Centre for International
Governance Innovation

CIGI Papers No. 282 — September 2023

State-Centric Data Governance in China

Alex He

Centre for International
Governance Innovation

CIGI Papers No. 282 — September 2023

State-Centric Data Governance in China

Alex He

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

Credits

Managing Director of Digital Economy Robert Fay
Director, Program Management Dianna English
Project Manager Jenny Thiel
Senior Publications Editor Jennifer Goyder
Publications Editor Susan Bubak
Graphic Designer Abhilasha Dewan

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Table of Contents

About the Author

Xingqiang (Alex) He is a CIGI senior fellow. He is an expert on digital governance in China, the Group of Twenty (G20), China and global economic governance, domestic politics in China and their role in China's foreign economic policy making, and Canada-China economic relations.

Prior to joining CIGI in 2014, Alex was a senior fellow and associate professor at the Institute of American Studies at the Chinese Academy of Social Sciences (CASS) and a visiting scholar at the Paul H. Nitze School of Advanced International Studies, Johns Hopkins University, in Washington, DC (2009–2010). Alex was also a guest research fellow at the Research Center for Development Strategies of Macau (2008–2009) and a visiting Ph.D. student at the Centre of American Studies at the University of Hong Kong (2004).

Alex is the author of *The Dragon's Footprints: China in the Global Economic Governance System under the G20 Framework*, published in English (CIGI Press, 2016) and Chinese editions, and co-author of *A History of China-U.S. Relations* (Chinese Social Sciences Press, 2009). Alex has published dozens of academic papers, book chapters, and newspaper and magazine articles.

Alex has a Ph.D. in international politics from the Graduate School of CASS and previously taught at Yuxi Normal University in Yunnan Province, China. Alex is fluent in Chinese and English.

Acronyms and Abbreviations

AI	artificial intelligence
BRI	Belt and Road Initiative
CAC	Cyberspace Administration of China
CCAC	Central Cyberspace Affairs Commission
CII	critical information infrastructure
CLOUD Act	Clarifying Lawful Overseas Use of Data Act
CPTPP	Comprehensive and Progressive Agreement for Trans-Pacific Partnership
CSL	Cybersecurity Law
DEPA	Digital Economy Partnership Agreement
DSL	Data Security Law
DSR	Digital Silk Road
FTZs	free trade zones
GDPR	General Data Protection Regulation
IPO	initial public offering
MIIT	Ministry of Industry and Information Technology
NDA	National Data Administration
NDRC	National Development and Reform Commission
NPC	National People's Congress
NYSE	New York Stock Exchange
PIPL	Personal Information Protection Law
PRC	People's Republic of China
RCEP	Regional Comprehensive Economic Partnership
SAC	Standardization Administration of China
SAMR	State Administration for Market Regulation
WTO	World Trade Organization

Executive Summary

China's state-centric data governance regime has evolved into a framework characterized by the pursuit of a dual goal to bolster both economic growth and national security at the expense of personal information protection, which is significantly compromised due to the government's mostly unfettered access to personal data.

With the rapid growth of the digital economy in the country since 2014–2015, data was initially recognized as a fundamental factor of production and a strategic resource for economic development in China. In the years that followed, data was freshly defined as the core engine to deepen the development of the digital economy in China. The role of data as a factor endowment is further recognized as the crucial element to empower the realization of building a digital China, with the digital transformation of traditional industries, digital industrialization, as well as the digitalization of public services and the governance system, as the ultimate goal.

At the same time, national security, not personal information protection, has become the crux of China's data regulations and laws, which focus on protection of the widely used and vaguely defined "important data" and "core data."

Although the Personal Information Protection Law (PIPL) stipulates extensive protection of personal data and protection for users' interests from being abused by large private platforms, an analysis of the key articles in the PIPL, and the Data Security Law (DSL) and its implementing regulations clearly indicated that the Chinese government has mostly free rein to access all data, including personal data and the data of any organization or internet operator, in the name of national security or public interest.

The dual goal of seeking to bolster both economic growth and national security in its data governance regime was plainly illustrated in China's regulation of large digital tech platforms, which stands out as a typical example of the Chinese government's efforts to handle the balance between development and security. On the basis of safeguarding national security and protection of individual data, China has deemed large digital tech platforms as critical infrastructure and enacted strict regulations to protect personal data in their business practices while expecting these platforms to promote the country's data-driven economic development.

The evolving regulatory regime of cross-border data flows also demonstrates the dual goal in data governance. While recognizing the great potential gains of the data-based digital economy, Chinese policy makers are concerned about the possible significant negative impacts free cross-border data flows could have on national security and individual data protection.

In summary, the government's mostly unfettered access to personal data is clearly stipulated in the PIPL and the DSL, which have the highest legal authority in China's data governance system. In the governance of large digital platforms and cross-border data flows, national security and economic growth are prioritized as a dual goal, while the protection of personal data is essentially compromised by the government's mostly free hand to access personal data.

