Zhang *Asian Review of Political Economy* (2024) 3:6
https://doi.org/10.1007/s44216-024-00028-2

Asian Review of Political Economy

RESEARCH ARTICLE Open Access

China's privacy protection strategy and its geopolitical implications

Chi Zhang[1*]

*Correspondence: cz38@st-andrews.ac.uk

[1] University of St Andrews, St Andrews, UK

Abstract

How has China's privacy protection strategy been developed, with its broad scope and stringent requirements for data localization and cross-border data flows? What are the broader geopolitical implications of its divergence from Western models of data privacy? This paper argues that China's privacy protection strategy, characterized by its comprehensive regulatory framework and government access to data, is redefining the contours of global data governance and creating new geopolitical fault lines. Drawing on official documents, laws, regulations, and a case study, this paper highlights the evolution of the regulatory framework in response to emerging challenges posed by technological innovations and the wider geopolitical environment. This paper contributes to the broader discussion regarding the implications of China's privacy protection approach, highlighting potential normative clashes with countries that favor a more open digital economy. China's efforts in developing its own privacy protection strategy have also resulted in the formulation of global standards for data privacy.

Keywords: Data sovereignty, Digital economy, Privacy protection, Data localization, Cross-border data flow, Global data governance

Introduction

Data has woven itself into the very fabric of the global economy, with the digital economy further solidifying its presence in the wake of the COVID-19 pandemic. Against this backdrop, privacy protection has garnered significant attention, given its profound implications for international digital trade the geopolitical relations. How has China's privacy protection strategy been developed, with its broad scope and stringent requirements for data localization and cross-border data flows? What are the broader geopolitical implications of its divergence from Western models of data privacy?

This paper argues that China's privacy protection strategy, characterized by its comprehensive regulatory framework and government access to data, is redefining the contours of global data governance and creating new geopolitical fault lines. The landscape of global data governance is experiencing a significant shift due to the divergent privacy protection strategies adopted by China in contrast to those of the United States (US) and the European Union (EU). China's approach, characterized by a comprehensive scope, stringent data localization requirements, and a substantial allowance for government

intervention, represents an alternative model to the prevailing norms of digital privacy and data management championed by the US and EU.

This paper examines the evolution of China's privacy protection strategy with a focus on the balance between individual privacy and national security. Drawing on official documents, laws, regulations, and a case study, this paper highlights the evolution of the regulatory framework in response to emerging challenges posed by technological innovations.

This paper also contributes to the broader discussion regarding the implications of China's privacy protection approach, highlighting potential normative clashes with countries that favor a more open digital economy. China's efforts in developing its own privacy protection strategy have also resulted in the formulation of global standards for data privacy. This has created a bifurcation from the norms established by the EU's General Data Protection Regulation (GDPR), leading to a fragmentation of the global data governance regime.

For China, these different normative expectations and standards may potentially deter foreign enterprises. Different privacy standards introduce complexities into international trade, posing compliance challenges for transnational corporations and influencing the dynamics of global digital trade. These complexities can, in turn, have an impact on China's economy. For the international community, the normative competition evident in China's approach reflects the broader geopolitical rivalries and may also influence developing countries as they craft their own data governance policies, looking to major rule-makers such as the EU, US, and China as models to follow.

This paper proceeds as follows. The second section will lay out a theoretical framework for discussing China's privacy protection approach, focusing on China's distinct perspective on human security and the relationship between individual privacy and national security. The third section will examine the developmental path of China's privacy regulatory framework. The fourth section focuses on the case of Didi to illustrate the changing power dynamics between regulatory authorities and digital platforms, as well as the co-evolution of technological innovation and the regulatory framework. The fifth section explores the global implications of China's approach to privacy protection.

Human security and *Yinsi* protection

The concept of human security is highly relevant to the discussion of privacy protection, given the perceived distinctions between "collectivist" Chinese society and "individualist" liberal democracies. This concept serves as an analytical lens for exploring the different referent objects – the state and individuals – as the subjects to whom security is being provided.

This concept also helps tease out the relationship between individual privacy and national security, offering a perspective through which the states' concern regarding data sovereignty can be further examined – a concern that different types of regimes share. Given the challenges posed by technological innovation and the increasing capabilities of using data for various governance tasks, as well as the potential security risks associated with data misuse, China is not alone in its emphasis on data sovereignty. The US's decision to invalidate the EU-US Privacy Shield and the issuance of US executive orders targeting TikTok underscore Western concerns regarding the control over data

sovereignty (Hu 2021). Similarly, Canada implemented its own measures to safeguard Canadian data against the provisions of the US Patriot Act, which grant US authorities access to data stored within the US, irrespective of its source or origin (Treasury Board of Canada Government of Canada 2006). This shared concern highlights the importance of avoiding an oversimplified dichotomy between China's approach and the "Western approach" (Gao 2022a).

However, it is a challenging task to determine precisely at which point individual privacy becomes a matter of national security concern. China's regulatory framework has sought to offer clarity on this. For instance, it sets a threshold for subjecting an operator to a cybersecurity review, which is triggered by the personal information of 1 million users (Cyberspace Administration of China et al. 2022). Another example of attempting to determine the threshold for national security concerns regarding data is the categorization of data into "core data", "important data", and "other data" (Bi 2021). However, relying solely on the former quantitative approach is clearly inadequate, while the latter qualitative approach still lacks clarity in terms of its categorization criteria.

This regulatory underdevelopment in practice necessitates a more in-depth exploration of the relationship between state security and human security in the context of cyberspace governance. The debate surrounding human security reflects a shift in normative and policy focus from the state to individuals, who are now considered the primary "referent object" and "beneficiary" of security (Newman 2016). Like many other concepts, when brought into China, human security undergoes a process of Sinification, making it suitable for application in the Chinese context (Breslin 2015). Within the human security discourse as articulated in Chinese official documents, the state is portrayed as the "*source* of human security" (original emphasis), rather than being a potential challenge to it, thus shifting the focus from the individual as the reference point back to the role of the state (Breslin 2015, 249). Chinese scholars hold similar views. Mao and Ren argue that, from a national security perspective, the focal point of data sovereignty is the state rather than individuals. Building upon this premise, they advocate that the state should be able to control, manage, and safeguard the production, storage, flow, analysis, and utilization of data generated within the country (Mao and Ren 2023, 43).

Instead of outright rejecting the notion of human security, China has sought to engage and adapt this concept by defining "human" in a more collective sense (Jones 2022). Jones questions the interchangeable use of the terms "security" and "safety" in the translation of Chinese official documents to refer to the Chinese term "*anquan*" and argues that the distinction between these terms lies in the role of the state and the implications for state actions (Jones 2022). China's discourse on *anquan* emphasizes the role of the Chinese state as a safety provider, which helps explain the rationale behind its preference for strong government intervention. Building on Jones' argument, China's security strategy places a greater emphasis on offering "safety" as a public good, rather than solely focusing on establishing the institutional framework for security guarantees.

