, opposition to Ant Financial's acquisition of Moneygram, and the Clean Network Initiative, which sought to prohibit Chinese cloud providers from operating in the US and allied countries (He, 2024b; Shen & He, 2022; Steinbower, 2020).

Domestically, the heydays of neoliberal platform capitalism gradually came to an end in 2020, giving way to a new era of tighter control under "state platform capitalism" (Rolf & Schindler, 2023), whereby the state began to exert growing influence over platform development. Notably, rising inequality and poverty in the Chinese society prompted the central leadership under Xi Jinping to consolidate power and to counter threats to political stability and the legitimacy of China's techno-nationalist agenda by, among other measures, introducing reforms to digital governance to reassert government control and promote more balanced socioeconomic development (Au, 2023; A. H. Zhang, 2024; Zhao, 2022). Official discourse emphasized "common prosperity" and the "virtual economy serving substantive economy," justifying the tech crackdown as a policy experiment to combat rising inequality (Qiu, 2023).

Heightened geopolitical contestations provided further impetus for the government to strengthen data protection and enhance data security frameworks, especially as they relate to personal data. Beijing introduced a series of regulatory and legal measures, including the imposition of export controls on algorithms used in social media platforms in August 2020, a move that is widely perceived to influence the overseas operations of TikTok and other Chinese firms. In October 2020, Chinese officials halted the 34 billion USD initial public offering (IPO) of Ant Group, the financial services arm of Alibaba, on the Shanghai and Hong Kong stock exchanges, presumably in a move to reassert the government's authority over domestic commerce and society and to enforce the party's will (Zhong, 2020). This was followed by the levying of a record 18 billion RMB (2.75 billion USD) fine on Alibaba for allegedly abusing its dominant market position according to an anti-monopoly probe (Murdoch & Stanway, 2021). In 2021, two major new legal developments significantly reshaped China's data governance landscape. The Data Security Law introduced requirements for government approval for the transfer of data stored in China to protect national security and public interest (Creemers, 2022), including more stringent requirements for processing "important," "core state," or "sensitive" data (Belli, 2021). Another legislation, the Personal Information Protection Law, regulated the collection and processing of personal data, further expanding the scope of application of the earlier National Cybersecurity Law and broadening data localization requirements (Creemers, 2022). While the Personal Information Protection Law bears resemblance to the GDPR in its scope, key principles, and concepts, and in the provision of some important safeguards to protect individuals, it also diverges in certain areas. These include the lack of meaningful constraints on the state's access to and use of personal data, the institutional arrangements to enforce the law, and the imposition of ex ante state oversight on data localization (Creemers, 2022; W. Li & Chen, 2024).

The case of Didi further illustrates the evolving power dynamics between platform companies and the state. In June 2021, the CAC initiated antitrust investigations against the ride-hailing giant Didi Chuxing, shortly after its successful IPO on the New York Stock Exchange caught the regulators by surprise. The CAC stated that the firm had breached data protection rules and issued an order to remove Didi's app from local app stores (Eamon & Lau, 2021). Didi was fined 8 billion RMB (1.2 billion USD) for violating data privacy, data security, and cybersecurity laws, and was subsequently delisted from the New York Stock Exchange in June 2022 (Warren & Zhu, 2022). Although initially viewed as a partner in digital development, Didi gradually came under increased government scrutiny as concerns grew over the national security risks posed by foreign entities potentially accessing vast amounts of sensitive data (C. Zhang, 2024). The listing of companies such as Didi in the US may have further heightened concerns that such firms might be compelled to comply with foreign regulations and even cede their data to foreign governments, thereby compromising Beijing's oversight. A new version of the Cybersecurity Review Measures took effect in 2022, requiring businesses holding more than one million Chinese individuals' data to apply to the CAC for authorization and pass a cybersecurity review before being listed overseas (Warren & Zhu, 2022).

However, amid the economic downturn compounded by the Big Tech slump and the pandemic, the Chinese government has come under increasing pressure to strike a balance between regulation and business facilitation, prompting the relaxation of certain cross-border data transfer requirements and introducing flexibilities in actual policy implementation. For example, in 2024, one year after implementing the Measures of Security Assessment for Data Export, the CAC narrowed the scope of the security assessment mandate, clarified alternative compliance mechanisms (such as standard contracts and certification), and expanded the range of business scenarios that qualify for exemption from compliance requirements, in an effort to reduce firms' compliance burdens (CAC, 2024; Tencent Research Institute, 2024). Numerous Free Trade Zones in China worked with firms and local cyberspace administrations to implement "negative lists" of cross-border data transfer, essentially exempting some businesses from strict compliance requirements ("Shuju kuajing liudong de zhongguo fangan," 2024). Businesses in the Guangdong–Hong Kong–Macao Greater Bay Area were allowed to coordinate data transfer between the mainland and Hong Kong/Macao through the Greater Bay Area Standard Contract (Au & Witzleb, 2024). In its effort to revive foreign investment, Beijing also faced the imperative to address foreign firms' concerns over regulatory constraints on data transfers. For example, European industry lobbying was among the factors leading the CAC to significantly relax its data export rules in 2024 (Arcesati, 2024). The Regulations on Network Data Security Management, active in 2025 following three years of discussions with stakeholders, further eased restrictions on cross-border data transfer, while clarifying firms' compliance obligations (including special requirements for large platforms), liabilities for violations, and measures for strict enforcement (B. Li, 2024).