Introduction

The embryonic idea of data governance in China began to emerge along with China embracing the digital economy as a new engine for economic growth around 2014–2015. The initial thoughts were focused on how data could drive the economy, while recognizing the necessity and significance of cybersecurity protection and developing related laws and regulations. Before that, the protection of internet information, network information and personal information of internet users along with the regulation of internet information services and the telecommunications market were the main issues. There were sporadic rules in a few regulations and laws (Sacks, Webster and Shi 2019) that address these issues. The idea of data regulation or data governance has not fully developed in China.

In parallel with the rapid growth of China's digital economy, which has been bolstered by the mushrooming e-commerce and mobile payment systems in the country since 2014–2015, the Cybersecurity Law (CSL) was enacted in November 2016 and came into effect in 2017, after years of preparation and drafting. This represented the

first of the major laws that constitute China's data governance system and laid the foundation for the DSL and the PIPL that followed. When the latter two major laws were in force in 2021, China's framework for data governance emerged. It contains regulations on a wide range of issues, including data regulation, data security, personal information protection and the data-driven economy, as well as cross-border data flows, data localization, China's engagement in global data governance, and so on.

This paper first examines three components of data governance in China and then considers data governance institutions in the country, followed by a detailed explanation in the third part of why seeking to bolster both economic growth and national security is the dual goal of China's state-centric data governance and how this priority comes at the expense of personal information protection. The fourth and fifth parts of the paper, respectively, focus on how digital platform governance and regulation on cross-border data flows have illustrated this. The final part concludes the paper with a discussion of the global implications of China's data governance system.

The Three Components of the Data Governance System in China

Data as a Fundamental Factor of Production and Strategic Resource for Economic Development

By October 2014, the Action Outline for Promoting the Development of Big Data had been drafted, led by the Ministry of Industry and Information Technology (MIIT) and the National Development and Reform Commission (NDRC), two prominent government agencies responsible, respectively, for industry and information technology and strategy planning for economic growth. China began to designate data as an important factor of production, along with other traditional factors — land, capital, labour and technology. In addition to being acknowledged as a key driver for the growth of the digital economy, data as a new type of factor of production is expected to bring significant, transformative impact on traditional modes of production and generate new industries and businesses in China.

In the official version of the Action Outline, which was released in September 2015, data is defined as "the new driver of the digital transformation of economy," an important "national strategic resource," the new opportunity to promote innovation-based industrial development and reshape China's competitive advantage, and a new approach to improve the governance capacity of government (State Council 2015; MIIT 2015). This represented the formation of an economic component in data governance in China. The Action Outline, which was regarded as the strategic guiding document for China's big data industry, gives the priorities on how data could perform as factors for economic and industrial development and how to improve the governance capability of government via data sharing and use.

Establishing security guarantee mechanisms for big data was mentioned but was not the most important issue in the Action Outline. The concept of "data security" was not formed in China until the development of national data security regulation in the following years.

Data Security as a Crucial Component of State Security Should Be Strictly Protected

Data security is a newer concept in China compared to the perception of cybersecurity, which was first included in China's annual government report in March 2014, one month after President Xi Jinping established and headed the Central Leading Group of Cybersecurity and Informatization (renamed as the Central Cyberspace Affairs Commission in 2018). As part of President Xi's "overall concept of national security" that was raised in April 2014 (Xinhua 2014), the CSL, along with the newly updated National Security Law and Counterterrorism Law were drafted and adopted during 2015–2016.

The draft of the CSL was approved in June 2015 and adopted in November 2016; the law came into effect in June 2017. The CSL contains the initial regulation on data security, data classification, protection, data localization and so on, indicating the beginning of the security concern of data

governance being incorporated into China's data governance system. In particular, the definition and regulation of critical information infrastructure and subsequent requirement of data localization set the tone for the forthcoming draft and adoption of the DSL, which came into effect in September 2021.

In 2018, China's national legislative body, the National People's Congress (NPC), put the legislation of data security and personal information protection on its legislative agenda (Huang, Yuan and Hu 2020) in response to the increasingly urgent need for data protection from external cyber hacking and invasion and to improve the level of data governance among national and regional governments. Data security includes a wide range of issues, such as protecting national security and public interests in data regulation. The Clarifying Lawful Overseas Use of Data Act (CLOUD Act) passed in the United States under the administration of Donald Trump and the General Data Protection Regulation (GDPR) passed in the European Union in 2018 acted as an external push for China's drafting of the DSL (DBAPPSecurity 2021). A data security law was needed for China to catch up in this regard to counter the influence of the CLOUD Act on acquiring data from US companies and institutions operating across the world, and to draw level with the GDPR as the model of data protection.

Data as Personal Information Should Be Properly Protected

The component of personal information protection was finally put into place in China's data governance system when the PIPL came into effect in November 2021. Prior to the drafting of the PIPL, previous laws and regulations in related fields already contained articles and clauses on protecting personal information in China. Articles on personal information protection can be found in the CSL, the newly revised Consumer Rights Protection Law, the E-Commerce Law, amendment no. 9 to the Criminal Law, and Civil Law Code. Beyond the data security concern, the drafting of the PIPL was spurred externally by the passing of the GDPR and internally by the increasingly louder voices calling for the protection of personal information from giant digital platforms in the emerging digital economy.