As such, China's approach to human security is primarily centered on the state, characterized by a fragmented and protection-oriented strategy (Zhang 2022). Through scholars' engagement with the concept of human security, China has developed sophisticated mechanisms to assimilate the idea of human security into its national security agenda (Zhang 2022). In the context of China, where the state has firmly established itself as the

guarantor of individual safety and privacy, any endeavors to uphold its ongoing commitments in this regard must be undertaken in conjunction with, rather than against, the exercise of state sovereign power (Zhang 2022).

As a byproduct of the process of Sinification, the incorporation of ideas related to human security into everyday practices equips citizens with the ideational framework to understand security on both an individual and communal level. This has contributed to an increased public awareness of privacy as a contemporary concept. This development is important because the term "privacy" (*yinsi*) is a borrowed concept, and indigenous Chinese notions associated with it carry derogatory connotations related to unspeakable immorality, indecency or shame (Ma 2008; Zhai and Li 2008; McDougall 2004). Within the cultural context in which the borrowed concept "privacy" took root, its value is diminished and met with resistance, making it challenging to establish it as a recognized and legitimate right (Ma 2008). In this context, the act of divulging others' secrets has evolved into a widely accepted social norm, while invasions of privacy, such as searching students' dormitories and implementing surveillance cameras, have become normalized (Ma 2008).

Due to the absence of a cultural foundation in China akin to where the concept of privacy originated, primarily in the West, China's regulatory framework not only bears the burden of combating illegal privacy violations but also delineating, within the realm of morality and socially accepted norm, what should be considered acceptable and what should not. A notable example is that what is considered an expression of care for other members of the collective in the Chinese context may be perceived as intrusive in the West, such as inquiring about people's age, income, marital status and political inclination (Zhai and Li 2008). The introduction of the concept of privacy has been reshaping Chinese social norms regarding what should be regarded as *yinsi*.

On the other hand, McDougall (2004) rejects ahistorical conclusions, emphasizing that the absence of a directly corresponding term for "privacy" in the English language should not lead us to dismissing the existence of indigenous concepts related to privacy throughout Chinese history. While the term *yinsi* may have different origins, the associated notion does not emerge from nothing.

In traditional Chinese culture, *yinsi* possesses a collective dimension that prioritizes public and communal interests (Zhai and Li 2008). In the Chinese context, the privacy of the collective often takes precedence over that of individuals, with everything pertaining to an individual being subordinate to the collective to varying degrees (Zhai and Li 2008). The traditional idea of "*yinsi* protection" in China reflects a collectivist and instrumentalist mindset, the purpose of which is to maintain the harmony and stability of society as a whole, in contrast to the Western emphasis on preserving individuality and human rights (Zhai and Li 2008).

Some other studies emphasize how cultural inclinations shape individuals' attitudes toward privacy. In collectivist societies, trust tends to be higher within in-groups where significant social relationships are formed, whereas in individualist societies, social relationships are not confined to specific in-groups (Hamamura 2012). The distinctions between individualist and collectivist orientations manifest in various aspects of privacy concerns. Information privacy concerns revolve around the protection of personal data and online information, while psychological privacy pertains to feeling comfortable

expressing oneself without concern about how others may judge their disclosed information (Li et al. 2022). Prior research indicates that Chinese and Koreans tend to be more concerned about psychological privacy, specifically the fear of being judged, in contrast to users in the United States, who are more inclined to express worry regarding the security of their personal information when using social media (Li et al. 2022). A 2011 study shows that Chinese users exhibited a higher level of trust in both the social network site system and its operator compared to their American counterparts (Wang, Norice, and Cranor 2011). These studies seem to suggest a distinctive cultural inclination among Chinese people in their privacy concerns.

Nevertheless, this cultural determinist approach certainly has its limitations. Some studies suggest that individuals' privacy concerns are primarily linked to the prevalence of internet usage rather than cultural distinctions such as individualism or collectivism (Engström et al. 2023). In other words, greater internet utilization is correlated with reduced levels of privacy concerns. From a Weberian perspective, the swift emergence and expansion of major technology corporations in China are bound to precipitate a heightened sense of individualism within Chinese society.

The emphasis on collectivism in Chinese culture partly explains why some citizens were willing to compromise their privacy rights during the COVID-19 pandemic. This cultural penchant is compounded by the socializing role of social media, which has cultivated more relaxed attitudes toward privacy (Tsay-Vogel et al. 2018). Despite this predisposition, the COVID-19 pandemic was a shock to Chinese society in the sense that it exacerbated the tensions between human security and state security (Zhang 2022). During the COVID-19 pandemic, China instituted a nationwide telecom data analysis platform overseen by the Ministry of Information Industry Technology (Norton Rose Fulbright 2021), which collected data even before the risks to public health and safety had been fully substantiated (Liu 2022). Nonetheless, despite individual concerns about privacy, the dissatisfaction with tracking did not result in any legal actions or lawsuits against local governments, as they retain discretionary authority to balance the interests of individuals and the collective well-being (Liu 2022). The "crisis mode" triggered by COVID-19 normalized the use of tracking technology and facial recognition.

The heightened public awareness of individual privacy prompts scholars to scrutinize the extensive use of health codes for governance, which has emboldened local governments to extend their authority into other areas, including gathering information not only on individuals' health conditions but also to monitor their behavior as responsible citizens (Zou 2023). With 900 million internet users, a thriving digital economy, and the prevalence of data theft and fraud, Chinese consumers are increasingly uneasy about unrestricted data collection by private firms (Pyo 2020). An example of this heightened awareness is the lawsuit filed by a university professor named Guo Bing, who took legal action against Hangzhou Safari Park over the use of facial recognition technology. Guo Bing accused the park of infringing upon consumer protection laws by forcibly gathering visitors' facial characteristics (BBC 2019). On 9 April 2021, this landmark case reached its long-awaited final verdict. Hangzhou Safari Park, the defendant, was mandated by the court to expunge all facial feature data collected from Guo Bing. Guo's plea against the compulsory collection of biometrics resulted in Hangzhou becoming the first city to outlaw mandatory facial recognition practices (Mo 2021).

Corroborating the growing awareness of individual privacy is the survey conducted by the Nandu Personal Information Protection Research Center, a think tank affiliated with Southern Metropolis Daily. It published the *Public Survey Report on Facial Recognition* in 2020. The findings revealed a significant sentiment among respondents, with 60% expressing concerns about the excessive use of facial recognition technology. Alarmingly, over 30% of those surveyed reported experiencing privacy breaches or property losses attributed to the unauthorized dissemination and misappropriation of their facial information (Fu 2020). Concerns have also emerged in relation to AI technologies, such as those used for self-driving, which rely on facial data for training purposes. Linking individual privacy concerns around facial data with national security, Zhang Xinbao, Director of the Information Law Center at Renmin University, argues that when essential traffic and pedestrian data is transmitted abroad, it might pose a national security risk (Economic Information Daily 2021).

The above discussions delineate the importance of the concept of human security and its relevance to the discussions concerning privacy protection in Chinese society, which is often characterized as collectivist. In this context, the concept of "privacy"differs somewhat from its Western origins (Creemers 2022). The concept of human security helps understand the different referent objects of security. Beyond the state/individual dichotomy, China's interpretation of privacy introduces an additional layer of analysis: security at the communal level. This layer of analysis could further facilitate the exploration of when individual privacy becomes a matter of national security concern.