Consequently, instead of approaching the Chinese data governance regime merely from the perspective of great power competition between two major internet powers, recent policy development should be viewed in the context of the historical trajectory of the Chinese tech industry and the evolving, dialectical relationships between the Chinese government, domestic firms, and global capital. While the state undertook major initiatives in response to rising external and internal pressures, firms were not completely passive receivers of regulatory shifts; instead, they actively influenced the implementation or interpretation of high-level laws by leveraging their economic significance.

5. The Case of India

This section examines the geopolitical economy of India's evolving data governance approach, focusing on the historical development of India's tech industry and its evolving relationships with the Indian state, foreign platforms, and transnational capital.

5.1. Historical Path of State–Business Relations in Digital Development

With the transition from Soviet-style central planning and self-sufficiency towards more open trade and investment promotion in the 1980s and 1990s, India emerged as an important global player in software and IT services, hosting numerous major companies such as Tata Consulting Services and Infosys and subsidiaries of international firms such as Motorola. However, in comparison to China, internet services such as e-commerce grew much more slowly in India, due to relatively low internet penetration, slow network speeds, diminished spending power of citizens, poor supporting infrastructure, and limited policy support (Singh, 2016; Subramanian, 2020; Thomas, 2009).

Nonetheless, a major wave of growth started in the late 2000s with the rise of homegrown companies like Flipkart, which was established in 2007 and became a leading e-commerce platform in India before its acquisition by Walmart in 2016. The entry of global platforms (eBay in 2004, Facebook in 2006, Amazon in 2013) led to the expansion of transnational tech capital within India's nascent internet industry. Meanwhile, until the early 2010s, the Indian government had implemented only a few regulations on data governance, mainly the IT Act and its amendments and regulations. These regulations focused on expanding the government's power of information monitoring and developing security practices and procedures for dealing with sensitive personal information (Chaudhuri & Joseph, 2024). Enhanced government surveillance drew criticisms from civil society, yet the government justified the legislation on the grounds of fighting terrorism and cybercrime (Subramanian, 2020).

5.2. Changing State–Business Relations Under Modi's "Digital India" Campaign

Prime Minister Narendra Modi's tenure as the country's leader starting in 2015 saw seismic changes in India's digital policy and state–business relations. Digital India, his flagship policy project, seeks to "transform India into a digitally empowered society and knowledge economy," envisioning "infrastructure as a utility to every citizen," "governance & services on demand," and "digital empowerment of citizens" (Ministry of Electronics and Information Technology of India, n.d., p. 14). The passage of the Aadhaar Act in 2016 launched a nationwide digital identity platform and created the world's largest biometric and personal information database containing Indian citizens' pictures, iris scans, and fingerprints, and the assignment of a unique identification number overseen by the Unique Identification Authority of India. A collection of associated software platforms and applications, called the "India Stack," was developed based on the state-generated Aadhaar database, and was promoted as a unique digital infrastructure to help India's digital transformation (Parsheera, 2024). For example, the United Payments Interface (UPI), a real-time instant payment system, was developed by the government for online payments. The 2016 demonetization initiative, by demonetizing certain banknotes (albeit with a haphazard rollout), facilitated the rapid rise of digital payments. As Hicks (2020, p. 331) has argued, the India Stack represents India's move towards "hybrid state–business digital capitalism." Mishra (2023, p. 255) critically characterized the government's close ties

with certain private companies as a relationship in which "the government depend[s] on the private sector for intimate surveillance of citizens, and the private sector depend[s] on the public digital infrastructure."

The datafication of the Indian society and the resultant market expansion of its tech industry led to rising interest from global tech capital and broadened India's integration in global digital capitalist networks. Global Big Tech and capital played major roles as shareholders and partners of domestic players. For example, Jio Platforms, the digital business arm of India's largest family-owned conglomerate and telecom provider Reliance Industries, raised billions of dollars from Google, Facebook, and private-equity firms like Silver Lake (Otto & Bellman, 2020). Chinese platforms and capital were also active: Before India tightened investment by Chinese firms in 2020, Chinese investors such as Alibaba, Tencent, and ByteDance held stakes in 18 of India's 30 unicorns (startups valued at over 1 billion USD), often alongside other major global investors like SoftBank, Sequoia Capital, and eBay (Bhandari et al., 2020).

5.3. Evolving Relations Between State and Non-State Actors Shaping India's Data Regulations Development

India's evolving data governance approach mirrored the government's intent to capitalize on the economic value of data and to promote platform capitalism by shaping market expansion, along with its quest for sovereignty and political stability. Rhetorically, "Data is the new gold (or oil)" was the catchphrase used in Modi's public speeches (Vila Seoane, 2021) and in documents such as the Draft E-Commerce Policy (Mishra, 2023) to justify data localization proposals. Sector-specific regulations mandating data storage on servers located in India were introduced in the telecom, banking, and health sectors. These included the 2018 Reserve Bank of India (India's central bank) regulation to require all system providers to store payment transactions data in India, and a subsequent decision in 2021 to bar new customer onboarding for payment services like Mastercard until successful compliance (Basu & Swaminathan, 2023). However, given India's limited state capacity, some argue that these regulations were not strongly enforced (Mishra, 2023).