The PIPL exploited the GDPR for its articles and regulations on personal information protection. It stipulated informed-consent rules for privacy protection, protection of personal information from being abused by giant platforms, strengthened duties of personal information handlers, and guidelines for government and state agencies' access to personal information, even instructions for cross-border personal data flows. Different from the GDPR, however, the PIPL contains more constraints and stricter regulations on cross-border data flows in the name of cybersecurity and data sovereignty, including the requirements of passing a security review organized by the state cybersecurity and informatization department, obtaining individuals' separate consent, undergoing personal informational protection certification, data localization for critical information infrastructure operators and personal information handlers handling personal information reaching quantities provided by the state cybersecurity and informatization department. Plus, the PIPL does not differentiate between the definition of data "controller" and "processor," unlike the GDPR. The PIPL only stipulates a vague definition of "personal information handler," which could be interpreted in practice as individuals, organizations or state organs and institutions. This will cause confusion in law practices.

It seems that China has provided more personal data protection to its population than the United States did for its own citizens, since the latter does not have a single federal data and privacy regulation law yet (Nussipov 2020). However, the comprehensive definition of national security and the government's unilateral access to personal data in the name of national security or criminal investigation (article 35 of the DSL) and the lack of essential and effective constraints on government access to personal data (articles 63 and 64 of the PIPL), plus its almost ubiquitous mass digital surveillance equipment across China, all indicate that China's promise in the PIPL does not provide enough credibility to assure personal information would be properly protected against the state power in the country.

China's Data Governance Institutions

Cybersecurity and informatization has been held as one of the crucial areas in which President Xi positioned himself as the head to take direct control (He 2020). President Xi updated the existing Central Leading Group for Internet Security and Informatization to the Central Cyberspace Affairs Commission (CCAC) in 2018 and made himself its chief. The CCAC, as the highest power organ within the Chinese Communist Party, has its enforcement agency and office established in the central government echelon, the Cyberspace Administration of China (CAC).

The CAC, or the "State Internet Information Office" in the Chinese language, is China's powerful internet and information regulator in charge of regulation on a wide range of affairs, including cyberspace security, internet, and oversight and censorship of internet-related (online) information and data. In China's centralized, top-down bureaucratic system, the CAC and all the Internet and Information Offices at the provincial, municipal and other local levels, constitute a complex network of internet information and data regulation.

Data governance as part of the regulation of internet information falls within the jurisdiction of the CAC. The CAC had been deeply involved in promoting and drafting the three major laws on data regulations — the CSL, the DSL and the PIPL — and all related specific regulations and measures of implementation issued at different (national, ministerial) levels to enforce the laws.

The CAC coordinated its responsibility of internet information and data regulation with other party and government agencies such as the Central Publicity Department, the State Administration for Market Regulation (SAMR), the MIIT and so on. In the area of data governance, it also relies on some specialized agencies such as the standard-setting body, the Standardization Administration of China (SAC), for making identification guides for key data.

As the formidable internet regulator in China, the CAC's main duties focus on supervising security matters and internet information censorship in digital and data governance, while the responsibility to develop the digital economy falls under the jurisdiction of the NDRC, the MIIT and the Ministry of Commerce, three powerful government departments. All these government agencies, including the CAC, share parts of the duty of promoting the overarching goal of building a digital China. With data as the core engine for economic growth being increasingly recognized, the overlapping duty among different government agencies needs to be improved for better data governance to serve the goals of economic growth, national security and personal data protection under the all-embracing ambition of building a digital China.

The latest reforms on state and party institutions, announced in March 2023, established a new government agency, the National Data Administration (NDA) under the NDRC, to oversee basic systems for data and data valuation and to coordinate the goal of building a digital economy and digital society in China. The new agency integrated the responsibilities of coordinating informatization of public service, smart city projects and the development of information resources previously under the CAC and the duties previously shouldered by the NDRC in coordinating the development of the digital economy (national big data strategy and basic systems for data elements and digital infrastructure).

After the latest restructuring in state and party institutions, China's data governance regime is divided into a dual agency model, in which the CAC is in charge of data security-related issues, internet and online information censorship, and the NDA is responsible for data-based economic growth and information and data-based public services. The dual agency governance framework is expected to manage a dual goal of bolstering both economic growth and data security in China's data governance system.

A Dual Goal of Economic Growth and National Security

Data as the Core Engine for the Digital Economy and a Digital China

Data as a key element for economic growth has been further recognized after five years of development of the digital economy in the period of the 13th Five-Year Plan (2016–2020). Data has been defined as "the core engine driving the digital economy" (State Council 2021), and "the role of data as a factor endowment" (Xinhua 2021) has been established in China's most authoritative documents and guidelines for economic and social development (see Table 1).