China's approach to privacy protection

Scholars based in China often perceive individual privacy as an integral component of state sovereignty (Cao 2013; Que and Wang 2022). Data sovereignty is a key element in China's official discourse, emphasizing the Chinese government's authoritative control over data collection and the transmission of data across international borders. While cyber sovereignty primarily centers around protecting critical infrastructure and defending against cyber-attacks by foreign entities, data sovereignty is a more specific concept that revolves around asserting authority over inherently mobile and fragmented data. As Chen and Gao (Forthcoming) point out, cyber sovereignty is one of the core principles China has upheld in its approach to cyber governance both domestically and internationally. The nature of data itself often leads governments to seek physical control over it in an effort to govern it more effectively. Nevertheless, the degree to which territorialization of data might hinder innovation continues to be a topic of debate.

China's approach to privacy and data protection encompasses a combination of policy responses, legislative measures, and law enforcement (Jia 2023). The rapid and extensive process of datafication that China has undergone, which has surpassed many other countries worldwide, is a significant driver for the country's regulatory framework in this regard (Jia 2023). In 2019, the global digital economy reached a scale of $31.8 trillion US dollars, with China ranking second in the world with an economic scale of $5.2 trillion US dollars (China Industrial Control Systems Cyber Emergency Response Team and Huawei 2021). The ongoing evolution of regulatory framework development is shaped by the interplay of competing interests within the domestic business landscape and transnational interactions (Shen 2016).

The emergence of a data-driven economy is reallocating power dynamics, shifting power away from individuals toward organizations, from traditional businesses to data-driven enterprises, and from governments to data-driven businesses (OECD 2015, 18). Companies, by virtue of their data resources alone, can wield substantial influence, at times even surpassing that of governments. Indeed, one of the reasons behind Beijing's crackdown on Didi is to prevent the company from amassing a data reservoir that surpasses the state's control (Borak 2021; Kurth 2021). This concern is further revealed by the recent case of Jack Ma being stripped of his role as the actual controller of Alipay (Bloomberg News 2023).

China's regulatory framework for privacy protection is far from being a monolithic, coherent, and well-coordinated set of rules. Instead, it has evolved alongside technological innovations and key events that raised public concerns about the widespread use of technology that encroaches upon individual privacy. As a result, China's regulatory framework appears fragmented at times, with occasional overlapping responsibilities among different governmental departments. For example, since the Cyberspace Administration of China (CAC)'s establishment in 2014, it has been engaged in a continuous turf war with the Ministry of Public Security concerning critical infrastructure protection and various other issues (Lee 2021; Creemers 2022). While the Personal Information Protection Law (PIPL) was established as the main authority overseeing personal information protection, the Ministry of Public Security was involved in the punitive actions against Didi (Hu 2021).

Expanding upon the discussion on *yinsi* in the previous section, the notion of "privacy" carries a somewhat distinct connotation in China, lacking the same constitutional status linked to liberal principles of the rule of law and economic values, as seen in Europe or the US (Creemers 2022). As Creemers notes, while PIPL primarily centers on *regulating* the relationship between individuals and data controllers, the Data Security Law (DSL) places a greater emphasis on *assessing* and *managing* the risks emanating from data held in China. The former is primarily concerned with balancing domestic interests and mitigating tensions between individual rights and collective economic growth, while the latter primarily focuses on safeguarding Chinese interests against deliberate hostile threats originating from foreign sources. As domestic scam cases and deteriorating relations with the US fed into the policy-making processes on digital governance, the distinction between safeguarding personal information for individual interests and its potential significance for national security began to blur (Creemers 2022).

Bearing in mind the caveat regarding cultural determinism, it appears that the Sinicized concept of human security does indeed take on an added dimension of collectivism. In the context of privacy protection, this dimension becomes evident in the guidelines that determine the threshold at which the volume of data raises national security concerns. As clarified in the Cybersecurity Review Measures, operators in possession of personal information from over 1 million users are mandated to undergo a cybersecurity review before proceeding with their overseas initial public offering (Cyberspace Administration of China et al. 2022). The focus on determining the threshold at which individual privacy transitions into a national security concern reflects an implicit assumption that individual privacy protection can only be provided by a capable state that can safeguard its sovereign rights.

From the perspective of governance, the expansion of state power over data heightens the risk of abuse, which could in turn undermine the government's credibility. The massive amount of data collected is vulnerable to cyberattacks, and if leaked, could potentially threaten both individual privacy and national security (Zou 2023). A case in point is the Shanghai National Police Database breach, involving data from 1 billion Chinese residents, including sensitive information like ID numbers and criminal records (Goh et al. 2022; Ni 2022; Hurst 2022).

The commitment to protecting individual privacy helps the Chinese state to bolster its legitimacy in the face of widespread digital abuse (Jia 2023). This motivation is exemplified by recent efforts against telecom scams and fraudulent activities. According to the Supreme People's Procuratorate of China, during the initial ten months of 2023, procuratorates across the country have taken legal action against more than 34,000 individuals involved in telecom and online fraud cases, representing a substantial 52 percent year-on-year increase (Xinhua 2023). In response to criminal activities conducted abroad, China is actively seeking international cooperation to facilitate the extradition of fugitives. A recent case involving the repatriation of 2,349 individuals implicated in telecom fraud from Myanmar has garnered significant public attention (Global Times 2023).

Case study: Didi

The case of Didi serves as an example of the evolving power dynamics between platforms and the state, as well as the co-evolution between technological innovation and regulatory frameworks. Considering their role as holders of vast amounts of data, platforms function as techno-cultural constructs and integral components of the socioeconomic structure (Dijck, Poell, and Waal 2018). Platforms are subject to state governance while also functioning as rule-makers in their own right. Multinational platforms wield significant influence due to their ability to mediate social interactions and regulate public discourse through opaque content moderation processes (Helmond et al. 2019). Such influence compels governments to enhance their governance endeavors to adapt to the evolving challenges posed by the digital economy. Platforms are reshaping the boundaries and norms associated with the concept of freedom of expression (Afina 2023).

As such, "governance *by* platforms" and "governance *of* platforms" work together to shape the regulatory landscape. Research on the distinction between these two modes of governance highlights the increasing influence of platforms in decision-making in data governance (Gorwa 2019; Poell, Nieborg, and Duffy 2021). The vast amount of data facilitates smart city development and digital governance, but also shifts the power dynamic in favor of the authorities and capital, which hide behind algorithms to discipline the public and foster acceptance of injustice (Zhang 2023).

Didi's development trajectory along with China's evolving regulatory landscape highlights how government policies can both shape and incentivize data-driven innovation and vice versa. Established in 2012, Didi swiftly ascended to the pinnacle of the ride-sharing industry in China, solidifying its position as the largest platform in the country following its acquisition of Uber's operations in China. By the time it prepared an initial public offering in the US, Didi had extended its services to 14 countries beyond China, amassing an estimated 50 million users in overseas markets (Chen 2021).

Didi's personalized algorithms, powered by vast datasets of user behavior, pose potential challenges regarding data-driven innovation in the service industry to both individual privacy and national security. Holding an extensive repository of consumer data, Didi's operations fall under the purview of various Chinese laws and regulations, including the DSL, Cybersecurity Law, PIPL, and Cybersecurity Review Measures (*People's Daily* 2022). The concern around national security was significantly amplified when Didi chose to list on the NYSE, as this move raised concerns about the potential exposure of sensitive data collected in China to foreign entities (Wang et al. 2024).

