The International Spectator

Italian Journal of International Affairs

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/rspe20

Justifying a Privacy Guardian in Discourse and Behaviour: The People's Republic of China's Strategic Framing in Data Governance

Ruoxi Wang, Chi Zhang & Yaxiong Lei

To cite this article: Ruoxi Wang, Chi Zhang & Yaxiong Lei (19 Feb 2024): Justifying a Privacy Guardian in Discourse and Behaviour: The People's Republic of China's Strategic Framing in Data Governance, The International Spectator, DOI: 10.1080/03932729.2024.2315064

To link to this article: https://doi.org/10.1080/03932729.2024.2315064

Published online: 19 Feb 2024.

THE INTERNATIONAL SPECTATOR
https://doi.org/10.1080/03932729.2024.2315064

RESEARCH ARTICLE

OPEN ACCESS Check for updates

Justifying a Privacy Guardian in Discourse and Behaviour: The People's Republic of China's Strategic Framing in Data Governance

Ruoxi Wang, Chi Zhang and Yaxiong Lei

University of St. Andrews

ABSTRACT

The People's Republic of China's (PRC) approach to data governance, centred on data sovereignty, is much debated in academic literature. However, it remains unclear how the PRC's different state actors justify this approach. Based on an analysis of the discourse and behaviour of the PRC's state actors through strategic framing theory, their role as a privacy guardian can arguably be described as strategically constructed. The Chinese government and legislative bodies have tailored their communications to present themselves as champions of individual privacy, aiming to secure support for state policies. This strategic framing encompasses four mechanisms: the reframing of privacy threats through political narratives; legal ambiguities; selective framing; and the implementation of censorship to influence public discourse. An examination of how the Chinese government responded differently to data breaches in the cases of Didi and the Shanghai National Police Database leak highlights the Chinese government's efforts in maintaining framing consistency to construct itself as a guardian, rather than a violator, of individual privacy.

KEYWORDS

data sovereignty; cyberspace governance; strategic framing; privacy; security

The People's Republic of China's (PRC) approach to data governance has recently become a topic of public debate, as the country has increasingly institutionalised legal and policy tools to regulate the collection and flow of data. A key concept in the PRC's approach is 'data sovereignty' (*shuju zhuquan*数据主权) (Kokas 2022; Cai and Wang 2020; Barrinha and Christou 2022; Que and Wang 2022; Borgogno and Savini Zangrandi 2023). It involves "the control of data flows via national jurisdiction" (Hummel *et al.* 2021, 2). Despite considerable debate surrounding the PRC's stance on data sovereignty and cyber governance (for example, see Gao and Chen 2022; Gao 2022), the justification provided by the Chinese government for its approach to data sovereignty warrants deeper scholarly examination. In the PRC, the concept of data sovereignty is employed as a means for the state to assert its exclusive jurisdiction

CONTACT Chi Zhang cz38@st-andrews.ac.uk

over data collection and cross-border data flow. When it comes to striking a balance between safeguarding national security and protecting individual privacy in data sovereignty practices, some scholars within the PRC tend to view individual privacy as an integral component of state sovereignty. In other words, the protection of individual privacy aligns with the broader objectives of defending national security and ensuring regime stability.

This is particularly important to understanding the PRC's approach to global governance, especially considering the mobile nature of data, which may have implications for the international landscape of data governance. Numerous state actors are increasingly promoting the concept of data sovereignty, each with their own unique interpretations and practices (He 2021). The PRC's approach to data sovereignty diverges from that of the European Union (EU) and the United States (US). The EU places a stronger emphasis on safeguarding consumers rights (Moerel and Timmers 2021), considering data sovereignty as a key element within its strategic autonomy and human rights agenda, wherein data sovereignty revolves around the EU's control of its citizens' data (Broeders *et al.* 2023). On the other hand, the US prioritises the economic potential of Information and Communications Technology (ICT) companies, accommodating the data collection and algorithm training needs of technology players (Que and Wang 2022). Despite this subtle distinction, both the US and EU are attentive to the location of data storage and its ramifications for data sovereignty. For instance, the 2018 Clarifying Lawful Overseas Use of Data (CLOUD) Act, enables the US government to request data stored on servers belonging to US-based technology companies, regardless of the servers' physical locations. This provision comes into conflict with the EU's General Data Protection Regulation (GDPR) Article 48, which restricts foreign courts' requests for access to personal data collected within the EU (Wood and Lewis 2023).

The PRC's approach carries global implications, as it is progressively asserting itself as a leader in setting norms and regulations within the realm of cyberspace (Gao 2022, 15; Segal 2020). In the PRC's perspective on data sovereignty, national security and regime stability take precedence. Chinese scholar Cao Jun (2013) contends that data sovereignty serves as a fundamental prerequisite for any other rights related to data. Scholars have also helped portray the Chinese government as a guardian of individual privacy rights who would protect individuals from the mishandling of data collection and algorithm training by technology companies (Cai and Wang 2020, 52-3). Others depict the state's role as that of a mediator that intervenes between citizens and technology companies to rectify the asymmetrical power dynamic between them (Wang 2022).

How do the Chinese government and legislative bodies justify their role as a privacy guardian instead of a violator, which is one of the key prerequisites of legitimating strong state control over data flow? Furthermore, how does the Chinese government overcome the disparity between its discourse and behaviour to construct a coherent image as a guardian of privacy? Using strategic framing as an analytical tool, we argue that the PRC's regulatory authorities have strategically framed the state's role in data governance, selectively emphasising certain data breaches while downplaying others. We also compare how the Chinese government responded differently to the data breaches in the cases of Didi and the Shanghai National Police Database. The disproportionate penalties and conspicuous silence in the latter demonstrate the Chinese government's efforts to maintain framing consistency in constructing itself as a guardian, rather than a violator, of individual privacy.

The PRC's approach to data governance

For the purpose of this article, we draw a distinction between cyber sovereignty and data sovereignty. The concept of cyber sovereignty holds greater significance in terms of national security, particularly concerning the protection of critical infrastructure and networks against deliberate cyber attacks by foreign actors. The PRC's approach in this regard was first introduced in its 2016 Cybersecurity Law, emphasising the state's capacity to defend itself against cyberattacks originating from foreign entities. Subsequent discussions on data sovereignty emerged with a more specific focus on state control over cross-border data flow, encompassing the participation of companies, organisations and the daily online activities of citizens (Hang and Zhou 2022).