The 14th Five-Year Plan (2021–2025)[1] (ibid.), which is China's overarching framework of economic and social development, defines building a digital China as its ultimate goal and calls for "tak[ing] full advantage of massive data to promote the in-depth integration of digital technology and the real economy, empower the transformation of upgrading of traditional industries, catalyze the birth of new industries"[2] to facilitate the realization of the goal. The role of data as a factor endowment is described as the crucial element to enable capacities for the digital transformation of traditional industries through the establishment of the industrial internet and centre for digital transformation, as well as digital industrialization such as artificial intelligence (AI), big data, blockchain, cloud computing and 5G-based smart industrial ecosystems such as smart cities, logistics, energy and health care.

China's central government, i.e., the State Council and relevant departments such as the CAC and MIIT, followed up and introduced specific documents in their jurisdictions to promote the top goal of building a digital China through deepening the development of the digital economy and establishing highly efficient data factor resource systems, strengthening national data governance and coordination, and building a nationwide integrated system for big data centres (see Table 1).

Serious challenges and hindrances exist in key areas of the big data industry, the overall data-enabled digital economy and the digital transformation of industries, society and public services, and the government's open data projects. These obstacles include the long-standing problem of data silos and fragmentation among different industries, sectors and government departments and agencies, a poorly performing and regulated data trading market and system because of a lack of standards and mechanisms in defining data rights, data circulation, data quality, data pricing and data trading.

To find solutions to these problems, the latest "data twenty measures," issued in December 2022, try to establish an efficient and compliant system of data circulation and trading markets and a well-performing data trading system. Whether China can fully tap the potential role of data elements and release its data-enabling role through the development of the big data industry and an efficient and competitive data trading system for the development of the digital economy will depend on the country's practices in the years to come.

Data Security at the Expense of Personal Data Protection

Data security, including strict regulations on cross-border data flows, data localization and the protection of source code, stands out in China's state-centric data governance regime. This can be seen clearly through the passing of the CSL and the DSL.

The CSL introduced the concept of cyber sovereignty and other noticeable data-related regulations, such as protection of data from being leaked, stolen or damaged (especially data from key information infrastructure facilities), data classification, and so on. Among these, the most striking feature of the law is data localization (article 37 of the CSL).[3] The DSL is a comprehensive law aiming to prevent national security, public

1 The full official name of the plan is the "14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035 of the People's Republic of China."

2 The English translation is cited from https://cset.georgetown.edu/wp-content/uploads/t0284_14th_Five_Year_Plan_EN.pdf.

3 See NPC (2016). An English version of the CSL can be found here: www.lawinfochina.com/display.aspx?id=22826&lib=law.

Table 1: Major Documents Promoting Data as a Key Element for Economic Growth in the 14th Five-Year Plan Period (2021–2025)

Title	Goal	Main Contents	Issued By	Date Issued
14th Five-Year Plan for National Economic and Social Development	Build a digital China	Data as a key factor for the integration of digital technology and the real economy, development of the digital economy in digital transformation of the industries and digital industrialization, and digitalization of public services and digital government.	The Party Central and the State Council	March 2021
Plan for Development of the Digital Economy during the "14th Five-Year" Period	Develop a competitive digital economy by 2025 and an advanced digital economy by 2035	Set major indicators for the development of the digital economy by 2025; upgrade digital infrastructure; cultivate data market and unleash data value; digital transformation of the industries and digital industrialization; digitalization of public services; improve governance for digital economy and engage in international cooperation in digital economy.	The State Council	December 2021
14th Five-Year Plan for National Informatization	Achieve decisive developments in Digital China and national informatization	Set major indicators for the development of informatization by 2025, including overall goal in Digital China and digital economy, digital infrastructure, innovation capacity for digital technology, industrial transformation, digital society, and government services.	CAC	December 2021
Outline for Big Data Development in the "14th Five-Year" Period	Develop the big data industry	Accelerating, nurturing and developing an efficient data element market; improving data quality, diversity, circulation and governance; growing the big data industry in infrastructure, technological innovation, standard setting, and a stable and efficient supply chain and a robust industrial ecosystem.	MIIT	November 2021
Data Twenty Measures[4]	Establish a database system to maximize a better role of data elements	Establish an efficient and compliant system of data circulation and trading markets; establish a well-performing data trading system; improve the governance efficiency and income distribution of data elements.	The Party Central and the State Council	December 2022

Sources: Xinhua (2021), State Council (2021; 2022), CAC (2021b), MIIT (2021).

4 The document contains 20 articles. Its full official name is "Opinions of the CPC Central Committee and the State Council on Establishing a Basic System for Data to Maximize a Better Role of Data Elements" (see State Council 2022).

interests or lawful rights and interests of individuals and organizations from being harmed if data is altered, destroyed, leaked or accessed or used unauthorizedly (article 21 of the DSL).[5] It also introduced and detailed data classification, which was regarded as the main feature of the law. However, its most noticeable component is establishing all-inclusive regulation over broad and vague definitions of important data and core data that constitute China's national security. This attribute has the potential to securitize data governance in China, in particular when it comes to cross-border data flows.