Meanwhile, the desire to attract international capital investment and technology partnerships seemed strong enough to prompt the government to make some compromises. During the negotiations over the Regional Comprehensive Economic Partnership (RCEP), a mega free-trade agreement in the Asia Pacific region, India relaxed its foreign direct investment restrictions on e-commerce to allow for 100% foreign ownership. India also reversed early objections to RCEP's e-commerce draft chapter, which contained a prohibition of data localization but provided broad carve-outs for domestic security and public policy exemptions, to allow the chapter to go through. However, India ultimately withdrew from the RCEP negotiations in 2019 due to other concerns (He & Zeng, 2024).

The evolving relationships between the government, domestic businesses, and foreign Big Tech, grounded in India's political economic context, were apparent in the debates shaping India's key data legislation. The first draft of the Personal Data Protection Bill in 2018, along with its 2019 revised version, shared many high-level principles and specific provisions with the EU's GDPR. However, crucial divergences remained, including in international data transfer (Sen, 2021; Wimmer et al., 2020). The Bill advised prohibiting the transfer of "critical personal data" beyond Indian borders, and the processing of such data exclusively within India to avoid foreign surveillance, apparently alluding to the Snowden revelations of US intelligence operations (Vila Seoane, 2021). Geopolitical framing was employed to push for data localization. Prominent

politicians of Modi's ruling Bharatiya Janata Party, which has a history of nationalist ideology, framed Western platforms' dominance in the Indian market as "digital colonialism," and data localization requirements as necessary countermeasures (Vila Seoane, 2021). Domestic firms that stood to benefit from exclusive data access and localization, including platforms like Paytm, and conglomerates like Reliance, which owns Jio Platforms, similarly touted localization requirements (Basu & Nachiappan, 2020). Chinese tech firms like Alibaba, having invested in physical data centers in India, also supported data localization. Meanwhile, US firms fiercely opposed data localization, enlisting lobbyist groups to engage US officials and Indian lawmakers to express concerns (Kalra, 2019). The US Trump administration subsequently made data localization a crucial talking point in US–India trade negotiations and threatened retaliation. Industry associations such as the Internet and Mobile Association of India also opposed data localization, citing the cost to start-ups and hurdles to innovation (Sinha & Basu, 2019). After several revisions and the withdrawal of the initial bill, the final Digital Personal Data Protection Act was passed in 2023. Compared to the initial draft, the final Act was significantly watered down in data localization requirements, permitting data transfer outside India to countries other than those blacklisted by the central government, while allowing sector-specific regulations. Nevertheless, it expanded the government's power over data usage and commercialization, granting broad exemptions for government agencies and providing the government with discretion to exempt certain companies from compliance while subjecting others to increased scrutiny (Grover et al., 2024).

5.4. Rising State Scrutiny of Platforms' International Capital Linkages and Data Practices

Another case of evolving relationships between the state, domestic platforms, and transnational capital concerns the UPI payments, which involved three major platform players, including the Walmart-owned PhonePe (part of Flipkart), Google Pay, and the homegrown Paytm. Following the 2020 Sino-Indian border clash, the Modi government banned scores of Chinese apps out of security concerns, and tightened investment rules in India for Chinese companies (Kharpal, 2020). At the time, Paytm was 30% owned by Ant Group and had received capital and technology support, as noted in Ant Group's IPO prospectus. The imposed restrictions subsequently prohibited any further investments. In 2022, the Reserve Bank of India punished Paytm for data flows overseas to Chinese entities that indirectly held stakes in the firm, while Paytm denied the allegations (Roy & Rai, 2022). In the same year, the Reserve Bank of India rejected Paytm's payment aggregator licensing application, granting the company an extension to reapply by March 2023. To alleviate concerns over Chinese investment, Ant Group reduced its stake to 9.88%, so that by August 2023, Paytm's CEO became the single-largest shareholder (Cornish, 2023). In early 2024, regulators closed part of Paytm's payment business for numerous compliance issues. Regulatory restrictions led to Paytm's market share shrinking to 8%, in comparison to PhonePe and Google Pay which processed 87% of UPI transactions. Meanwhile, a parliamentary panel report raised concerns of the foreign duopoly dominating the payments market, urging the government to support domestic fintech growth. By October 2024, regulators approved Paytm's onboarding of new users, while delaying actions on capping market share for PhonePe and Google Pay (Shetty, 2025). This suggests that while the government is still prioritizing the growth of the digital economy in view of the "emerging" stage of India's development, the platforms' expansion may continue to be subject to the state's scrutiny of their international capital linkages and data practices amidst geopolitical tensions.

6. Conclusion

This study seeks to unpack the dynamics of transnational data governance in large emerging economies, namely China and India, by examining the historical contexts of tech industry development and highlighting the mediating role of state–capital relations against the background of evolving global geopolitics. It contributes to the growing political economy scholarship on how geopolitical tensions shape internet governance and digital platforms development in emerging economies (Qiu et al., 2022; Shen & He, 2022; Tang, 2022b). Analytically, it advances the literature by employing a regional and historical approach to study platform capitalism (L. Zhang & Chen, 2022). More broadly, this study echoes the call for a geopolitical economy approach in international relations research that goes beyond "geopolitical fetishism" to understand geopolitical contestations within the broader context of capitalist transformation (Wijaya & Jayasuriya, 2024). Because of space constraints, this study does not discuss in-depth the institutional transformations within various state agencies or the role of civil society in influencing policymaking. Nevertheless, it serves as an exploratory endeavor to move the analysis beyond the narrow focus on inter-state security politics, towards a broader consideration of the interactions among various state and non-state actors.