Data comprises sets of symbols used by computer systems and is a fundamental by-product of the internet (O'Hara *et al.* 2021). When data is endowed with social significance and meaning, it transforms into information. Data is inherently mobile and divisive, which poses challenges in pinpointing specific territorial locations. The locations of users, data collectors and data infrastructures may vary, collectively presenting challenges to territorial jurisdictions. This diversity has prompted different states and state actors to develop various approaches to territorialise data. In this regard, the PRC's approach to data sovereignty is not markedly distinct from the 'Western' approach, as exemplified by the CLOUD Act and GDPR, both of which aim to establish territorial control over data. Nonetheless, the PRC places a significant emphasis on data sovereignty, primarily linked to national security, in contrast to the EU's prioritisation of privacy protection and the US's inclination towards technological advancement (Priol and Vincent-Galtie 2022, 4)

The party-state manages data governance through a combination of policy responsiveness, legislative measures and law enforcement (Jia 2023). It is worth noting that, while national security remains a top priority, Chinese regulators struggled to strike a balance among competing interests, including those related to economic development. The PRC's policy formulation process is the result of interactions among various state agencies and corporate entities; its approach has been shaped by the interplay of competing interests within the domestic business landscape and interactions between businesses in both domestic and transnational contexts (Shen 2016).

The tensions stemming from the competing needs of safeguarding national security, fostering economic development and ensuring individual privacy protection become apparent in conflicting priorities within different laws. For instance, the 2021 Personal Information Protection Law (PIPL) prohibits the illegal collection, use, processing, or transfer of personal information, while the 2021 Data Security Law (DSL) encourages "reasonable" and "effective" use of data to develop the digital economy (*Xinhua* 2021). Given the legal ambiguities in the PRC, this could result in labelling the same circumstances as either illegal or reasonable, depending on the specific context. Furthermore, although privacy protection has traditionally been associated with democratic practices, autocracies are increasingly embracing the rhetoric of privacy protection to bolster their legitimacy in the face of widespread digital abuse (Jia 2023).

These tensions underscore a crucial gap in understanding the disparity between the PRC's official stance and its practices in specific contexts. This article endeavours to bridge this gap through a two-fold approach. Firstly, at the discursive level, it scrutinises how the PRC's different state actors have framed the state's role as the guardians of

privacy. Secondly, at the behavioural level, it analyses when and how the state intervenes in data breach incidents. The strategic framing in terms of discourse and varying responses to different cases in terms of practice collectively function to construct a cohesive image of the Chinese state as a guardian of privacy protection.

Methodology and theoretical framework

We use strategic framing as an analytical lens to examine the PRC's discourse and behaviour, and to understand how Beijing justifies its approach to data sovereignty, particularly the strong state control over data flows. This article adopts a combination of qualitative text analysis and comparative case studies to understand the relationship between discourse and behaviour. At the discursive level, we use document analysis of the PRC's legislative regulations and official statements on data governance from 2016 to mid-2023. This timeframe covers the inception of the PRC's publication of cyber-related legislation, including the Cybersecurity Law and its subsequent policies and legislation (see Figure 1),

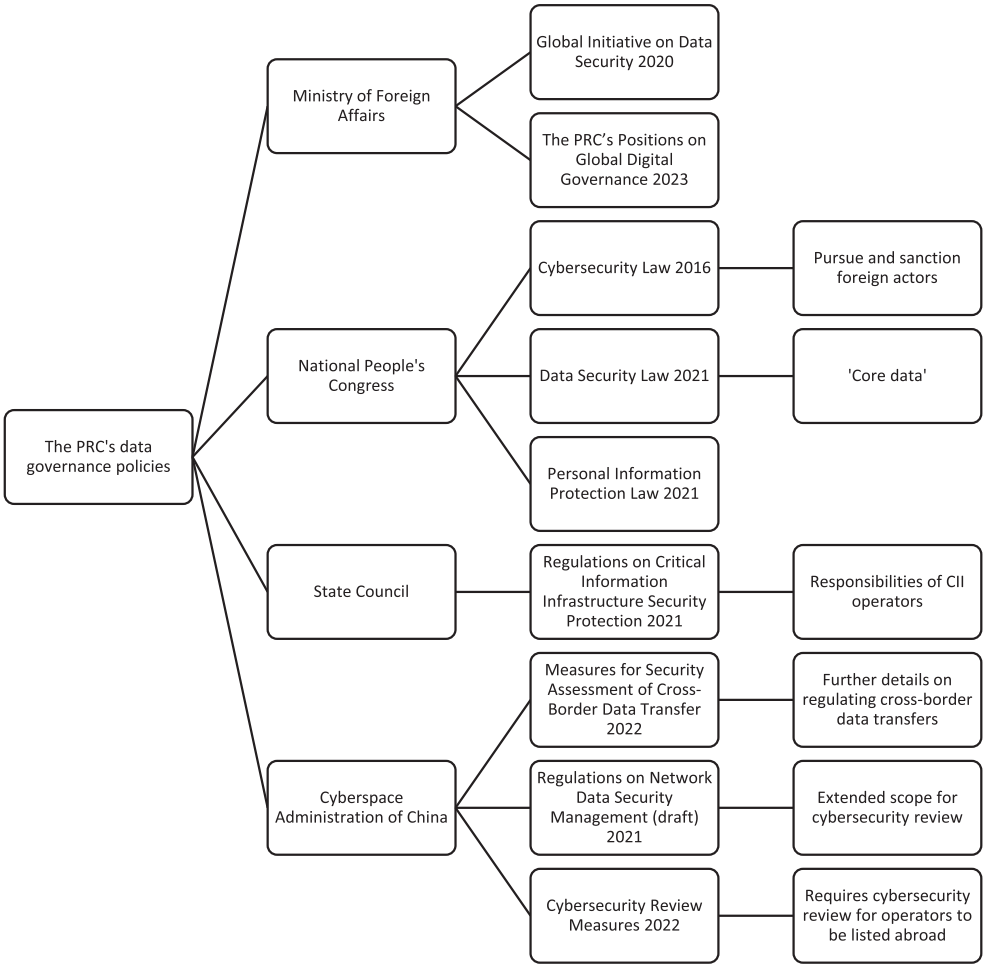

Figure 1. The PRC's data governance legislation and policies.

and provides a contemporary lens for analysis. At the behavioural level, we use comparative case studies of two major data breach incidents in 2022 to show how the Chinese government used strategic framing to construct its image as privacy guardian, instead of violator, by attempting to align its actions with its rhetorical commitments.

Strategic framing

We employed Rodger Payne's (2001) strategic framing as an analytical lens to better understand how the PRC justifies its approach to data sovereignty. Frames play a pivotal role as cognitive tools, allowing individuals or groups to organise their experiences and provide guidance for their actions (Snow *et al.* 1986). They achieve this by offering a structured set of assumptions through which events and information can be comprehended and interpreted. This can be likened to picture frames, where specific frames emphasise particular aspects of the pictures they enclose (Kuypers 2009). Through the act of framing issues in specific ways, individuals can ascribe meaning and significance to their experiences, thereby influencing their subsequent decisions and behaviours. By highlighting certain elements over others, frames enable people to filter their perceptions in particular ways (Ibid).

As such, framing serves as a discursive tactic used to "name, interpret, and dramatize issues", thereby shaping broader social meanings and providing justifications for specific actions or policies (Payne 2001, 43). Framing gives meaning to facts that may otherwise lack intrinsic significance by placing them within a framework that organises and imparts coherence, selecting specific elements while disregarding others (Gamson 1989). Therefore, framing is persuasive as it allows certain actors to alter the pre-existing beliefs of others (Finnemore and Sikkink 1998). Consequently, framing is a crucial discursive tool for building norms and constructing normative relations (Acharya 2004).