Data security has a different meaning in China compared to the definition of the term in Europe and the United States. In China, concepts such as data sovereignty, data control and jurisdiction over data have been more frequently raised. Accordingly, stricter restrictions on cross-border data flows, the requirement of data localization and protecting source code and other important data from being obtained by foreign forces and entities are at the centre of data security in China. Subsequently, national security, rather than personal information protection, is at the crux of China's data regulations and laws, which focus on protection of the broadly defined "important data" and "core data" that are deemed to concern China's national security and public interests.

Coming into effect three years after the CLOUD Act and the GDPR were adopted in 2018, China's DSL followed suit and established a similar extraterritorial jurisdiction on data governance as in the two regulations. Article 2[6] of the DSL stipulated that China has the similar extraterritorial jurisdiction over data control as in the CLOUD Act and the GDPR, extending its jurisdiction to data-handling activities beyond the border of China. As a reference, article 3 of the GDPR extends its jurisdiction to any data controller or processor in the European Union that processes personal data of subjects who are in the European Union, or any data controller or processor not in the European Union but that processes personal data of subjects who are in the European Union and the processing activities are related to offering goods or services to the subjects or monitoring the subjects' behaviour, regardless of whether the processing takes place in the European Union or not.[7] Article 36[8] of the DSL is deemed to counterbalance the CLOUD Act, which requires data providers subject to US jurisdiction to disclose data that is responsive to valid US legal process, no matter where the data is stored.[9]

Chinese laws and regulations consider protection of personal data as part of data security in a broad sense. Government regulators believe that through these laws and regulations, Chinese citizens' personal data would be protected from a wide range of external and internal threats, such as foreign entities and governments, hackers and terrorists, and platform giants. Both the PIPL and the DSL mainly regulate the collection of personal data by companies instead of the government itself. Following this logic, the government deems personal data protection as regulations and measures to protect personal data from being abused or leaked by big tech, institutions both within and outside China, and foreign governments, not from the Chinese government itself.[10] Sections 1 and 2 under chapter II of the PIPL stipulate many measures in this regard.[11]

The Chinese party-state, which tightly controls the whole society through its institutions and all levels of governments, has been trying to get access to data and grasp control of data as well. Before the DSL and the PIPL, there existed sporadic provisions in Chinese laws that granted governments access to data in a vague way, including the Constitution of the PRC, the Criminal Procedure Law, the CSL, the National Security Law, the National Intelligence Law and the Counter-espionage Law (European Data Protection Board 2019).

5 See NPC (2021a). An English version of the DSL can be found here: www.lawinfochina.com/display.aspx?lib=law&id=35666.

6 Article 2 stipulates that "When data handling activities outside the territory of People's Republic of China harm the national security, the public interests, or the lawful rights and interests of individual and organization, liability is to be pursued."

7 See article 3 of the GDPR here: https://gdpr-info.eu/art-3-gdpr/.

8 Article 36 stipulates that "Domestic organizations and individuals must not provide data stored within the territory of the PRC to the justice or law enforcement institutions of foreign countries without the approval of the competent authorities of the PRC."

9 See the official website of the US Department of Justice: "Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act" (www.justice.gov/criminal-oia/page/file/1153436/download).

10 However, the breach of a database that contains the personal information of as many as one billion Chinese citizens used by the Ministry of Public Security in Shanghai in July 2022 exposed the lack of protection of information collected and controlled by the government. See Lu (2022).

11 See NPC (2021b). An English version of the CSL can be found here: www.lawinfochina.com/display.aspx?id=36358&lib=law.

The articles and regulations in the DSL and the PIPL make it specifically clear that the government is granted more access through the broad and unclear definition of national security and criminal investigations, as well as protection of personal information (see Table 2). Article 35 of the DSL gives public security authorities and national security agencies access to data of any individual and organization on the basis of safeguarding public security and national security.

A few key articles in the PIPL allow the government greater access to personal data. Chapter II of the PIPL includes many provisions with the requirement to obtain consent from individuals before collecting and handling personal information, but it also includes a wide range of exceptions, with some exceptions covering a much more inclusive range of circumstances. Article 13 sets out six conditions under which obtaining individual consent in the handling of personal information is not required[12] (NPC 2021b). These conditions cover a wide array of situations, including responding to a public emergency such as public health incidents, involving an event concerning public interest, fulfilling statutory duties, and so on. The last condition specified in article 13, "other circumstances provided in laws and administrative regulations" (ibid.), is a typical "catch-all provision" in Chinese laws and regulations and could include a significantly broader range of scenarios.