Several conclusions and implications for research can be drawn from the above comparative case studies. First, both cases show that the geopolitics of transnational data governance in emerging economies should be approached not simply from the realist perspective of inter-state security politics seen in much of the digital sovereignty literature, but also from a political economy lens that gives more attention to the interactions among state and non-state actors rooted in the domestic socioeconomic contexts of technology industry development. In both the cases of China and India, the government's interests in shaping the domestic digital economy and promoting market expansion to serve the overall national development agenda, along with interests in maintaining national security and political stability, have been an essential focus of data governance regulations. Various private-sector entities are also important players in tech industry development and, in turn, data policy formulation in both countries. They include homegrown platforms that are increasingly infrastructuralized and internationalizing, other forms of domestic private capital, and global firms and transnational capital (such as global venture capital, private equity firms, and international stock markets) that seek to expand capitalist accumulation in emerging markets. The relationships amongst these non-state players and the government involve both collaboration and competition and, indeed, realignment under global information geopolitics (e.g., concerns over surveillance following the Snowden revelations and US–China tensions over trade and high-tech development). Yet these state–capital dynamics are also more complex than what some pundits may call "digital protectionism" or "digital authoritarianism" when critiquing localization rules, or "digital colonialism" when arguing for localization. Inter-state rivalries or alignments that appear on newspaper headlines should not blind us from viewing these internal and external state–capital interactions in the context of the processes of capitalist accumulation and transformation that influence the evolution of transnational data regulations in emerging economies.

Second, while our study has highlighted the common pressure exerted by geopolitical tensions on internet governance in both countries, there are also some differences between the two cases. These differences are rooted in each country's distinct historical trajectories of digital development, the dynamics of state–business relations, and the country's positioning within broader geopolitical shifts. The internet industry in China took

off in the 1990s, almost a decade earlier than in India. Beijing's push for techno-nationalist development since the late 2000s also predated Modi's Digital India project starting in 2015. While global Big Tech and transnational capital were indispensable players in the early development of the Chinese tech industry and still play viable roles as partners to Chinese firms, major Chinese tech platforms have dominated the Chinese market and society and become important players in global digital capitalist networks. This resulted in growing tensions with the Chinese state's leadership and policy autonomy, and an increasingly competitive relationship with US Big Tech, despite ongoing collaboration in areas where profit-seeking interests align, such as the financing of startups. Amidst broader US–China trade and tech wars, the Chinese state has sought to reassert its control and developed a comprehensive set of laws and regulations governing platforms and data flows. In comparison, India's homegrown tech industry is still relatively "emerging" and relies on global Big Tech and transnational capital for the technology, infrastructure, and financing needed for its development. This has led the government to adopt a more ambiguous and flexible approach towards regulating data flows in key data legislation, with watered-down mandates for data localization and yet broad executive power to scrutinize firms. As India's partnerships with US Big Tech and capital have strengthened after the forced exit of Chinese players following Sino-India tensions, one might expect the Modi government to continue to be somewhat amenable to the economic interests of US firms in follow-up regulations. While China's vision for digital sovereignty seems to be more clearly articulated through its data regulations, India currently leans toward more cautious rule-making and less concrete mandates to preserve the state's executive power in shaping domestic market development without seriously alienating US Big Tech and transnational capital that remain crucial to its high-tech ambitions.

The differences between China and India's political systems may at least partly account for the above variation. China's one-party system placed Beijing in a better position to exert strong controls over data flows, as seen in its ability to pass a series of legislations that increased the state's oversight over private firms. Despite the rising clout of domestic tech giants, the party-state's dominance in the domestic political economy enabled wide-reaching regulatory measures vis-à-vis domestic firms, though regulatory implementation showed some flexibility in response to business concerns. In contrast, India's multi-party democratic system provided greater room for domestic stakeholders and international businesses to shape and contest narratives and policies in data governance through lobbying and negotiation, leading to more open debates and challenges in policy rollout.

Finally, our study has broader implications for understanding data governance in emerging economies. Complementing existing scholarship's focus on the emerging economies' push for digital sovereignty, this study shows that regulations concerning cross-border data in both countries are still evolving, with nuances, flexibilities, and even scale-backs in policy formation and implementation. One may argue that this reflects the pragmatic interest of emerging economy governments in juggling internal political and economic considerations, external security concerns, and global standards in developing data regulations to deal with the challenges of changing global geopolitics. While the US's liberalization approach towards digital trade and the EU's privacy-focused GDPR frameworks certainly influence policy formulation in emerging markets, this study demonstrates that the distinct historical paths of national development and local socioeconomic realities continue to shape the government's vision for the internet economy and governance of digital platforms that handle massive amounts of data and expand internationally. Moreover, instead of a one-way street of the government imposing its will, data governance in emerging economies involves a dynamic process where various domestic and international non-state players influence state policymaking. This

means that, instead of trying to force analysis of data governance in emerging economies into frameworks aligned with the "US," "EU," or increasingly the "China" model, or a mix of them, a contextualized approach can unveil on-the-ground forces that mediate geopolitical considerations and shape policy development. While acknowledging the influence of major powers in data governance in emerging economies, such an approach gives due consideration to how the distinct dynamics of the local political economy have shaped the trajectory of data governance.