After taking down the Didi Chuxing app, on 5 July 2021, the Chinese Cyberspace Administration announced inquiries into other companies, including Full Truck Alliance and Boss Zhipin, citing concerns regarding national data security risks (Kharpal 2021). This marks the start of the government's endeavors to regain control and reshape the power dynamics in the digital governance landscape, which had long been dominated by major technology corporations.

In July 2022, CAC announced the penalties on Didi in accordance with the Cybersecurity Law, DSL, and PIPL (*People's Daily* 2022). This breach resulted in a substantial fine of 8.026 billion yuan, surpassing even the 743 million euros fine imposed on Amazon for its GDPR violation, setting a record as the highest fine in the global history of data protection (Goh et al. 2022).

However, it is worth noting that despite the ongoing tension between state authorities and major tech companies, their relationship has not always been contentious. In the past, Didi's data collection had been used to assist the government in matters related to security governance. As of 2017, Didi had initiated collaborations with the local governments of more than 20 cities across China on smart transportation (China Net 2017). In September 2017, Didi initiated a strategic partnership with the Traffic Police of the Guangzhou Municipal Public Security Bureau. Synergizing Didi's extensive big data and analytical capabilities with the rich traffic data reservoir of the Guangzhou Traffic Police, this collaboration helps the government understand risky driving behaviors, crack down on drunk driving, and mitigate traffic congestion (China Net 2017). In 2020, Didi bolstered its collaboration with national law enforcement agencies to enhance background checks of drivers (Didi Global 2020). By August 2020, Didi had established partnerships with more than 50 local police departments to bolster crime deterrence on its platform (Didi Global 2020). As part of its Safe Driving System, Didi employs cameras for monitoring of both the road ahead and behind the vehicle while recording GPS data (Xiao 2017). Furthermore, Didi is training its AI systems to discern particular human behaviors as indicators of driver fatigue (Xiao 2017).

Besides Didi's collaboration with law enforcement in security governance, the company's practice of collecting excessive data is also driven by public concern about the drivers. In May 2018, a 21-year-old female passenger was murdered by a Didi driver, igniting intense discussions on Chinese social media platforms. In response, Didi Chuxing announced a reward of 1 million yuan to help locate the suspected driver and actively cooperated with the Ministry of Public Security to conduct background checks on the drivers employed by the platform (BBC 2018). Following the incident,

Didi implemented enhanced security measures, including a "one-click police report" feature, continuous ride recording, and mandatory driver identity verification through facial recognition (Wu 2019).

Nevertheless, there are some issues regarding these measures implemented in the name of customer safety. First, despite its name, the "one-click police report" in Didi does not directly contact the police. Instead, it sends information to an emergency contact who can then make the call (China Youth Net 2018). This is because police networks operate on a system separate from the public. The customer or their contact still needs to initiate the actual call. The act of Didi contacting the police on behalf of the customer would alter the nature of its relationship with its customers from a typical commercial relationship into that of an agent for criminal prosecution, acting on behalf of the potential victim, the legality of which remains unclear under Chinese law (China Youth Net 2018). Second, by associating the practices of ride recording and facial recognition with customer safety, these actions have become normalized despite their encroachment upon individual privacy. This normalization grants the platform significant power, which, in turn, may necessitate cooperation with law enforcement agencies in China. Third, the line between the platform and public security departments becomes blurred. It remains unclear to what extent the police can access all the data collected by Didi, and Didi's responsibility for ensuring safety has grown substantially due to its extensive data holdings.

Despite the crackdown, Didi's dominance in the Chinese market remains unshakable. In 2022, Didi further expanded its reach to cover 16 countries, including the US, India, Japan, and Australia (Wang and Xing 2023). The company also ventured into the field of autonomous driving, with the goal of achieving mass commercialization of self-driving vehicles by 2025 (Wang and Xing 2023). This implies that the Chinese government will continue to rely on and collaborate with Didi for data governance, and Didi may also have the potential to influence the international data governance landscape as the company seeks to navigate local data governance laws and regulations in its target countries.

Global implications

The governance of data carries significant global implications. According to the Organisation for Economic Co-operation and Development (OECD), "Underpinning digital trade is the movement of data. Data is not only a means of production, it is also an asset that can itself be traded, and a means through which GVCs [global value chains, *author's note*] are organised and services delivered" (OECD n.d.). Data has become intricately interwoven within global political dynamics as a key component of self-governance and indigenous sovereignty (Kukutai and Taylor 2016). A total of 86 World Trade Organization (WTO) member states engaged in discussions regarding cross-border data flows, while 78 developing countries abstained from participation due to concerns that data flows might potentially disrupt their development (Aaronson 2021, 5). Data governance conducted hastily risks evolving into another dimension of capitalist mechanisms that reinforce inequalities between the Global North and Global South.

At the outset of 2021, data privacy laws were in place in 145 countries, a number that had risen to 157 by mid-March 2022 (Greenleaf 2022). The fragmentation of data privacy laws across the globe results in overlapping sovereignty claims concerning the

control and ownership of data. Similarly, the current regulatory landscape concerning digital platforms is also complex and fragmented (Afina 2023). The competition for discourse power in data sovereignty, with cross-border data flow governance as a key element, is emerging as a central focus in future international competition (Shen 2023).

With these advancements in legal and regulatory frameworks, various interpretations of data sovereignty are being promoted and diffused (He 2021). The EU's concept of data sovereignty aligns with its strategic autonomy and human rights agenda, whereas the US places greater emphasis on harnessing the economic potential of information and communication technology companies, accommodating the data collection and algorithm training requirements of technology giants (Broeders, Cristiano, and Kaminska 2023; Que and Wang 2022). Despite differences in the normative foundations of their respective approaches to data sovereignty, both parties share a growing concern about the location of data storage due to its implications for data sovereignty (Wang et al. 2024).

As China emerges as a frontrunner in shaping norms and regulations concerning cyberspace governance, its strategies for privacy and data protection also carry global ramifications (Gao 2022a; Segal 2020). China's approach to data privacy, as exemplified by its PIPL, encompasses a broader scope compared to that of the US and EU. While the US employs a fragmented regulatory framework consisting of state and sector-specific laws, China adopts a centralized approach involving the implementation of stricter data localization requirements and the regulation of cross-border data flows. Notably, China's approach to data privacy is intertwined with its cybersecurity laws, signifying a more pronounced emphasis on national security concerns. PIPL grants the Chinese government the authority to blacklist overseas data controllers and processors, thereby enabling it to leverage its data and privacy regulations as a means of retaliating against countries seen as engaging in discriminatory practices (Lee 2021). This reflects the broader security approach of the Chinese government, which prioritizes safeguarding and controlling the data of its citizens, providing safety as a public good.

Building upon the earlier discussions of human security and *yinsi* protection, China's approach to data protection places an emphasis on data sovereignty as a fundamental prerequisite for safeguarding all other rights associated with data (Cao 2013). The Chinese state has endeavored to position itself as an intermediary between citizens and technology companies in order to address the asymmetrical power dynamics that exist between them (Cai and Wang 2020; Wang 2022).