Article 34 of the PIPL states that "state organs handling personal information to fulfill their statutory duties and responsibilities shall conduct them according to the powers and procedures provided in laws or administrative regulations; they may not exceed the scope or extent necessary to fulfill their statutory duties and responsibilities" (ibid).[13] It literally provides any state organ in China access to personal data due to the broad scope of "laws or administrative regulations" and vague definition of the state organ's "statutory duties and responsibilities." Article 63 lists a broad range of measures for government departments responsible for fulfilling personal information protection duties and responsibilities. These measures give government agencies almost unlimited leeway and discretion when dealing with personal data. The article further stipulates that "concerned parties shall provide assistance and cooperation, and they may not obstruct or impede them" where these departments are fulfilling personal information protection duties and responsibilities (ibid.), which double ensured the government's full access to personal data.

The Regulations on Network Data Security Management (draft for comments) released in November 2021, which is the implementation regulations of the DSL, grants the CAC, public authorities, national security agencies and other government departments the authority to supervise data security (article 55). Article 57 lists a broad range of means for these agencies to supervise and inspect data in the name of data security. The last item of article 57 specified "other necessary means provided in laws and administrative regulations and rules" (CAC 2021a), which, again, is a typical catch-all provision that could include a very broad range of means.

These above-mentioned articles fully demonstrate that as a strong state controlling everything, the Chinese government deems itself justified in getting access to all the data whenever the government believes it necessary for public security or public interest. Plus, with decades of operation of state surveillance programs such as Safe Cities, Skynet Project, Smart Cities and Project Sharp Eyes (He 2022), and increasing advanced facial recognition technology and other technologies, China's government has accumulated huge amounts of individuals' and private institutions' data, which greatly undermined the effectiveness of the laws protecting personal and private information. In addition, there are no significant articles and clauses clearly defined in these laws that provide individuals and the private sector enough protections against government intrusion.

The Dual Goal in China's Participation in Global Data Governance

China encourages international cooperation on the digital economy and participation in negotiations on rulemaking and standard setting in cyberspace governance, data governance, digital trade and the digital economy through international organizations and multilateral

12 Judging from the structure of chapter II and the whole PIPL, as well as the unclear definition of personal information handler in the attachment chapter, state organs are considered personal information handlers and article 13 applies to state organs.

13 An English version of the PIPL can be found here: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/.

Table 2: Key Articles Securing Government Access to Personal Data

Law or Regulation	Article	Provision and Its Implications for Government Access to Data
PIPL	13	Items 2–7 define a wide range of conditions under which obtaining individual consent in the handling of personal information is not required.[14] Item 7 as a catch-all provision, in particular, could include even broader ranges of conditions.
	33	Empowers state organs to handle personal information under the PIPL.
	34	Authorizes state organs to handle personal information according to the powers and procedures provided in laws and administrative regulations within their statutory duties and responsibilities. None of the powers, procedures, laws, regulations and statutory duties and responsibilities are clearly defined, which gives state organs extensive power to handle personal information.
	60	Empowers the CAC, all departments under the State Council, and all county-level and higher governments to get access to personal data in the name of protecting personal information.
	63	Lists a wide range of measures that government departments can take to fulfill personal information protection duties and responsibilities. These measures would then allow them to get access to personal information.
	64	Authorizes government departments to interview personal information handlers or to require them to entrust specialized institutions to audit their personal information handling activities.
DSL	35	Authorizes public security departments and state security agencies to access data of any individuals and organizations to safeguard national security or investigate crimes.
Regulations on Network Data Security Management (draft)	55	Grants government, including the CAC, public security authorities, national security agencies and other government departments the power to supervise data security.
	57	Lists a broad range of means for these agencies to get access to data in the name of supervising and inspecting data security. The last item in article 57 as a catch-all provision could include even broader ranges of means to get access to data.

Source: Author's analysis based on the text of the PIPL, the DSL and the Regulations on Network Data Security Management (draft for comments).

14 See footnote 12 on page 8.

mechanisms. Its top-level official documents (see Table 1) listed the priorities in China's participation in global digital governance, including building international cyberspace governance mechanisms,[15] the development of digital trade, deepening the Digital Silk Road (DSR) initiative, and engaging in rulemaking on data security, cross-border data flows, market access, digital currency, data privacy protection and so on.

China has updated its policies on global data security governance in the Global Initiative on Data Security announced in September 2020. Except for repeating its stance on respecting the state's "sovereignty, jurisdiction and governance of data," China stated in the initiative that "states should not request domestic companies to store data generated and obtained overseas in their own territory," "states shall not obtain data located in other states through companies or individuals without other states' permission" and "ICT products and services providers should not install backdoors in their products and services to illegally obtain users' data, control or manipulate users' systems and devices" (Xinhua 2020). China made clear that the initiative is its commitment to protecting global data security (Ministry of Foreign Affairs of China 2020) and advocated for it on a number of occasions, including the G20 Leaders' Summit in 2020 and the recent first-ever China-Central Asia Summit in May 2023 (Ministry of Foreign Affairs of China 2023a).