Funding

This project was partially supported by the University of Kentucky's OPVR CURATE Grant and UKinSPIRE (Seeding Partnerships for International Research Engagement) Grant.

Conflict of Interests

The authors declare no conflict of interests.

References

Adonis, A. A. (2019). Critical engagement on digital sovereignty in international relations: Actor transformation and global hierarchy. *Global: Jurnal Politik Internasional*, *21*(2), 262–282.

Aouragh, M., & Chakravartty, P. (2016). Infrastructures of empire: Towards a critical geopolitics of media and information studies. *Media, Culture & Society*, *38*(4), 559–575.

Arcesati, R. (2024, May 6). The data quagmire for German carmakers in China. *The Diplomat*. https://thediplomat.com/2024/05/the-data-quagmire-for-german-carmakers-in-china

Arner, D. W., Castellano, G. G., & Selga, E. K. (2022). The transnational data governance problem. *Berkeley Technology Law Journal*, *37*(2), 623–700.

Arsène, S. (2016). Global internet governance in Chinese academic literature. *China Perspectives*, *2016*(2), 25–35.

Au, A. (2023). China's internet sector reforms and the rise of ESG in the state techno-nationalist agenda. *Policy & Internet*, *15*(4), 646–664.

Au, A., & Witzleb, N. (2024). Data flows and data protection in the Greater Bay Area: The need for a coordinated legal framework. *The Chinese Journal of Comparative Law*, *12*, Article cxae013.

Barrinha, A., & Renard, T. (2020). Power and diplomacy in the post-liberal cyberspace. *International Affairs*, *96*(3), 749–766.

Basu, A., & Nachiappan, K. (2020, July 31). India and the global battle for data governance. *Seminar*. https://www.india-seminar.com/2020/731/731_arindrajit_and_karthik.htm

Basu, A., & Swaminathan, M. (2023, August 4). Will the India–US tech handshake foster digital trade and policy convergence? *The Diplomat*. https://thediplomat.com/2023/08/will-the-india-us-tech-handshake-foster-digital-trade-and-policy-convergence

Belli, L. (2021). Cybersecurity policymaking in the BRICS countries: From addressing national priorities to seeking international cooperation. *The African Journal of Information and Communication*, *28*, 1–14.

Belli, L., Gaspar, W. B., & Singh Jaswant, S. (2024). Data sovereignty and data transfers as fundamental elements of digital transformation: Lessons from the BRICS countries. *Computer Law & Security Review*, *54*, Article 106017.

Bhandari, A., Fernandes, B., & Agarwal, A. (2020). *Chinese investment in India*. Gateway House. https://www.gatewayhouse.in/wp-content/uploads/2020/07/Chinese-Investments_2020-Final.pdf

Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press.

Calderaro, A., & Blumfelde, S. (2022). Artificial intelligence and EU security: The false promise of digital sovereignty. *European Security*, *31*(3), 415–434.

Carr, M. (2016). *US power and the internet in international relations: The irony of the information age*. Springer.

Cartwright, M. (2020). Internationalising state power through the internet: Google, Huawei and geopolitical struggle. *Internet Policy Review*, *9*(3). https://doi.org/10.14763/2020.3.1494

Chander, A., & 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. 1–32). Oxford University Press. https://doi.org/10.1093/oso/9780197582794.003.0001

Chaudhuri, R., & Joseph, A. K. (2024). Living in a fragmented world: India's data way. *India Review*, *23*(2), 154–176.

Chen, J. Y., & Qiu, J. L. (2019). Digital utility: Datafication, regulation, labor, and DiDi's platformization of urban transport in China. *Chinese Journal of Communication*, *12*(3), 274–289.

Chen, W. (2022). Zoom in and zoom out the glocalized network: When transnationalism meets geopolitics and technopolitics. *Information, Communication and Society*, *25*(16), 2381–2396.

Chen, X., & Gao, X. (2024). Norm diffusion in cyber governance: China as an emerging norm entrepreneur? *International Affairs*, *100*(6), 2419–2440.

Cornish, C. (2023, August 7). China's Ant Group swaps stake in India's Paytm for debt. *Financial Times*. https://www.ft.com/content/1bd35c18-867d-48de-9c83-16ecd885d44b

Creemers, R. (2022). China's emerging data protection framework. *Journal of Cybersecurity*, *8*(1), Article tyac011.

Creemers, R., Webster, G., & Triolo, P. (2017). *Translation: Cybersecurity Law of the People's Republic of China (effective June 1, 2017)*. DigiChina. https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017

Cyberspace Administration of China. (2024). *Cujing he guifan shuju liudong guiding da jizhe wen*. https://www.cac.gov.cn/2024-03/22/c_1712776611649184.htm

DeNardis, L. (2009). *Protocol politics: The globalization of internet governance*. MIT Press.

Drezner, D. W. (2004). The global governance of the internet: Bringing the state back in. *Political Science Quarterly*, *119*(3), 477–498.