A significant distinction exists between PIPL's clear-cut mandates for data localization and GDPR's mechanisms designed to facilitate data transfers when certain conditions are met (Lee 2021). The requirement for personal information holders to store data within China's geographical borders is a key element of China's cyber sovereignty vision (Pyo 2020). This disparity poses challenges for interoperability among different data regulatory regimes (Lee 2021). The differences between China's state-centric model of cyber governance and the decentralized model prevalent in Western countries could also potentially give rise to new alliances and divisions in the realm of global cybersecurity politics. For instance, Vietnam, embracing a "sovereign and controlled" internet model, adopts China's approach to data localization, mandating the storage of specific data types in designated locations (Sherman 2019). Similarly,

countries such as Zimbabwe, Djibouti, and Uganda are expressing apprehension regarding U.S. hegemony in cyberspace, which they perceive as yet another iteration of colonialism (Gao 2022b).

On the one hand, the EU's stringent requirements concerning data belonging to EU citizens might be perceived as a form of regulatory bullying, as it compels other countries to align themselves with EU standards in order to facilitate the exchange of personal data (Aaronson 2021). China's stringent privacy law requirements can potentially escalate existing tensions with countries that uphold different data protection standards, leading to strained trade relations.

On the other hand, China's data localization requirements mandate that transnational corporations must store data collected within the country itself. Foreign companies operating in China are obligated to adhere to data localization requirements, obtain consent for data processing, and collaborate with law enforcement authorities on matters related to data security. If a company has committed to regional voluntary agreements like Cross-Border Privacy Rules, it will be restricted from transferring personal information to countries with lower standards in personal information protection, which could potentially compel other countries to consider adopting China's standards (Hu 2021).

The localization requirements may also entail establishing local data centers or collaborating with local service providers to manage and process the collected data. The stringent security assessments required for cross-border data transfers might pose challenges for these corporations, impeding their global operations (Hu 2021). Multinational companies will be required to reconfigure their information technology systems to ensure compliance, which might involve seeking the guidance of local government before exporting data that was initially collected in China or is currently stored within China (Junck et al. 2021).

In order to adhere to these regulations, transnational corporations are compelled to invest in local infrastructure, adapt their data management protocols, and stay vigilant in keeping pace with evolving regulatory changes. This might necessitate the appointment of dedicated staff members to oversee these compliance efforts. As the regulatory framework and practices are still under development, it remains unclear whether the mandatory security assessment by the CAC for transferring data to other countries grants the company one-time approval for a data transfer or a license for a given period (Hu 2021). Collectively, these legal and regulatory barriers may lead to increased fragmentation in global business operations. After a period of tightening control over data generated in China, recent efforts to expedite approvals for foreign companies awaiting data transfer clearance offshore (Yu and Tham 2024), along with the implementation of the Regulations on Promoting and Regulating Cross-Border Data Flows (Guo, Li, and Feng 2024), signal a notable relaxation of policies aimed at alleviating clearance difficulties and facilitating operations in China.

As other countries seek to strike a balance between data-driven economic opportunities and privacy concerns, China's approach could potentially serve as a model, particularly for countries with significant economic ties to China, due to the need to comply with Chinese standards. China's model may appear attractive to governments seeking to retain substantial state control over individual privacy while

simultaneously promoting economic growth (Pyo 2020). Furthermore, the Belt and Road Initiative (BRI) might serve to promote Chinese standards and thus advance Beijing's vision of the internet within BRI countries (Sherman 2019).

Overall, while there is little concrete evidence that other countries are directly imitating China's model, there are shared aspirations to exercise a higher level of control over their citizens' data. Countries such as Thailand (Chachavalpongpun 2023), Indonesia (Hunton Andrews Kurth 2022), Myanmar (Thean-ngarm and Oo 2023), and Vietnam (Aw 2023) are introducing stricter laws and regulations in order to exert greater control over their cyberspace. A similar effort toward data localization can be observed in Cambodia's draft data protection law (Kelliher 2023) and in Kazakhstan (Marina Kahiani and Abdukhalykova 2023), as well as in Russia (Andreeva, Kiseleva, and Neskoromyuk 2021). This signifies that countries are reshaping geopolitical faut lines as a result of shared concerns regarding data localization.

Conclusion

This paper offered an analytical perspective to understand the concept of *yinsi* and the intricate relationship between the individual, the community, and the state within the discourse of security and data privacy. Drawing a novel theoretical approach building on the Sinicized concept of human security and the indigenous concept of *yinsi*, this paper argues that China's regulatory framework for privacy protection has evolved alongside technological innovations and key events that raised public concerns about the widespread use of technology that encroaches upon individual privacy.

Given that it is still in the early stages of development, China's regulatory framework sometimes appears fragmented, with overlapping responsibilities among various government departments. Due to its emphasis on state sovereignty over individual privacy, China's approach to privacy protection tends to downplay the perspective that societies could benefit from the use, sharing, and transfer of large quantities of data.

This paper complements Chen and Gao's (Forthcoming) observation regarding a shift in China's official narratives on cyber governance concerning the transition from a primary focus on national security to an increased emphasis on the protection of digital infrastructure and the control over data flows. This paper further demonstrates that this shift has incentivized the Chinese government to regulate cross-border data flows, especially when such flows involve the data of a significant number of users.

China's approach to privacy protection carries several global implications. Firstly, it presents challenges for multinational corporations engaged in global operations, as they must incur increased operational costs to ensure compliance. The state control over the movement of data may contribute to the fragmentation of digital businesses and slow down global digital trade. Secondly, it exacerbates preexisting geopolitical tensions with other major rule-making powers such as the US and EU, as their differing normative expectations become evident in their respective approaches. Thirdly, as other countries endeavor to strike a balance between data-driven economic opportunities and privacy concerns, China's approach may be seen as a potential model for governments looking to maintain significant state control over data.

Author's contributions
Chi Zhang is the sole contributor to this work.

Declarations

Competing interests
I am one of the Guest Editors of the special issue 'Nexus Between Digital Trade and Security: Geopolitical Implications for Global Economy in the Digital Age' in this journal. Other than this, I declare no conflicts of interest related to the research presented in this paper. This includes financial, personal, or professional affiliations that could potentially influence the study's integrity or outcomes. This research does not receive funding from any external sources, and it does not require ethical approval.

Received: 25 January 2024 Accepted: 6 May 2024
Published online: 28 May 2024

References

Aaronson, Susan Ariel. 2021. Data Is Disruptive: How Data Sovereignty Is Challenging Data Governance. Hinrich Foundation. https://www.hinrichfoundation.com/research/article/digital/data-is-disruptive-how-data-sovereignty-is-challenging-data-governance/.

Afina, Yasmin. 2023. Digital Platform Regulation: Governing the Ungovernable. Chatham House – International Affairs Think Tank. 24 Feb 2023. https://www.chathamhouse.org/2023/02/digital-platform-regulation-governing-ungovernable.

Andreeva, Ksenia, Anastasia Kiseleva, and Alena Neskoromyuk. 2021. Data Localization Laws: Russian Federation. Morgan Lewis.