However, as Payne (2001) highlights, framing is not always employed by actors following the logic of appropriateness (March and Olsen 1998). Some actors use strategic framing to rename or reinterpret issues to minimise audience resistance and advance their hidden agendas (Payne 2001). Moreover, an actor can establish frame resonance by aligning new ideas with already accepted ones, making it easier to gain the target audience's trust and reduce resistance (Ibid).

This analytical lens facilitates our examination of the state's strategies in conveying its data governance priorities to various audiences. As our analysis will demonstrate, disparities exist between the state's discourse and its practical responses to different data breaches. Despite the PRC's discursive efforts to justify its role as a privacy guardian, at the behavioural level, the mishandling of data protection by Chinese local authorities posed significant risks to individual privacy.

We argue that strategic framing functions at both discursive and behavioural levels to help the Chinese government bridge the gap between discourse and behaviour, aiming to construct an image of privacy guardian to justify strong state control over data flows. The strategic framing mechanisms include the reinterpretation of sources of privacy threats through political narratives, fostering legal ambiguity, employing selective framing, and implementing censorship to control public narratives. These mechanisms collectively function to mitigate resistance and legitimise state control over data collection and transfers.

Document analysis

We conducted two rounds of document analysis. Firstly, we examined how the Chinese government framed its role through its global initiative and its position paper Global Digital Governance. These broad efforts served as key frames, encompassing recurring themes that often appeared in other related documents. Secondly, we scrutinised all laws and regulations spanning 2016-23. Key themes emerged during this analysis, such as the securitisation of foreign actors' handling of cross-border data as a matter of national security.

To code the data, we initially identified activities that had the potential to harm 'public interests' or 'privacy'. These identified activities were then categorised as sources of threats to privacy. Since individual privacy represents just one facet of online human rights (Renieris 2023), we deliberately excluded passages that specifically addressed other aspects of digital human rights, focusing solely on privacy-related content during the coding process. Three coders with backgrounds in international relations and computer sciences independently coded the same dataset and convened regularly to review and resolve any discrepancies in coding, thereby ensuring a high level of inter-coder agreement.

The emphasis on the framing of discourses has its limitations. By concentrating on the deliberate use of framing as a tool of persuasion by the state, we primarily focus on the message-producing side rather than the message-receiving side. Although the frames presented in official documents do not guarantee automatic acceptance by either the international community or the state's own citizens, they do provide a framework for social order and stability in terms of normative expectations. Through our comparison of the state's rhetoric with its practices in the two selected cases, we aim to underscore that inconsistencies between discourse and practice can breed resentment and potentially exacerbate existing tensions between citizens and ICT companies on the one hand and the state on the other.

Comparative case studies

At the behavioural level, we use two cases of major data breach incidents in 2022 to demonstrate how the Chinese government employed strategic framing to construct its role as a privacy guardian. Both incidents took place in 2022 and entailed a substantial amount of data being exposed. Meanwhile, 2022 also witnessed the conceptualisation and implementation of broader regulatory frameworks for data governance. However, the Chinese government's response to these cases varied significantly.

The first case is that of Didi, China's largest ride-sharing platform. Its overt collection, processing and alleged illegal transfer of data, led to the administrative penalties amounted to approximately RMB 8.026 billion, marking one of the largest regulatory penalties imposed on a Chinese tech company (*Reuters* 2022). The second case is the Shanghai National Police Database leak in July 2022. An extensive trove of data, amounting to 23 terabytes, which included sensitive personal details such as names, places of birth, national ID card numbers and phone numbers, was illicitly offered for sale online by an anonymous hacker (Ni 2022). If the scale of the data involved is accurate, this could potentially become the largest data leak scandal involving the Chinese government in the global history of data protection (Goh *et al.* 2022). The conspicuous absence

of public discussions in mainstream media, corroborated by reports of relevant information within the Chinese internet being deleted, highlights a double standard when it comes to data breaches involving technology companies and state organs, which is consistent with the strategic framing of the PRC's state actors as a privacy guardian.

Discursive level: the PRC's self-projection as a privacy guardian in official discourse

Through our document analysis, we find that the Chinese state's efforts to portray itself as a protector of individual privacy are substantiated by a foundation of legal and policy documents. The PRC's state organs disguise the potential of the state itself to be a privacy breacher in policy documents and create legal ambiguity in determining if state organs overtly collect or process data. The process of framing is highly strategic, orchestrated through the deliberate drafting and enactment of numerous legislations and policy documents that oversee data governance.

Notably, this institutionalisation process has gained momentum in the late 2010s, primarily as a response to allegations by Western actors regarding covert surveillance activities involving Chinese ICT companies like Huawei and TikTok (Williams 2020). As of May 2023, the PRC has enacted seven significant laws and regulations at the central state level. The PRC's legislative process is primarily driven by the state and is distinguished by its comprehensive and systematic approach (Wang 2022). The institutionalisation of this process commenced with broad policy appeals and subsequently evolved into the development of more targeted laws, regulations and measures. The rapid proliferation of the PRC's data security regulations primarily underscores its concerns regarding the susceptibility of the vast amount of data collected within its borders to foreign entities. Furthermore, these regulations are in alignment with the pressing need to address the aforementioned international accusations of Chinese companies mishandling user data by establishing domestic regulatory standards.

GIDS (2020) and the Position Paper on Digital Governance (2023)

The Foreign Ministry played a pivotal role in disseminating the PRC's position to both global and domestic audiences through the Global Initiative on Data Security (GIDS) (2020). According to the United Nations Development Group, "data security is crucial in ensuring data privacy and data protection" (United Nations Development Group 2017, 5). GIDS shows how the Chinese government understands and legitimises its data privacy protection efforts. It emerged as the overarching framework for government officials, lawmakers and state media to "name, interpret, and dramatize issues" (Payne 2001, 43), shaping the broader societal narratives related to privacy threats.

The Chinese government's commitment to data privacy protection is clearly articulated in GIDS, with recurring passages conveying the message that "states should take actions to prevent and put an end to activities that jeopardize personal information through the use of ICTs" (Ministry of Foreign Affairs of the PRC 2020). As such, the document highlights the central role of the state in countering data breach incidents by ICT service providers. GIDS was a response to the Clean Network Initiative

introduced by the Trump administration to prevent the unauthorised access of sensitive data by Chinese IT vendors. Overall, GIDS established a comprehensive framework comprising eight key expectations for data regulation, offering guidance to both state and non-state entities. These expectations include ensuring supply chain security, safeguarding critical infrastructure, implementing anti-surveillance measures against other states and advocating for data localisation (Ibid).