Eamon, B., & Lau, Y. (2021, July 6). Not just Didi: China's internet watchdog targets more U.S.-listed firms for 'national security' review. *Fortune*. https://fortune.com/2021/07/05/didi-chuxing-stock-app-cybersecurity-full-truck-alliance-boss-zhipin

Falkner, G., Heidebrecht, S., Obendiek, A., & Seidl, T. (2024). Digital sovereignty—Rhetoric and reality. *Journal of European Public Policy*, *31*(8), 2099–2120.

Farrand, B., & Carrapico, H. (2022). Digital sovereignty and taking back control: From regulatory capitalism to regulatory mercantilism in EU cybersecurity. *European Security*, *31*(3), 435–453.

Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security*, *44*(1), 42–79.

Fefer, R. F. (2020). *Internet regimes and WTO e-commerce negotiations*. Congressional Research Service.

Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philosophy & Technology*, *33*(3), 369–378.

Foster, C., & Azmeh, S. (2020). Latecomer economies and national digital policy: An industrial policy perspective. *The Journal of Development Studies*, *56*(7), 1247–1262.

Glasze, G., Cattaruzza, A., Douzet, F., Dammann, F., Bertran, M.-G., Bômont, C., Braun, M., Danet, D., Disforges, A., Géry, A., Grumbach, S., Hummel, P., Limonier, K., Münßinger, M., Nicolai, F., Pétiniaud, L., Winkler, J., & Zanin, C. (2023). Contested Spatialities of Digital Sovereignty. *Geopolitics*, *28*(2), 919–958.

Grover, R., Jang, K., & Su, L. W. (2024). Beyond digital protection(ism): Comparing data governance frameworks in Asia. *Journal of Information Policy*, *14*, 161–193. https://doi.org/10.5325/jinfopoli.14.2024.0005

Han, R. (2018). *Contesting cyberspace in China: Online expression and authoritarian resilience*. Columbia University Press.

He, Y. (2024a). Chinese digital platform companies' expansion in the Belt and Road countries. *The Information Society*, *40*(2), 96–119.

He, Y. (2024b). Chinese fintech goes global: Political challenges and business strategies. *Asia Policy*, *19*(1), 35–50.

He, Y., & Zeng, K. (2024). China in global digital trade governance: Towards a development-oriented agenda? *International Affairs*, *100*(5), 2195–2215.

Hicks, J. (2020). Digital ID capitalism: How emerging economies are re-inventing digital capitalism. *Contemporary Politics*, *26*(3), 330–350.

Hong, Y., & Goodnight, G. T. (2020). How to think about cyber sovereignty: The case of China. *Chinese Journal of Communication*, *13*(1), 8–26.

Jayasuriya, K. (2021). Beyond geopolitical fetishism: A geopolitical economy research agenda. *Australian Journal of International Affairs*, *75*(6), 665–677.

Jiang, M. (2024). Models of state digital sovereignty from the global south: Diverging experiences from China, India and South Africa. *Policy & Internet*,*16*(4), 727–738. https://doi.org/10.1002/poi3.427

Jongen, H., & Scholte, J. A. (2022). Inequality and legitimacy in global governance: An empirical study. *European Journal of International Relations*, *28*(3), 667–695.

Kalra, A. (2019, December 18). U.S.–India business groups plan to lobby for dilution of India's privacy bill—Sources. *Reuters*. https://www.reuters.com/article/world/us-india-business-groups-plan-to-lobby-for-dilution-of-indias-privacy-bill--idUSKBN1YM0H3

Kaye, D. B. V., Chen, X., & Zeng, J. (2021). The co-evolution of two Chinese mobile short video apps: Parallel platformization of Douyin and TikTok. *Mobile Media & Communication*, *9*(2), 229–253.

Kharpal, A. (2020, September 4). 'Chinese firms are learning a painful lesson': India's app crackdown opens doors for U.S. tech giants. *CNBC*. https://www.cnbc.com/2020/09/04/india-crackdown-on-chinese-tech-opens-doors-for-us-giants.html

Khatri, V., & Brown, C. V. (2010). Designing data governance. *Communications of the ACM*, *53*(1), 148–152.

Kumar, A., & Thussu, D. (2023). Media, digital sovereignty and geopolitics: The case of the TikTok ban in India. *Media, Culture & Society*, *45*(8), 1583–1599.

Lei, Y. W. (2023). *The gilded cage: Technology, development, and state capitalism in China*. Princeton University Press.

Lessig, L. (1998). Open code and open societies: Values of internet governance. The Charles Green lecture in law and technology. *Chicago-Kent Law Review*, *74*(3), 1405–1422.

Li, B. (2024). China issues the Regulations on Network Data Security Management: What's important to know. *IAPP*. https://iapp.org/news/a/china-issues-the-regulations-on-network-data-security-management-what-s-important-to-know

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*, Article 105994.

Ministry of Electronics and Information Technology of India. (n.d.). *Digital India*. https://www.meity.gov.in/static/uploads/2024/03/Running-single-file.pdf

Mishra, N. (2021). Building bridges: International trade law, internet governance, and the regulation of data flows. *Vanderbilt Journal of Transnational Law*, *52*(2), 463–510.