Aw, Charmian. 2023. Vietnam Issues Much-Awaited Landmark Data Protection Law. Privacy World. 18 Apr 2023. https://www.privacyworld.blog/2023/04/vietnam-issues-much-awaited-landmark-data-protection-law/.

BBC. 2018. Three Controversies Surrounding the Didi Driver Murder Case [*Didi siji sharen an beihou de sange zhengyi xuanwo*]. BBC News. 12 May 2018. https://www.bbc.com/zhongwen/trad/chinese-news-44093798.

BBC. 2019. China Facial Recognition: Law Professor Sues Wildlife Park. *BBC News*, 8 November 2019, sec. China. https://www.bbc.com/news/world-asia-china-50324342.

Bi, Lei. 2021. The First Mention of "National Core Data": The "Data Security Law" Defines the Basic "Red Line" of Data Security Risks [*Shouti guojia hexin shuju shuju anquan fa heading shuju anquan fengxian jiben hongxian*]. 24 June 2021. http://finance.people.com.cn/n1/2021/0624/c1004-32139926.html.

Bloomberg News. 2023. Ant Completes Process of Removing Jack Ma's Control. *Bloomberg.Com*, 30 Dec 2023. https://www.bloomberg.com/news/articles/2023-12-30/ant-completes-process-of-removing-billionaire-jack-ma-s-control.

Borak, Masha. 2021. What Does Didi's Probe Mean for the Industry and China's Tech Giants? South China Morning Post. 5 Jul 2021. https://www.scmp.com/tech/big-tech/article/3139888/why-didis-cybersecurity-review-important-and-what-will-it-mean-ride.

Breslin, Shaun. 2015. Debating Human Security in China: Towards Discursive Power? *Journal of Contemporary Asia* 45 (2): 243–265. https://doi.org/10.1080/00472336.2014.907926.

Broeders, Dennis, Fabio Cristiano, and Monica Kaminska. 2023. In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions. *JCMS: Journal of Common Market Studies* n/a (n/a). https://doi.org/10.1111/jcms.13462.

Cai, Cuihong, and Yuanzhi Wang. 2020. Global Data Governance; Challenges and Responses [*Anquan shuju zhili: Tiaozhan yu yingdui*]. *International Studies* 6: 38–56.

Cao, Lei. 2013. Analysis of Data Rights in Cyberspace [*Wangluo kongjian de shuju quan yanjiu*]. *International Review* 1: 53–58.

Chachavalpongpun, Pavin. 2023. Nationhood in the Cloud: Cyber Sovereignty in Thailand. *Asian Studies Review* 47 (2): 392–411. https://doi.org/10.1080/10357823.2022.2109591.

Chen, Xuechen, and Xinchuchu Gao. Forthcoming. Norm Diffusion in Cyber Governance: China as an Emerging Norm Entrepreneur? *International Affairs*.

Chen, Caiwei. 2021. Didi, Grab, and the Future of Asia's Ride-Hailing Giants. KrASIA. 19 May 2021. https://kr-asia.com/didi-grab-and-the-future-of-asias-ride-hailing-giants.

China Industrial Control Systems Cyber Emergency Response Team and Huawei. 2021. Data Security White Paper [*Shuju anquan baipi shu*].

China Youth Net. 2018. Public Security Expert Weighs In: Didi's "One-Click Alarm" Implementation Is More Complex Than It Appears [*Gong'an zhuanjia: didi shixian yijian baojing bingfei name jiandan*]. Huanqiu. 20 September 2018. https://www.huanqiu.com/article/9CaKrnKcQb6.

Creemers, Rogier. 2022. China's Emerging Data Protection Framework. *Journal of Cybersecurity* 8 (1): tyac011. https://doi.org/10.1093/cybsec/tyac011.

China Net. 2017. Guangzhou Traffic Police and Didi Chuxing Forge Strategic Partnership for Joint Advancement in Smart Transportation [*Guangzhou jiaojing yu didi chuxing dacheng zhanlue hezuo gongjian zhihui jiaotong*]. Huanqiu. 12 September 2017. https://www.huanqiu.com/article/9CaKrnK59R4.

Cyberspace Administration of China, National Development and Reform Commission, Ministry of Industry and Information Technology, Ministry of Public Security, Ministry of National Security, Ministry of Finance, Ministry of Commerce, et al. 2022. Cybersecurity Review Measures [*Wangluo anquan shencha banfa*]. http://www.gov.cn/zhengce/zhengceku/2022-01/04/content_5666430.htm.