The PRC's endeavours to engage with international and domestic audiences go beyond GIDS. Another noteworthy document is the Position Paper on Global Digital Governance (2023), which articulates the PRC's perspective on data governance. This position paper was presented to the Global Digital Compact, representing the PRC's preferences for data governance on both the global and domestic scales (Ministry of Foreign Affairs of the PRC 2023). It provides comprehensive guidelines for national security at the collective level and personal privacy at the individual level.

Regarding data privacy protection, the position paper identifies "ICT products and services providers" and "other states" as potential violators, posing the risk of "jeopardiz[ing] personal information and privacy" or "massive surveillance against other states" (Ibid). However, like GIDS, the position paper does not make any references to the constraints placed on state actors themselves when collecting and processing individual privacy data within their own territories. Hence, both documents externalise the threats to data privacy, attributing them to ICT enterprises and other states.

Targeting both an international and domestic audience and widely circulated in both the PRC's domestic and international media coverage, these two documents set normative expectations for their audiences regarding the Chinese government's commitment to safeguard individual privacy rights through intra-state, inter-state and inter-stakeholder approaches. The Chinese government also strategically frames data governance issues in such a way that its target audiences can see how the newly proposed initiatives align with accepted ideas and practices related to human rights, such as the right to digital development and digital skills training (Ibid).

In other words, within these frames, the Chinese government consistently positions itself as the defender of individual privacy, attributing potential threats to large ICT service providers and foreign entities. The government portrays itself as actively combating illegal activities that encroach upon public interests and individual privacy, assuming the role of a mediator between ICT companies and the public in order to strike a balance between the ICT sector's need for large datasets for innovation and the imperative of safeguarding individual privacy. As Mark Jia (2023) observes, this image is beneficial for an authoritarian state. From a top-down perspective, the state must cultivate trust to foster the growth of its digital economy. From a bottom-up viewpoint, the invasion of privacy can potentially serve as a source of social instability, as the widespread use of personal data by the state, such as facial recognition technologies, may drive people to protest. Hence, authoritarian regimes derive advantages by presenting themselves as guardians of individual privacy, as this strategy helps bolster their perceived legitimacy. The benefit associated with monopolising privacy protection incentivises the authoritarian state to maintain framing consistency. Consequently, in specific cases, the state has to adapt its framing to ensure that its actions appear consistent with the image it has constructed.

Domestic legal framework development

Domestically, the PRC has been actively developing its legal and policy framework regulating data collection and flows. These efforts build upon the 2016 Cybersecurity Law, with the security component drawing upon the principles outlined in the 2015 National Security Law. Most data governance regulations have been introduced since 2021 (see Figure 1). While there are commitments made in promoting national security, safeguarding public interests and advancing economic digitisation, this legal and policy framework contains areas where policy goals may clash due to legal ambiguities.

For example, Article 28 of the 2016 Cybersecurity Law delineates the obligation of network operators to provide technical support for public and national security organs in protecting national security and investigating criminal activities, in compliance with legal provisions. In this context, when deemed essential, national security considerations supersede concerns related to the protection of privacy. The legislation also operates on the premise that potential threats to public interests associated with privacy protection predominantly emanate from technology companies and foreign entities. This also aligns with our findings from the document analysis of the abovementioned GIDS and the PRC's position paper.

Moreover, Article 37, in a more specific vein, deals with data localisation, obligating network operators to store their data within the territorial confines of the PRC and to obtain authorisation from the Cyber Administration of China (CAC) and State Council when planning cross-border data transfers. This law grants the state significant authority to intervene in the operations of technology companies by defining whether a certain data breach becomes an issue of national security. Furthermore, it obliges companies to 'alert' the government when engaging in cross-border data transfers, thereby affording the government the capability to halt such transfers if necessary.

The legislative landscape is shaped by laws enacted by the National People's Congress, most notably the 2021 PIPL and the 2021 DSL. Modelled on the GDPR, PIPL represents the PRC's first comprehensive legislation designed to regulate the protection of personal information (Junck *et al.* 2021). It does not overlook the possibility of data privacy breaches within government organisations either. Section 3 of the law specifically outlines the requirements for state organs.

However, legal ambiguity arises when state organs are mandated to confine their utilisation of personal data within the "scope and limits necessary to fulfil statutory duties" (*Xinhua* 2021), as the legislation does not elucidate the precise definition of what qualifies as 'necessary' in this context. It also mandates that state organs notify individuals when processing personal information. Nevertheless, there is an exception to the notification requirement when a notification could impede the ability of state organs to carry out their official duties. Afterall, state organs have significant authority in determining the extent and constraints they consider 'necessary' when it comes to their own collection of personal data. This legal ambiguity creates room for state organs to justify their breaches of the PIPL in practice. Likewise, Chapter V of the DSL is dedicated to limiting the authority of state organs in their acquisition and utilisation of personal data. While it instructs state organs to act within the confines required to fulfil their statutory obligations, it leaves room for open interpretation regarding the precise scope necessary for the state, the CAC and data operators.

When framing threats to individual privacy, the PRC classifies data based on its potential to be used against national security concerns and its sheer volume. The DSL places heightened emphasis on the categorisation of 'core data' and substantial volumes of data in cross-border flows, deeming them as more critical to national security and therefore necessitating more stringent state controls. Article 21 of the DSL defines 'core data' as data pertaining to national security, the lifelines of the national economy, important aspects of people's lives and major public interests. This framing enables the state to categorise specific data as a security concern, distinguishing it from both 'important data' and 'other data' (Bi 2021). However, the definition of 'core data' remains ambiguous, offering limited guidance to practitioners when it comes to making decisions and taking concrete actions (Lai 2021). Hence, the ambiguity surrounding the classification of 'core data' may give rise to various interpretations in practice.

In addition to these major legal pillars, the Chinese government, including bodies like the State Council and the Cyberspace Administration of China (CAC), regularly issues supplementary measures and regulations aimed at providing operational-level clarity and guidance.

The State Council has taken steps to provide clarity concerning critical information infrastructure (CII). In 2021, it issued the Regulations on CII Security Protection (关键信息基础设施安全保护条例), which delineated the specific responsibilities of companies designated as CII operators. These regulations outlined their obligations to report security-related issues to both the CAC and the National Security authorities. As will be discussed in the case studies section, this clarification allowed the Party-state to frame Didi Chuxing's excessive collection of personal data as a lapse in its role as a CII operator.

In November 2021, the CAC extended the PRC's data governance jurisdiction beyond its territorial borders. This clarification came in the form of the draft Regulations on Network Data Security Management (网络数据安全管理条例（征求意见稿）). This new draft brought data handlers listed in Hong Kong under the purview of cybersecurity review (Kurth 2022). At the time of writing, the draft Regulations on Network Data Security Management remain in the discussion phase, with the Chinese government seeking public feedback.