Mishra, N. (2023). Data governance and digital trade in India: Losing sight of the forest for the trees? In A. Chander & H. Sun (Eds.), *Data sovereignty: From the Digital Silk Road to the return of the state* (pp. 240–263). Oxford University Press. https://doi.org/10.1093/oso/9780197582794.003.0011

Mügge, D. (2024). EU AI sovereignty: For whom, to what end, and to whose benefit? *Journal of European Public Policy*, *31*(8), 2200–2225.

Murdoch, S., & Stanway, D. (2021, April 10). China fines Alibaba record $2.75 bln for anti-monopoly violations. *Reuters*. https://www.reuters.com/business/retail-consumer/china-regulators-fine-alibaba-275-bln-anti-monopoly-violations-2021-04-10

Mosco, V. (2009). *The political economy of communication*. Sage.

O'Hara, K., & Hall, W. (2018). *Four internets: The geopolitics of digital governance*. Centre for International Governance Innovation. https://eprints.soton.ac.uk/427838/1/Paper_20no.206web.pdf

Otto, B., & Bellman, E. (2020, July 15). Google to invest $4.5 billion in India's Jio Platforms. *The Wall Street Journal*. https://www.wsj.com/articles/google-to-invest-4-5-billion-in-indias-jio-platforms-11594815351

Parsheera, S. (2024). Stack is the new black? Evolution and outcomes of the 'India-Stackification' process. *Computer Law & Security Review*, *52*, Article 105947.

Plantin, J. C., & De Seta, G. (2019). WeChat as infrastructure: The techno-nationalist shaping of Chinese digital platforms. *Chinese Journal of Communication*, *12*(3), 257–273.

Pohle, J., Nanni, R., & Santaniello, M. (2024). Unthinking digital sovereignty: A critical reflection on origins, objectives, and practices. *Policy & Internet*, *16*(4), 666–671. https://doi.org/10.1002/poi3.437

Polatin-Reuben, D., & Wright, J. (2014, August 18). *An internet with BRICS characteristics: Data sovereignty and the balkanisation of the internet* [Conference paper]. 4th USENIX Workshop on Free and Open Communications on the Internet, San Diego, USA. https://www.usenix.org/system/files/conference/foci14/foci14-polatin-reuben.pdf

Purtova, N. (2018). The law of everything: Broad concept of personal data and future of EU data protection law. *Law, Innovation, and Technology*, *10*(1), 40–81.

Qiu, J. L. (2023). The return of billiard balls? US–China tech war and China's state-directed digital capitalism. *Javnost – The Public*, *30*(2), 197–217.

Qiu, J. L., Yu, P. K., & Oreglia, E. (2022). A new approach to the geopolitics of Chinese internets. *Information, Communication & Society*, *25*(16), 2335–2341.

Ragin, C. C., & Becker, H. S. (Eds.). (1992). *What is a case? Exploring the foundations of social inquiry*. Cambridge University Press.

Rolf, S., & Schindler, S. (2023). The US–China rivalry and the emergence of state platform capitalism. *Environment and Planning A: Economy and Space*, *55*(5), 1255–1280.

Rosenbach, E., & Mansted, K. (2019). *The geopolitics of information*. Belfer Center for Science and International Affairs.

Roy, A., & Rai, S. (2022, March 14). Paytm Bank punished for sharing data abroad, verification lapses. *Bloomberg*. https://www.bloomberg.com/news/articles/2022-03-14/india-said-to-punish-paytm-bank-for-data-leaks-to-chinese-firms

Sacks, S., Shi, M., & Webster, G. (2019, February 8). The evolution of China's data governance regime: A timeline. *New America*. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/china-data-governance-regime-timeline

Schroeder, R. (2022). Aadhaar and the social credit system: Personal data governance in India and China. *International Journal of Communication*, *16*, 2370–2386. https://ijoc.org/index.php/ijoc/article/view/19059

Sen, P. (2021). *EU GDPR and Indian Data Protection Bill: A comparative study*. SSRN. https://doi.org/10.2139/ssrn.3834112

Shen, H. (2016). China and global internet governance: Toward an alternative analytical framework. *Chinese Journal of Communication*, *9*(3), 304–324.

Shen, H. (2019). *China's tech giants: Baidu, Alibaba, Tencent*. Konrad-Adenauer-Stiftung. https://www.kas.de/documents/288143/4843367/panorama_digital_asia_v3b_HongShen.pdf

Shen, H. (2021). *Alibaba: Infrastructuring global China*. Routledge.

Shen, H., & He, Y. (2022). The geopolitics of infrastructuralized platforms: The case of Alibaba. *Information, Communication & Society*, *25*(16), 2363–2380.