The three principles calling for states to refrain from demanding overseas data via their companies operating abroad are included in China's Positions on Global Digital Governance, which was issued on May 25, 2023, as China's contribution to the United Nations' Global Digital Compact. The position paper emphasizes China's support for the United Nations playing a leading role in global digital governance and rulemaking. Notably, the position paper promotes 10 proposals for regulation of AI, including a people-centred approach and the principle of AI for good, priority for AI ethics, and algorithm security and controllability in AI research and development (Ministry of Foreign Affairs of China 2023b).

The Global Initiative on Data Security was interpreted in Western media as China's effort to set global rules on data security governance (Wong 2020; Tiezzi 2020). The interpretation was not wrong, but it neglected the main message the Chinese government wanted to convey in the initiative, which was a response to the long-standing criticism from Western countries that the Chinese government has been mandating access to overseas data held by Chinese tech companies operating abroad, including through the DSR initiative. With their digital technologies and equipment in facial recognition, video surveillance and smart city solutions, Chinese companies including Huawei, Hikvision, Uniview, Megvii, CloudWalk, Dahua and Yitu operated in some Belt and Road Initiative (BRI) countries (He 2022) and might have accumulated a vast amount of data from these countries (Council on Foreign Relations 2021). Chinese tech firms including Huawei have been accused of sharing data with the Chinese government through their construction of digital infrastructure in Nigeria and of transferring data back to servers located in Shanghai (Hungerland and Chan 2021; Sodiq Omolaoye 2022).

The Chinese government intended to clarify through the initiative that it will never ask Chinese companies to hand over overseas data they collected via their operation, and China will not ask its companies such as ByteDance to store or process data they collected overseas in China's territory, and that China does not allow its information and communications technology companies, such as Huawei, to install backdoors in their telecommunication equipment, products and services. But it seemed that the main message was not well received in the West. The lack of trust surrounding the Chinese government's self-claimed withholding from demanding data from Chinese companies operating overseas can probably explain the gap in understanding between the West's interpretation and the Chinese government's main point. With regard to China's tech giants, Huawei, for example, has been struggling on its own to convince Western countries that Chinese law, including the National Intelligence Law passed in 2017, does not empower China's government to plant "backdoor" eavesdropping devices or spyware in telecommunications infrastructure.[16]

At the same time, China keeps a close eye on the practices of Europe and the United States in terms of data governance while developing its own data governance system. The views of researchers

15 It refers to "building peaceful, secure, open, cooperative and orderly cyberspace community with a shared future" in the Plan for Development of the Digital Economy during the 14th Five-Year Period.

16 See www.huawei.com/nz/facts#Question_Answer.

and scholars shed light on the reasoning behind China's participation in global data governance by revealing that data security and data's fundamental role for bolstering trade and economic growth are clearly the two priorities China should pursue.

Although they perceive that the United States has followed a core principle of supporting data free flows globally and the European Union is developing a unified digital market to encourage free data flows within the European Union, Chinese researchers and scholars see that articles or regulations are included in both US and EU laws to seek extraterritorial jurisdiction to extend the government's capabilities to acquire data overseas (Fu 2019). For example, the Foreign Investment Risk Review Modernization Act of 2018 and the Committee on Foreign Investment in the United States required foreign companies invested in the United States to restrict export of data concerning citizens' sensitive information, privacy or key data in core industries such as telecommunications and technological parameters (Congressional Research Service 2020; Fu 2019).

Therefore, China should push for global data flows in a safe and ordered way, which means properly regulated cross-border data flows, for its own sake (NPC 2021a; Fu 2019; Que and Wang 2022; Liang, Zhang and Yu 2022). A safe and ordered global data flow serves China's interests in engaging and benefiting from global digital trade and economic development, maintains China's advantages in processing enormous data resources (Fu 2019; Que and Wang 2022; Liang, Zhang and Yu 2022) and bolsters China's DSR initiative (Fu 2019; Zhang 2020; Zhou and Yao 2021; Chen 2021). These Chinese researchers and scholars understand China is not alone by noticing that developing countries such as Brazil, India, Russia, Saudi Arabia, South Africa, Türkiye and Vietnam also tend to impose regulations and rules on restricting data export and advance data localization with national security as the top priority (Fu 2019; Liang, Zhang and Yu 2022).

Based on their understanding of data governance models in the United States and the European Union, they argued that China should prioritize developing a powerful data-based digital economy (Fu 2019) while balancing the use of data for economic development, individual information protection and national security in developing China's data governance model. Learning from the European Union's experiences, China should establish and improve its rules and regulations for data classification and export and integrate with the international governance system for cross-border data flows (Fu 2019; Zhang 2020; Que and Wang 2022; Liang, Zhang and Yu 2022).

Judging from the Global Initiative on Global Data Security and China's Positions on Global Digital Governance, the two latest documents China issued on global data governance, the Chinese government has been placing more emphasis on the national security element than the goal of economic growth in recent years. However, economic growth is still the indispensable part in China's dual goal in data governance that seeks to bolster both security and development, and China's Positions on Global Digital Governance emphatically advocated focusing on development as one of the basic principles for China's idea on global digital governance.