In February 2022, the CAC, in collaboration with 12 other government organisations, introduced a revised version of the Cybersecurity Review Measures (网络安全审查办法), replacing the prior iteration from April 2020 (Guo and Li 2022; Cyberspace Administration of China *et al.* 2022). The involvement of several government organisations underscores the profound national security considerations underpinning these measures. Notably, the National Administration of State Secret Protection and the PRC's State Cryptography Administration, typically less prominent in day-to-day state affairs, were among the key contributors to this effort. These new measures also provide clarity regarding the threshold at which the sheer volume of data becomes a matter of security concern. According to Article 7, operators holding personal information of more than 1 million users are mandated to undergo a cybersecurity review prior to conducting their overseas initial public offering, as the sheer volume of data itself, if analysed by foreign entities, can potentially yield insights that could pose a threat to national security.

In May 2022, the CAC further clarified the rules for network operators' activities pertaining to cross-border data transfers through the publications of the Measures for

Security Assessment of Cross-Border Data Transfers (数据出境安全评估办法). These measures require operators to report to their local cybersecurity administrations and conduct a thorough security risk assessment before engaging in such transfers. In effect, this empowers cybersecurity administration authorities to terminate cross-border data transfers in the interest of data security.

In summary, at the discursive level, the PRC's Ministry of Foreign Affairs strategically reframes the sources of data privacy threats for both domestic and international audiences. Threats to personal privacy are strategically framed as emanating from ICT products and services providers and other states, effectively redirecting accountability away from state actors operating within their own jurisdictions. In addition, the National People's Congress formulates laws to show the state's commitment to limiting even its own powers to prevent the excessive collection of personal data. Subsequently, the government, mainly the State Council and the CAC, issues measures and regulations to provide further operational-level clarity for the implementation of these laws. However, there is a legal ambiguity concerning the degree to which state organs consider it necessary to fulfil their statutory duties. This ambiguity opens the door to potential contestation by different state organs and leaves a legal loophole that could lead to privacy infringements by state actors themselves.

Behavioural level: comparative case studies of Didi and Shanghai National Police data leak

This section draws a comparison between two significant data breaches in 2022: the delisting of Didi Chuxing, including the subsequent investigation and fine imposed by Chinese authorities, and the Shanghai National Police Database leak. These two cases occurred around the same time but received notably distinct levels of public attention in the PRC due to selective framing and censorship tactics. By using these tactics, the Chinese state has sought to organise events into a cohesive narrative that is aligned with its discursive commitment, bolstering its self-image as a defender of individual privacy and providing rationale for its stringent state control over cross-border data transfers.

Didi

Didi's data breach and national security infringement were widely publicised in the PRC in 2022. Founded in 2012, Didi swiftly rose to prominence as the country's largest ride-sharing platform. The company made a significant move in 2016 by acquiring Uber's operations in the PRC, further solidifying its dominance in the Chinese market. By maintaining an extensive repository of consumer data, including crucial location and mapping information, Didi places itself under the jurisdiction of the DSL. Notably, the Didi app gathers detailed information about its drivers, including their location and speed, recorded at intervals of every three seconds (Etherington 2016). This wealth of data can be seen as a substantial privacy and national security concern, as possessing detailed knowledge of specific locations and the individuals who frequently access them could potentially enable foreign entities to gather personal information about important governmental officials and strategic sites. Despite claims made by Didi's Chief Technology

Officer, Bob Zhang, that the data was anonymised (Ibid), the broad scope of data collected proved to be a source of concern, as evidenced by the CAC's subsequent charge against it. Didi's data collection encompasses a staggering 120 types of information, ranging from users' identity and banking details to their location, device information, and even text data such as nicknames and status updates generated within Didi's ecosystem.

However, the extensive data collection was not solely driven by business concerns. As a platform operating within the PRC, Didi is legally obliged to cooperate with security departments to safeguard the wellbeing of both its drivers and passengers. This means that Didi is obligated to use its data and algorithmic capabilities to help law enforcement identify and prevent 'unsafe' behaviour. To this end, Didi has implemented data collection and analysis measures, using sensors and location data from both drivers' and passengers' cell phones. An example of Didi-police collaboration pertains to background and safety checks for drivers. To carry out comprehensive screenings, Didi worked with law enforcement to obtain access to drivers' criminal records and employed facial recognition technology (Didi Global 2020). Furthermore, the alarm function in the Didi app, which allows users to contact the police with a single click, facilitates data sharing between the user and law enforcement authorities. Moreover, Didi's Safe Driving System allows dashboard cameras and microphones to capture a wide range of crucial information, including road conditions, instances of reckless driving, driver-passenger disputes and potential signs of fatigue (Xiao 2017).

The substantial volume of data and AI training enabled the company to venture beyond the commercial sector and into digital utilities. The collected data played an indispensable role in the Traffic Information Platform, delivering real-time traffic updates and invaluable insights to transport authorities across the PRC. Through its contributions to this platform, Didi solidified its position as a crucial component of the infrastructure for smart and digital cities. Consequently, Didi emerged as an innovative solution that went beyond ride-sharing services, contributing to tackling urban planning challenges and addressing public discontentment.

While Chinese authorities had enlisted Didi for more efficient security governance and urban planning, they remained uncompromising when accusing the company of breaching privacy after its cross-border data transfers were associated with national security concerns. Shortly after the DSL came into effect, the CAC promptly issued a notice for the removal of Didi from app stores (*People's Daily* 2021). At the time, the CAC allowed Didi some time to rectify its excessive collection of personal data and did not impose any fines. However, when Didi later decided to list on the New York Stock Exchange (NYSE), the risks associated with cross-border data transfers became more pronounced, underlying the government's concerns that such data transfers could potentially compromise national security.

On 21 July 2022, the CAC imposed administrative penalties on the company, alleging that Didi had violated all data security laws, including the CSL, DSL and PIPL (*People's Daily* 2022). The administrative fines amounted to approximately RMB 8.026 billion (EUR 1.043 billion), with Didi's Chairman and CEO, Cheng Wei, and President, Liu Qing, each being fined RMB 1 million (EUR 130 million). This establishes a noteworthy precedent, marking the highest fine imposed in the global history of data protection (Goh *et al.* 2022), surpassing the EUR 743 million fine for Amazon's violation of GDPR.

It is interesting to note that while the substantial fines were primarily driven by concerns about data being exploited by foreign entities and the associated potential national security risks, the charges issued by the CAC primarily framed Didi's violation in terms of its infringement on individual privacy, which resonated more strongly with broader public concerns. The CAC identified 16 types of alleged illegal activities by Didi, none of which were explicitly linked to national security. However, it did assert that Didi's data processing posed risks to CII and data security. These specific risks were not disclosed to the public due to their implications for national security (*People's Daily* 2022).

The above analysis of the Didi case offers a nuanced perspective, highlighting that the excessive collection of personal data can become a heightened national security concern once cross-border data transfers occur. At this juncture the elevated risk of foreign entities using the data for intelligence and surveillance purposes comes into focus. Given the nature of Didi's business operations, it can easily be categorised as having potential national security implications, owing to the sensitive nature of the information it collects – particularly location information – and the substantial volume of data it amasses, exceeding one million users. The timing of the CAC's investigation, coinciding with Didi's listing on the NYSE, carries significant implications, as it underscores that the key consideration lies in cross-border data transfers in this context.