Dijck, José van, Thomas Poell, and Martijn de Waal. 2018. *The Platform Society: Public Values in a Connective World*. Oxford University Press.
Didi Global. 2020. Didi Security Report 7: Strengthening Police-Enterprise Collaboration and Pioneering Innovative Cooperative Models [*Didi anquan fabu diqi qi: chixu Shenhua jingqi hezuo, tansuo gengduo chuangxin liandong moshi*]. 25 Sept 2020. https://www.didiglobal.com/news/newsDetail?id=967&type=blog.
Engström, Emma, Kimmo Eriksson, Marie Björnstjerna, and Pontus Strimling. 2023. Global Variations in Online Privacy Concerns across 57 Countries. *Computers in Human Behavior Reports* 9 (March): 100268. https://doi.org/10.1016/j.chbr.2023.100268.
Economic Information Daily. 2021. Hidden Camera Concerns: Facial Recognition Raises Security Risks - Is Your Face Secure [*Shexiangtou cang maoni renlian xinxi anquan chudong gongzhong mingan shenjing*]. 12 Jul 2021. https://www.chinacourt.org/article/detail/2021/07/id/6144470.shtml.
Fu, Lili. 2020. Release of 2020 Public Survey Report on Facial Recognition Applications: 60% of Respondents Express Concerns About Potential Abuse of Facial Recognition Technology [*Renlian shibie yingyong gongzhong diaoyan baogao (2020) chulu liucheng shoufangzhe renwei renlian shibie jishu you lanyong qushi*]. 19 Oct 2020. http://ha.people.com.cn/n2/2020/1019/c351638-34357546.html.
Global Times. 2023. 2,349 Chinese Suspects of Telecom Scam Handed over to China, Marking the Largest Single Transfer since Launch of Crackdown Campaign. 16 Oct 2023. https://www.globaltimes.cn/page/202310/1299934.shtml.
Gao, Xinchuchu. 2022a. An Attractive Alternative? China's Approach to Cyber Governance and Its Implications for the Western Model. *The International Spectator* 57 (3): 15–30. https://doi.org/10.1080/03932729.2022.2074710.
Gao, Xinchuchu. 2022b. Sovereignty and Cyberspace: China's Ambition to Shape Cyber Norms. *China Dialogues* (blog). 18 Aug 2022. https://blogs.lse.ac.uk/cff/2022/08/18/sovereignty-and-cyberspace-chinas-ambition-to-shape-cyber-norms/.
Goh, Brenda, Sophie Yu, Stella Qiu, and Eduardo Baptista. 2022. Hacker Claims to Have Stolen 1 Bln Records of Chinese Citizens from Police. *Reuters*, July 2022. https://www.reuters.com/world/china/hacker-claims-have-stolen-1-bln-records-chinese-citizens-police-2022-07-04/.
Gorwa, Robert. 2019. What Is Platform Governance? *Information, Communication & Society* 22 (6): 854–871. https://doi.org/10.1080/1369118X.2019.1573914.
Greenleaf, Graham. 2022. Now 157 Countries: Twelve Data Privacy Laws in 2021/22'. 176 Privacy Laws & Business International Report 1. Rochester, NY: UNSW Law Research. https://papers.ssrn.com/abstract=4137418.
Guo, Bingna, Bob Li, and Xue Feng. 2024. China Released New Regulations to Ease Requirements for Outbound Cross-Border Data Transfers. White & Case LLP. 2 April 2024. https://www.whitecase.com/insight-alert/china-released-new-regulations-ease-requirements-outbound-cross-border-data-transfers.
Hamamura, Takeshi. 2012. Are Cultures Becoming Individualistic? A Cross-Temporal Comparison of Individualism-Collectivism in the United States and Japan. *Personality and Social Psychology Review* 16 (1): 3–24. https://doi.org/10.1177/1088868311411587.
Helmond, Anne, David B. Nieborg, and Fernando N. van der Vlist. 2019. Facebook's Evolution: Development of a Platform-as-Infrastructure. *Internet Histories* 3 (2): 123–146. https://doi.org/10.1080/24701475.2019.1593667.
Hu, Yiming "Ben". 2021. China's Personal Information Protection Law and Its Global Impact. 31 Aug 2021. https://thediplomat.com/2021/08/chinas-personal-information-protection-law-and-its-global-impact/.
Hurst, Luke. 2022. Shanghai Data Leak: China Censors Searches after Claim That Data of 1 Billion People Was Hacked. *Euronews.Next*, July 2022. https://www.euronews.com/next/2022/07/06/shanghai-data-leak-china-censors-searches-after-claim-that-data-of-1-billion-people-was-ha.
Jia, Mark. 2023. *Authoritarian Privacy*. Rochester, NY: SSRN Scholarly Paper. https://doi.org/10.2139/ssrn.4362527.
Jones, Catherine. 2022. (Ir)Responsible Centrality? External Representations of China's COVID-19 Diplomacy. In *Human Security in China: A Post-Pandemic State*, ed. Chi Zhang, 27–46. Singapore: Springer. https://doi.org/10.1007/978-981-16-4675-1_8.
Junck, Ryan D., Bradley A. Klein, Akira Kumaki, Ken D. Kumayama, Steve Kwok, Stuart D. Levi, James S. Talbot, Eve-Christie Vermynck, and Siyu Zhang. 2021. China's New Data Security and Personal Information Protection Laws: What They Mean for Multinational Companies. 3 November 2021. https://www.skadden.com/insights/publications/2021/11/chinas-new-data-security-and-personal-information-protection-laws.
Kahiani, Marina, and Lola Abdukhalykova. 2023. Kazakhstan - Data Protection Overview. DataGuidance. 4 Aug 2023. https://www.dataguidance.com/notes/kazakhstan-data-protection-overview.
Kelliher, Fiona. 2023. Cambodia's Draft Data Protection Law Fans Fears of Government Abuse. Nikkei Asia. 8 December 2023. https://asia.nikkei.com/Politics/Cambodia-s-draft-data-protection-law-fans-fears-of-government-abuse.
Kharpal, Arjun. 2021. After Crackdown on Didi, China Opens Cybersecurity Probes into 3 More Tech Firms. CNBC. 5 July 2021. https://www.cnbc.com/2021/07/05/china-opens-cybersecurity-probe-into-full-truck-alliance-boss-zhipin.html.
Kukutai, Tahu, and John Taylor, eds. 2016. *Indigenous Data Sovereignty: Toward an Agenda*. Research Monograph 38. Canberra: ANU Press. https://doi.org/10.22459/CAEPR38.11.2016
Kurth, Hunton Andrews. 2021. China Issues Data Security Law. 16 June 2021. https://www.natlawreview.com/article/china-issues-data-security-law.
Kurth, Hunton Andrews. 2022. Indonesia Ratifies Country's First Comprehensive Legal Framework for Personal Data Protection. Privacy & Information Security Law Blog. 8 November 2022. https://www.huntonprivacyblog.com/2022/11/08/indonesia-ratifies-countrys-first-comprehensive-legal-framework-for-personal-data-protection/.
Lee, Alexa. 2021. Personal Data, Global Effects: China's Draft Privacy Law in the International Context. New America. 4 Jan 2021. http://newamerica.org/cybersecurity-initiative/digichina/blog/personal-data-global-effects-chinas-draft-privacy-law-in-the-international-context/.
Li, Yao, Eugenia Ha Rim. Rho, and Alfred Kobsa. 2022. Cultural Differences in the Effects of Contextual Factors and Privacy Concerns on Users' Privacy Decision on Social Networking Sites. *Behaviour & Information Technology* 41 (3): 655–677. https://doi.org/10.1080/0144929X.2020.1831608.