Shetty, M. (2025, January 1). PhonePe, GPay get 2 years more to cut UPI market share. *The Times of India*. https://timesofindia.indiatimes.com/business/india-business/phonepe-gpay-get-2-years-more-to-cut-upi-market-share/articleshow/116843059.cms

Singh, N. (2016). Information technology and its role in India's economic development: A review. In S. Dev & P. Babu (Eds.), *Development in India: Micro and macro perspectives* (pp. 283–312). Springer. https://doi.org/10.1007/978-81-322-2541-6_14

Sinha, A., & Basu, A. (2019). The politics of India's data protection ecosystem. *Economic and Political Weekly*, *54*(49). https://www.epw.in/engage/article/politics-indias-data-protection-ecosystem

State Council of the People's Republic of China. (2010). *Guowuyuan guanyu jiakuai he fazhan zhanluexing xinxing chanye de jueding*. https://www.gov.cn/zwgk/2010-10/18/content_1724848.htm

Steinbower, C. (2020, August 18). President Trump accepts CFIUS's recommendation—Orders TikTok's Chinese owner to divest. *Winston & Strawn LLP Blog*. https://www.winston.com/en/blogs-and-podcasts/global-trade-and-foreign-policy-insights/president-trump-accepts-cfiuss-recommendation-orders-tiktoks-chinese-owner-to-divest

Su, C., & Flew, T. (2020). The rise of Baidu, Alibaba and Tencent (BAT) and their role in China's Belt and Road Initiative (BRI). *Global Media & Communication*, *17*(1), 67–86.

Subramanian, R. (2020). Historical consciousness of cyber security in India. *IEEE Annals of the History of Computing*, *42*(4), 71–93.

Shuju kuajing liudong de zhongguo fangan: Woguo tuidong shuju kuajing anquan youxu ziyou liudong shuping. (2024, June 1). *The Paper*. https://www.thepaper.cn/newsDetail_forward_27593350

Sun, H. (2019). U.S.–China tech war. *China Quarterly of International Strategic Studies*, *5*(2), 197–212.

Tang, M. (2019). *Tencent: The political economy of China's surging internet giant*. Routledge.

Tang, M. (2022a). Not yet the end of transnational digital capitalism: A communication perspective of the US–China decoupling rhetoric. *International Journal of Communication*, *16*, 1506–1531.

Tang, M. (2022b). The challenge of the cloud: Between transnational capitalism and data sovereignty. *Information, Communication and Society*, *25*(16), 2397–2411.

Tencent Research Institute. (2024, November 28). Yinshi zhiyi, mianxiang weilai: Woguo shuju kuajing liudong jizhi de chuangxin tansuo. *36kr*. https://36kr.com/p/3055821212488067

Thomas, P. (2009). Bhoomi, Gyan Ganga, e-governance and the right to information: ICTs and development in India. *Telematics and Informatics*, *26*(1), 20–31.

Thomas, P. (2019). *The politics of digital India: Between local compulsions and transnational pressures*. Oxford University Press.

Vila Seoane, M. F. (2021). Data securitisation: The challenges of data sovereignty in India. *Third World Quarterly*, *42*(8), 1733–1750.

Wang, Y., & Gray, J. E. (2022). China's evolving stance against tech monopolies: A moment of international alignment in an era of digital sovereignty. *Media International Australia*, *185*(1), 79–92.

Warren, S., & Zhu, L. (2022). *China's Didi fined over US$1 billion by Chinese data regulators*. Squire Patton Boggs. https://www.squirepattonboggs.com/-/media/files/insights/publications/2022/07/chinas-didi-fined-over-us-1-billion-dollars-by-chinese-data-regulators/chinas-didi-fined-over-1-billion-us-dollars-by-chinese-data-regulators.pdf

Wijaya, T., & Jayasuriya, K. (2024). A new multipolar order: Combined development, state forms and new business classes. *International Affairs*, *100*(5), 2133–2152.

Wimmer, K., Maldoff, G., & Lee, D. (2020). *Comparison: Indian Personal Data Protection Bill 2019 vs. GDPR*. IAPP. https://iapp.org/media/pdf/resource_center/india_pdpb2019_vs_gdpr_iapp_chart.pdf

World Bank. (2024). *Global digitalization in 10 charts*. https://www.worldbank.org/en/news/immersive-story/2024/03/05/global-digitalization-in-10-charts

Zhang, A. H. (2024). *High wire: How China regulates Big Tech and governs its economy*. Oxford University Press.

Zhang, C. (2024). China's privacy protection strategy and its geopolitical implications. *Asian Review of Political Economy*, *3*(1), Article 6.

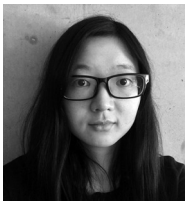
Zhang, L., & Chen, J. Y. (2022). A regional and historical approach to platform capitalism: The cases of Alibaba and Tencent. *Media, Culture & Society*, *44*(8), 1454–1472.

Zhao, S. (2022). *The dragon roars back: Transformational leaders and dynamics of Chinese foreign policy*. Stanford University Press.

Zhong, R. (2020, November 6). In halting Ant's I.P.O., China sends a warning to business. *The New York Times*. https://www.nytimes.com/2020/11/06/technology/china-ant-group-ipo.html

Zinovieva, E., & Shitkov, S. (2023). Sovereignty as practice in digital age. In A. Baykov & E. Zinovieva (Eds.), *Digital international relations* (pp. 75–90). Springer. https://doi.org/10.1007/978-981-99-3467-6_5

About the Authors



Yujia He is an assistant professor at the Patterson School of Diplomacy and International Commerce, University of Kentucky. Her research interests span science and technology policy, international political economy, development studies, and Asian studies.

Ka Zeng is professor of political science at the University of Massachusetts Amherst. Her research focuses on China's role in the global economy. She is the author or co-author of *Trade Threats*, *Trade Wars*, *Greening China*, and *Fragmenting Globalization*, all published by the University of Michigan Press.