The Didi case presents an opportunity for the Chinese government to frame itself as a staunch defender of individual privacy against violations by ICT service providers. Didi's privacy infringement issue was not publicly announced and fines were imposed only after cross-border data transfers were identified when the company announced its NYSE listing. In other words, privacy concerns were raised and brought into focus when the potential threat to national security was deemed significant. This created a convergence between individual privacy, national security and regime stability concerns, enabling the government to label Didi as an exploitative company whose excessive collection of personal data poses a threat not only to citizens but to the collective interests of the state. However, within this framing, the contributions of Didi's prior data collection and AI capabilities to government security governance and urban planning are downplayed, which obscures the shared responsibility of state organs in the overt data collection facilitated by Didi.

Shanghai National Police Database Leak

In July 2022, an anonymous hacker known as 'ChinaDan', offered to sell over 23 TB of data for 10 bitcoins (approximately equivalent to USD200,000) on the hacker forum Breach Forum. These databases comprise information on 1 billion Chinese national residents, encompassing sensitive details such as ID numbers, mobile numbers and even crime-related information (Goh *et al.* 2022; Ni 2022; Hurst 2022).

The Chinese authorities have never officially acknowledged the existence of this data privacy breach. Despite receiving extensive coverage in international media and sparking heated discussions on the PRC's social media platforms, which were subsequently censored in the country's domestic internet domain, the Chinese government refrained from making any official comments and maintained a conspicuous silence regarding the data leak scandal. Nevertheless, *The Wall Street Journal* managed to verify the

accuracy of the hacked information by confirming the story with five affected individuals (*The Economist* 2022).

One hypothesis is that the leak occurred due to the Shanghai Police's failure to adhere to data security protocols and data protection practices (Goh *et al.* 2022). Another ascribes the leak to an unsecured backdoor link (Xiong *et al.* 2022). The data had been reportedly left unsecured for 14 months on Alibaba's cloud servers without any protective measures (Kaur 2022). It was only when ChinaDan placed it for ransom that it garnered significant attention (Tang 2022; Qin 2022; Xiong *et al.* 2022). As Alibaba Cloud had secured the bid for the Smart Public Security Comprehensive Service Platform Construction Project of the Shanghai Public Security Bureau on 15 July 2019, the subsequent summoning of executives from its computing division has been seen by some as an indication that the police were shifting the blame to them for the mishandling of the data (Kaur 2022; Tang 2022). In September 2023, a report revealed that an unnamed contractor had used government data for testing purposes, failing to fulfil its obligations in terms of data security during data processing (*Xiaoxiang Morning Herald* 2023). Lacking a data security management system, its storage systems had vulnerabilities, resulting in the leakage of citizens' data – which was subsequently sold overseas – and an extensive privacy infringement (Ibid). The Shanghai Municipal Cyberspace Administration collaborated with relevant departments to investigate the matter and subsequently requested that the company take down the website and close the relevant cloud service ports, in addition to imposing administrative penalties (Ibid). Later, it came to light that the contractor had been held accountable for its negligence. The repercussions included the suspension of their services and the imposition of administrative penalties. Interestingly, however, these penalties appeared relatively lenient when juxtaposed with similar instances of data breaches (GoUpSec 2024). This suggests that the contractor may have been used as a scapegoat for the government's own negligence.

The way in which the leak has been handled illustrates that even though the state has remained conspicuously silent in public discussions, it is evidently aware of the risks linked to this scandal. As mentioned, in authoritarian states, safeguarding privacy also serves as a means for the regime to bolster its legitimacy (Jia 2023). The dramatic failure of the state to comply with its own data protection laws undermines the frame of the state as a guardian of individual privacy. While local authorities attempted to deflect responsibility onto the contractor, it is undeniable that the local authorities, and therefore the state, bear accountability for their failure to adequately oversee the storage of data.

Notably, the government did not raise a significant outcry in this instance. It is likely that the sheer magnitude and sensitivity of the data involved in this case were such that if the government were to acknowledge it, public anger over the government's own failure in safeguarding privacy might overshadow their anger toward foreign entities. This can pose a risk to regime stability, as it has become a common practice in the PRC for state actors to collect and store vast amounts of data through digital technologies, such as facial recognition and video surveillance (Zeng 2022). Ultimately, it is the government that decides to collect and store this data, therefore the discourse surrounding these incidents does more harm than good to the state's framing efforts.

In comparison, the data involved in the Shanghai National Police Database case is a staggering 1,000 times larger than that of Didi, yet the publicly announced penalties

Table 1. Privacy infringements by the PRC's state and non-state actors.

	Didi	Shanghai National Police Database
Scale of data involved	1 million personal information	Alleged leak of 1 billion personal information
Actor involved	Didi	Shanghai Police and a contractor (speculated by some to be Alibaba)
State responses	Administrative penalties of RMB 8.026 billion	Censorship, scapegoating, unknown amount of administrative penalties imposed on the contractor

imposed on those held accountable were disproportionately lower (see Table 1). This highlights the state's consistent efforts to frame itself as a guardian of individual privacy, selectively emphasising cases where individual privacy protection, national security and regime stability align, while downplaying instances where state actors could face accountability for mishandling data, due to concerns about jeopardising regime stability and legitimacy. Even in cases where there is an apparent government failure, it has sought to frame itself as the victim and shifts the blame onto contractors. Instead of using denial and condemnation to redirect public anger toward foreign entities, the state maintained a conspicuous silence in this instance, thereby avoiding further public attention that could potentially destabilise the regime itself.

Conclusion

This article illustrated that the Chinese legislative bodies and the government have used strategic framing to construct themselves as a privacy guardian instead of a potential privacy violator, especially when addressing their domestic audience. Such a strategic framing mechanism includes:

(i) Reinterpreting sources of threat in the 2020 GIDS and 2023 position paper
(ii) Legal ambiguity in the legislative process to govern data flow
(iii) Selective framing and censorship in major data breach incidents, exemplified by two significant scandals – the Didi case and the Shanghai National Police Database leak

As an authoritarian state, the PRC perceives data as a vital resource that necessitates strict state oversight, emphasising territorial control despite the inherently de-territorialised nature of data. The extent to which collected data can be used by foreign entities determines the Chinese government's level of interference toward privacy infringements in practice. In the case of Didi, government intervention became coercive when the necessity for cross-border data transfers arose. The convergence of individual privacy, national security and regime stability concerns meant that it was in the government's interest to emphasise the illegal activities committed by Didi, even though the government had previously co-opted the company in security governance and urban planning. Interestingly, while the government has asserted that Didi's practices posed a national security risk, all the publicly listed illegal activities were connected to individual privacy. The government exhibited a starkly contrasting stance in the Shanghai National Police Database case, which encompassed data on a scale 1,000 times greater than that of Didi. Nevertheless, the punitive measures were glaringly disproportionate given that state actors were

accountable for mismanagement of the database. Overall, through these mechanisms, the Chinese government, mainly the CAC, has sought to maintain coherence across discourse and behaviour in presenting the party-state as the guardian of individual privacy, further justifying strong state control over data collection and flows.