Liu, Jia. 2022. Health Security and Public Health Emergency Management in China. In *Human Security in China: A Post-Pandemic State*, ed. Chi Zhang, 175–98. Singapore: Springer. https://doi.org/10.1007/978-981-16-4675-1_8.
Ma, Te. 2008. Semantic Study and Legal Interpretation of Privacy [*Yinsi yuyi kaoju ji falü quanshi*]. *Seeker* 5: 131–133.
Mao, Xinjuan, and Jiayan Ren. 2023. Study on Data Sovereignty Security in China from the Perspective of National Security [*Guojia anquan shiyu Zhong woguo shuju zhuquan anquan mianlin de tiaozhan jiqi duice*]. *Social Governance Review* 1: 41–51.
McDougall, Bonnie S. 2004. Privacy in Modern China. *History Compass* 2 (1): 1–8. https://doi.org/10.1111/j.1478-0542.2004.00097.x.
Mo, Yichen. 2021. People's Daily Online Commentary: The Significance of the Final Verdict in the 'First Facial Recognition Case [*Renmin wangping: renlian shibie diyi an zhongshen panjue yiyi feifan*]]. People.Cn. 10 Apr 2021. http://opinion.people.com.cn/n1/2021/0410/c223228-32074599.html.
Newman, Edward. 2016. Human Security: Reconciling Critical Aspirations with Political 'realities.' *British Journal of Criminology* 56 (6): 1165–1183.
Ni, Vincent. 2022. Hacker Claims to Have Obtained Data on 1 Billion Chinese Citizens. *The Guardian*, 4 Jul 2022, sec. Technology. https://www.theguardian.com/technology/2022/jul/04/hacker-claims-access-data-billion-chinese-citizens.
Norton Rose Fulbright. 2021. Contact Tracing Apps: A New World for Data Privacy. 2021. https://www.nortonrosefulbright.com/en-cn/knowledge/publications/d7a9a296/contact-tracing-apps-a-new-world-for-data-privacy#China.
OECD. 2015. Data-Driven Innovation: Big Data for Growth and Well-Being. 6 October 2015. https://www.oecd.org/sti/data-driven-innovation-9789264229358-en.htm.
OECD. n.d. Digital Trade. Accessed 5 Jan 2024. https://www.oecd.org/trade/topics/digital-trade/.
People's Daily. 2022. Cyberspace Administration of China: Didi Engaged in Data Processing Activities with Serious National Security Implications [*Guojia wangxin ban: didi cuncai yanzhong yingxiang guojia anquan de shuju chuli huodong*]. 21 Jul 2022. http://finance.people.com.cn/n1/2022/0721/c1004-32482059.html.
Poell, Thomas, David B. Nieborg, and Brooke Erin Duffy. 2021. *Platforms and Cultural Production*. Wiley. https://www.wiley.com/en-gb/Platforms+and+Cultural+Production-p-9781509540501.
Pyo, Grace. 2020. The China Model for Privacy Rights? Examining China's Draft Laws on Data Security and Protection. Columbia Journal of Transnational Law. 3 December 2020. https://www.jtl.columbia.edu/bulletin-blog/the-china-model-for-privacy-rights-examining-chinas-draft-data-security-and-personal-data-protection-laws.
Que, Tianshu, and Ziyue Wang. 2022. Global Data Security Governance and Action Strategies for China's Participation in the Era of Digital Economy [*Shuzi jingji shidai de quanqiu shuju anquan zhili yu zhongguo celue*]. *Journal of International Security Studies* 1: 130–154.
Segal, Adam. 2020. China's Alternative Cyber Governance Regime. Council on Foreign Relations. https://www.uscc.gov/sites/default/files/testimonies/March%2013%20Hearing_Panel%203_Adam%20Segal%20CFR.pdf.
Shen, Hong. 2016. China and Global Internet Governance: Toward an Alternative Analytical Framework. *Chinese Journal of Communication* 9 (3): 304–324. https://doi.org/10.1080/17544750.2016.1206028.
Shen, Chuannian. 2023. Research on the Progress of Cross-Border Data Flow Governance [*Kuajing shuju liudong zhili jinzhan yanjiu*]. *Journal of Information Security Research* 7. https://h5.drcnet.com.cn/docview.aspx?version=emerging&docid=7013356&leafid=18532&chnid=4800.
Sherman, Justin. 2019. Vietnam's Internet Control: Following in China's Footsteps? The Diplomat. 11 December 2019. https://thediplomat.com/2019/12/vietnams-internet-control-following-in-chinas-footsteps/.
Thean-ngarm, Yuwadee, and Nwe Oo. 2023. Myanmar - Data Protection Overview. DataGuidance. 31 Aug 2023. https://www.dataguidance.com/notes/myanmar-data-protection-overview.
Treasury Board of Canada Government of Canada. 2006. Frequently Asked Questions: USA PATRIOT ACT Comprehensive Assessment Results. 28 Mar 2006. https://www.tbs-sct.canada.ca/pubs_pol/gospubs/tbm_128/usapa/faq-eng.asp.
Tsay-Vogel, Mina, James Shanahan, and Nancy Signorielli. 2018. Social Media Cultivating Perceptions of Privacy: A 5-Year Analysis of Privacy Attitudes and Self-Disclosure Behaviors among Facebook Users. *New Media & Society* 20 (1): 141–161. https://doi.org/10.1177/1461444816660731.
Wang, Xixin. 2022. The Bundle of Personal Information Rights from the Perspective of State Protection. *Social Sciences in China* 43 (2): 36–54. https://doi.org/10.1080/02529203.2022.2093062.
Wang, Ruoxi, Chi Zhang, and Yaxiong Lei. 2024. Justifying a Privacy Guardian in Discourse and Behavior: China's Strategic Framing in Data Governance. *The International Spectator*. https://doi.org/10.1080/03932729.2024.2315064.
Wang, Yang, Gregory Norice, and Lorrie Faith Cranor. 2011. Who Is Concerned about What? A Study of American, Chinese and Indian Users' Privacy Concerns on Social Network Sites. In *Trust and Trustworthy Computing*, ed. Jonathan M. McCune, Boris Balacheff, Adrian Perrig, Ahmad-Reza. Sadeghi, Angela Sasse, and Yolanta Beres, 146–53. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-642-21599-5_11.
Wang, Zhisheng, and Yiran Xing. 2023. A Glimpse Into the Future - From Didi's 1st Annual Report After Delisting. EqualOcean. 26 Jul 2023. https://equalocean.com/analysis/2023072619966.
Wu, Xinfan. 2019. Is Online Car-Hailing Safer with "One-Click Police Report" and "Shared Itinerary" as Standard Features? [*Yijian baojing fenxiang xingcheng cheng biaopei wangyue che geng anquan le ma?*]. 18 Nov 2019. http://m.xinhuanet.com/hn/2019-11/18/c_1125243645.htm.
Xiao, Eva. 2017. Didi's Master Plan to Win over Local Chinese Governments – with Data. Tech in Asia. 29 Apr 2017. https://www.techinasia.com/didi-big-data-traffic-platform.
Xinhua. 2023. Chinese Procuratorates Intensify Crackdown on Telecom, Online Fraud. 30 Nov 2023. https://www.chinadaily.com.cn/a/202311/30/WS65684892a31090682a5f0cdc.html.
Yu, Xie, and Engen Tham. 2024. Exclusive: Shanghai to Allow Faster Data Transfer from China for Foreign Firms-Sources. *Reuters*, 7 February 2024, sec. China. https://www.reuters.com/world/china/shanghai-allow-faster-data-transfer-china-foreign-firms-sources-2024-02-07/.
Zhai, Shilei, and Hao Li. 2008. Comparison of the Concept of "Privacy" between China Nad the Wesr under Globalization [*Quanqiuhua Beijing xia de zhongxi fang yinsi zhi bijiao*]. *Journal of Hebei Polytechnic University (social Science Edition)* 4 (March): 111–114. https://doi.org/10.3969/j.issn.2095-2708.2008.01.030.

Zhang, Chi. 2022. Introduction. In *Human Security in China: A Post-Pandemic State*, ed. Chi Zhang, 1–26. Singapore: Springer. https://doi.org/10.1007/978-981-16-4675-1_8.
Zhang, Fuli. 2023. Smart Governance or Digital Discipline? - How Smart Cities Dissolve Anonymity [*Zhihui zhili yihuo shuzi guixun? zhihui chengshi ruhe xiaojie nimingxing*]. *Ningxia Social Sciences* 1: 150–158.
Zou, Wenbo. 2023. Behind the Exit of Health Codes: Data Security Issues in the Post-Pandemic Era [*Jiankangma tuichang de beihou: hou yiqing shidai mianlin de shuju anquan wenti*]. *Contemporary Economics* 40 (9).

Publisher's Note

Chi Zhang Chi Zhang is an Associate Lecturer at the University of St Andrews, and an Associate Member of the Handa Centre for the Study of Terrorism and Political Violence. She has published in the journals such as the ***Journal of Contemporary China***, ***International Feminist Journal of Politics***, ***Terrorism and Political Violence***, ***Studies in Conflict and Terrorism***, ***Politics and Religion*** and ***Asian Security***. She is the editor of ***Human Security in China: A Post-Pandemic State*** and the author of ***Legitimacy of China's Counter-Terrorism Approach: The Mass Line Ethos***