The PRC's approach to data sovereignty, however, also highlights the shared concerns seen in the CLOUD Act and GDPR in terms of the need to exert territorial control over data, despite different motives and norms that have been driving this tendency. As Xinchuchu Gao (2022) argues, the lines between the PRC's sovereignty-oriented approach and the 'Western' approach are becoming increasingly blurred. The PRC's emphasis on data sovereignty and concerns about data abuse by foreign entities inevitably resonate with many other countries, both democratic and authoritarian, in the context of rising geopolitical tensions. This warrants further discussion regarding the extent to which various countries converge in their regulatory practices in the data governance realm, as well as the underlying reasons for such convergence.

Acknowledgements

The authors are immensely grateful to the three anonymous reviewers who helped refine the arguments, enhance the analysis, and elevate the overall quality of this paper. They wish to extend their heartfelt thanks to the editors for their exceptional editorial support and timely communication.

Notes on contributors

Ruoxi Wang received her PhD from the School of International Relations at the University of St Andrews, St Andrews, United Kingdom. She is a Research Fellow at the Centre for Global Law and Governance at the University of St Andrews. Email: ruoxiwang936@gmail.com

Chi Zhang is an Associate Lecturer at the University of St Andrews, St Andrew, United Kingdom.

Yaxiong Lei is a PhD candidate at the School of Computer Science at the University of St Andrews, St Andrews, United Kingdom. Email: yl212@st-andrews.ac.uk

ORCID

Ruoxi Wang http://orcid.org/0000-0002-7468-2601
Chi Zhang http://orcid.org/0000-0003-3881-0546
Yaxiong Lei http://orcid.org/0000-0002-0697-7942

References

Acharya, Amitav. 2004. How Ideas Spread: Whose Norms Matter? Norm Localization and Institutional Change in Asian Regionalism. *International Organization* 58 (2): 239–75.

Barrinha, André, and Christou, George. 2022. Speaking Sovereignty: The EU in the Cyber Domain. *European Security* 31 (3): 356–76.

Bi, Lei. 2021. 首提'国家核心数据' 《数据安全法》划定数据安全风险基本'红线' [The First Mention of 'National Core Data': The 'Data Security Law' Defines the Basic 'Red Line' of Data Security Risks] *People.cn*, 24 June. http://finance.people.com.cn/n1/2021/0624/c1004-32139926.html.

Borgogno, Oscar, and Savini Zangrandi, Michele. 2023. Chinese Data Governance and Trade Policy: From Cyber Sovereignty to the Quest for Digital Hegemony? *Bank of Italy Occasional Paper* 759: 5–26.

Broeders, Dennis, Cristiano, Fabio, and Kaminska, Monica. 2023. In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions. *Journal of Common Market Studies* 61 (5): DOI: https://doi.org/10.1111/jcms.13462.

Cai, Cuihong, and Wang, Yuanzhi. 2020. 全球数据治理: 挑战与应对 [Global Data Governance; Challenges and Responses]. 国际问题研究 [*International Studies*] 6: 38–56.

Cao, Lei. 2013. 网络空间的数据权研究 [Analysis of Data Rights in Cyberspace]. *国际观察* [*International Review*] 1: 53–8.

Cyberspace Administration of China *et al.* 2022. Cybersecurity Review Measures [网络安全审查办法]. http://www.gov.cn/zhengce/zhengceku/2022-01/04/content_5666430.htm.

Didi Global. 2020. 滴滴安全发布第7期：持续深化警企合作，探索更多创新联动模式 [Didi Security Report 7: Continue to Deepen Police-Enterprise Cooperation and Explore More Innovative Cooperative Models]. 25 September. https://www.didiglobal.com/news/newsDetail?id=967&type=blog.

Etherington, Darrell. 2016. Didi's CTO Explains Why China's Ride-Sharing Giant has a Data Advantage. *TechCrunch*, 2 December. https://techcrunch.com/2016/12/02/didis-cto-explains-why-chinas-ride-sharing-giant-has-a-data-advantage/.

Finnemore, Martha, and Sikkink, Kathryn. 1998. International Norm Dynamics and Political Change. *International Organization* 52 (4): 887–917.

Gamson, William A. 1989. News as Framing: Comments on Graber. *The American Behavioral Scientist (1986-1994)* 33 (2): 157–61.

Gao, Xinchuchu, and Chen, Xuechen. 2022. Role Enactment and the Contestation of Global Cybersecurity Governance. *Defence Studies* 22 (4): 689–708.

Gao, Xinchuchu. 2022. An Attractive Alternative? China's Approach to Cyber Governance and Its Implications for the Western Model. *The International Spectator* 57 (3): 15–30.

Goh, Brenda, Yu, Sophie, Qiu, Stella, and Baptista, Eduardo. 2022. Hacker Claims to Have Stolen 1 Bln Records of Chinese Citizens from Police. *Reuters*, 6 July 2022. https://www.reuters.com/world/china/hacker-claims-have-stolen-1-bln-records-chinese-citizens-police-2022-07-04/.

GoUpSec. 2024. 盘点：2023年网络安全事件处罚案例 [Checklist 2023 Internet Security Incident Punishment Cases]. 5 January. https://www.secrss.com/article/62512.

Guo, Bingna, and Li, Bob. 2022. China Issued New Measures for Cybersecurity Review in 2022. White & Case LLP. 8 February. https://www.whitecase.com/insight-alert/china-issued-new-measures-cybersecurity-review-2022.

Hang, Min, and Zhou, Changcheng. 2022. 互联网治理下的数据主权与媒介策略 [Data Sovereignty and Media Strategy in the Context of Internet Governance]. *Media*. https://m.thepaper.cn/newsDetail_forward_16834681

He, Aoxuan. 2021. 数据全球化与数据主权的对抗态势和中国应对——基于数据安全视角的分析 [Confrontation and China's Solution of Data Globalization and Data Sovereignty: Based on Data Security]. *Journal of Beijing University of Aeronautics and Astronautics (Social Sciences Edition)* 34 (3): 18–26.

Hummel, Patrik, Braun, Matthias, Tretter, Max, and Dabrock, Peter. 2021. Data Sovereignty: A Review. *Big Data & Society* 8 (1). DOI: https://doi.org/10.1177/2053951720982012.

Hurst, Luke. 2022. Shanghai Data Leak: China Censors Searches after Claim that Data of 1 Billion People Was Hacked. *Euronews*, 6 July. 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. SSRN Scholarly Paper. Rochester (NY) https://doi.org/10.2139/ssrn.4362527.

Junck, Ryan D., *et al.* 2021. China's New Data Security and Personal Information Protection Laws: What They Mean for Multinational Companies. *Skadden*, 3 November. https://www.skadden.com/insights/publications/2021/11/chinas-new-data-security-and-personal-information-protection-laws.

Kaur, Dashveenjit. 2022. Is Alibaba Responsible for the Largest Data Heist in China? *Tech Wire Asia*, 18 July. https://techwireasia.com/07/2022/is-alibaba-responsible-for-the-largest-data-heist-in-china/.

Kokas, Aynne. 2022. *Trafficking Data: How China Is Winning the Battle for Digital Sovereignty*. Oxford/New York: Oxford University Press.
Kurth, Andrews. 2022. China Releases Draft Regulations on Network Data Security Management. Hunton Privacy & Information Security Law Blog, 26 January. https://www.huntonprivacyblog.com/2022/01/26/china-releases-draft-regulations-on-network-data-security-management/.
Kuypers, Jim A. 2009. Framing Analysis. In Jim A. Kuypers, ed. *Rhetorical Criticism: Perspectives in Action*: 181–204. Maryland (MD): Lexington Books.
Lai, Karry. 2021. PRIMER: China's Data Security Law. IFLR, 11 November. https://www.iflr.com/article/2a6478kz8k2ue7ln620ao/primer-chinas-data-security-law.
March, James G., and Olsen, Johan P. 1998. The Institutional Dynamics of International Political Orders. *International Organization* 52 (4): 943–69.
Ministry of Foreign Affairs of the PRC. 2020. Global Initiative on Data Security. September. https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/202009/t20200908_679637.html.
Ministry of Foreign Affairs of the PRC. 2023. China's Positions on Global Digital Governance (Contribution for the Global Digital Compact). May. https://www.fmprc.gov.cn/eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/202305/t20230525_11083607.html.
Moerel, Lokke, and Timmers, Paul. 2021. Reflections on Digital Sovereignty. EU Cyber Direct. Research in Focus Series. https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/khGGovSY/rif_timmersmoerel-final-for-publication.pdf
Ni, Vincent. 2022. Hacker Claims to Have Obtained Data on 1 Billion Chinese Citizens. *The Guardian*, 4 July. https://www.theguardian.com/technology/2022/jul/04/hacker-claims-access-data-billion-chinese-citizens.
O'Hara, Kieron, and Hall, Wendy. 2021. Preliminary Concepts: Networks and Data. In O'Hara, Kieron, and Hall, Wendy. *Four Internets: Data, Geopolitics, and the Governance of Cyberspace*: 1–24. Oxford: Oxford University Press.
Payne, Rodger A. 2001. Persuasion, Frames and Norm Construction. *European Journal of International Relations* 7 (1): 37–61.
People's Daily. 2021. 国家网信办：滴滴出行，下架 [Cyberspace Administration of China: Didi Chuxing, Off the Shelves!] 4 July. https://wap.peopleapp.com/article/6241686/6140184.
People's Daily. 2022. 国家网信办：滴滴存在严重影响国家安全的数据处理活动 [Cyberspace Administration of China: Didi Engaged in Data Processing Activities with Serious National Security Implications]. 21 July. http://finance.people.com.cn/n1/2022/0721/c1004-32482059.html.
Priol, Jacques, and Vincent-Galtie, Joe. 2022. Neither Surveillance Nor Algorithm-Driven Consumerism: Toward an Alternative European Model for Smart Cities. French Institute of International Relations. 16 November. https://www.ifri.org/en/publications/etudes-de-lifri/neither-surveillance-nor-algorithm-driven-consumerism-toward.
Qin, Amy, Liu, John, and Chang Chien, Amy. 2022. Chinese Police Database Was Left Unsecured long before Hackers Seized It. *The New York Times*, 7 July. https://www.nytimes.com/2022/07/07/business/china-police-database-hack.html.
Que, Tianshu, and Wang, Ziyue. 2022. 数字经济时代的全球数据安全治理与中国策略 [Global Data Security Governance and Action Strategies for China's Participation in the Era of Digital Economy]. *Journal of International Security Studies* 1: 130–54.
Renieris, Elizabeth M. 2023. *Beyond Data: Reclaiming Human Rights at the Dawn of the Metaverse*. Cambridge (MA): MIT Press.
Reuters. 2022. China to Fine Didi More than $1 Billion for Data Breaches, Sources Say. 19 July. https://www.reuters.com/technology/chinese-regulators-fine-didi-more-than-1-billion-over-data-breaches-wsj-2022-07-19/.
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): 304–24.

Snow, David A., Burke Rochford, E., Worden, Steven K., and Benford, Robert D. 1986. Frame Alignment Processes, Micromobilization, and Movement Participation. *American Sociological Review* 51 (4): 464–81.

Tang, Jane. 2022. Shanghai Data Breach Exposes Suppression of 'White-Hat' Security Research in China. *Radio Free Asia*, 16 July. https://www.rfa.org/english/news/china/breach-07152022152546.html.

The Economist. 2022. A Huge Data Leak in China Was Not Unexpected. 7 July. https://www.economist.com/china/2022/07/07/a-huge-data-leak-in-china-was-not-unexpected.

United Nations Development Group. 2017. Data Privacy, Ethics and Protection: Guidance Note on Big Data for Achievement of the 2030 Agenda. https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf.

Wang, Xixin. 2022. The Bundle of Personal Information Rights from the Perspective of State Protection. *Social Sciences in China* 43 (2): 36–54.

Williams, Robert D. 2020. Beyond Huawei and TikTok: Untangling US Concerns over Chinese Tech Companies and Digital Security. Brookings, 30 October. https://www.brookings.edu/articles/beyond-huawei-and-tiktok-untangling-us-concerns-over-chinese-tech-companies-and-digital-security/.

Wood, Georgia, and Lewis, James Andrew. 2023. The Cloud Act and Transatlantic Trust. Center for Strategic & International Studies. March. https://www.csis.org/analysis/cloud-act-and-transatlantic-trust.

Xiao, Eva. 2017. Didi's Master Plan to Win over Local Chinese Governments – with Data. *Tech in Asia*, 29 April. https://www.techinasia.com/didi-big-data-traffic-platform.

Xiaoxiang Morning Herald. 2023. 公民个人信息遭境外披露兜售，上海市一政务信息系统技术服务公司被行政处罚 [Shanghai Government Information Systems Tech Firm Penalized for Overseas Disclosure and Sale of Citizens' Personal Information]. 15 September. https://www.sohu.com/a/720831050_120914498.

Xinhua. 2021. 中华人民共和国数据安全法 [Data Security Law]. 11 June. https://www.gov.cn/xinwen/2021–06/11/content_5616919.htm.

Xiong, Yong, Ritchie, Hannah, and Gan, Nector. 2022. Nearly One Billion People in China had their Personal Data Leaked, and It's been Online for More than a Year." *CNN*, 5 July. https://www.cnn.com/2022/07/05/china/china-billion-people-data-leak-intl-hnk/index.html.

Zeng, Jinghan. 2022. *Artificial Intelligence with Chinese Characteristics*. London: Palgrave Macmillan.