The dual goal of pursuing both economic growth and national security at the expense of personal information protection can be illustrated in two (mostly) noticeable areas in data governance: digital platform governance and cross-border data flows. The following two sections provide case studies to demonstrate this feature.

Digital Platform Governance

How to strike a balance between security and development is an important matter in the evolution of China's state-centric data governance regime. Chapter II in the DSL specifies measures to handle the balance in an effort to make the two aspects mutually beneficial to each other (NPC 2021a). Governance of digital platforms, a key topic that involves economic growth, national security and personal information protection, stands out as a central issue in data governance. While loaded with responsibility on data security compliance under the strict and comprehensive requirements in the DSL and other regulations, digital platforms, as data processors, are expected to help boost the digital economy to serve the ultimate goal of building a digital China.

Digital platform governance in China experienced a business-friendly regulatory environment

before 2020, tight regulation — even regulatory crackdown — between 2020 and 2022 and a slight relaxation of regulation since the beginning of 2023. Before 2020, the need for e-commerce and digital platforms to promote economic growth explains the pro-business regulatory environment for platforms, and, since 2020, national security concerns and personal information protection justify the regulatory crackdown on these platforms.

China has developed its own governance model based on its understanding of the experiences of the United States and the European Union. In China's understanding, platforms, with the nature of quasi-public goods, play important economic and societal roles in acting as infrastructure (China Academy for Information and Communications Technology 2019). Platforms assume the burden of so-called non-comprehensive liability of reviewing content on the platform, which refers to establishing supervision and inspection mechanisms and technological monitoring tools and means required by government for reviewing platform content and addressing illegal content in time. On the condition that these required mechanisms and technological tools are in place and perform well, platforms are deemed to have immunity. Under these circumstances, platforms will not be legally responsible for individual cases of infringement or other forms of illegal activities. On the issue of platform monopoly, Chinese regulators take a similar tolerant, cautious and innovation-prioritized approach to their American counterparts while regulating the platforms with the Anti-unfair Competition Law, the Anti-Monopoly Law and the Law of the People's Republic of China on the Protection of Consumer Rights and Interests.

China's pro-corporate tendency and practices in platform governance created a platform-friendly regulatory environment, which greatly boosted China's thriving huge platforms such as e-commerce giant Alibaba, and other types of platform companies such as Baidu and Tencent (Hong and Xu 2019). Since 2015, these giant platforms have expanded and touched almost every corner of China's economy and society and have contributed to China's growth by bolstering the digital economy in China (He 2021). In the years that followed, these digital platforms aspired to compete with world digital powers such as Google, Facebook and Amazon, reaching their heyday in 2019 before the Chinese government began its regulatory crackdown on these giant tech platform companies in 2020–2021 out of concerns over their increasingly growing control of data and influence on China's economy and society.

It was at this time that the government's strategies and policies toward large tech platforms pivoted. Through anti-trust laws and competition policy, three data-related laws (CSL, DSL and PIPL) and other national policies such as "common prosperity," the government has increasingly tightened its control over these big platforms since 2020–2021, ensuring they are not becoming too powerful to endanger the government's ruling and control over data, economy and society.

On the one hand, large digital platforms are deemed as internet operators, data handlers and even critical information infrastructure (CII) operators that shoulder duties and responsibilities to safeguard cybersecurity and data security. The CSL stipulated a variety of duties and responsibilities for internet operators and CII operators on safeguarding internet information security while the DSL lays down similar duties and responsibilities for data processors (handlers) and CII operators to protect data security. The Critical Information Infrastructure Security Protection Regulation released in July 2021 defines the CII as important network infrastructure and information systems in key industries and sectors such as public telecommunications and information services, as well as where their destruction, loss of functionality or data leakage may gravely harm national security, the national economy and people's livelihood, or the public interest (State Council 2021).[17]

With respect to the specific scope of CII, article 31 of the CSL stipulates that the State Council will formulate it (NPC 2016), but it is still not available. But the Guidance for Identification of Critical Informational Infrastructure, which is in the attachment of Guidance for Operations of National Cybersecurity Check made by the Bureau of Cybersecurity Coordination of the CAC in June 2016, is the document that has the most referential importance so far in identifying the scope of CII. It defines any platform that has more than 10 million subscribers or more than one million active subscribers (log in at least once per day) or the value of daily trading volume or confirmed order surpassing 10 million yuan as CII.

17 An English version of the regulations can be found here: https://digichina.stanford.edu/work/translation-critical-information-infrastructure-security-protection-regulations-effective-sept-1-2021/.

On the other hand, large digital platforms are required to undertake great responsibilities in protecting personal data under the PIPL. Article 58 of the PIPL specifically regulated the duties in protecting personal data for personal information handlers who provide internet platforms services and have a large number of subscribers and complex structure in the types of businesses. Regulations on Network Data Security Management (draft for comments) details duties and responsibilities for data processors in the protection of data security. In particular, data processors such as large platforms handling important and core data or massive data and personal information are required to report to the CAC for security review and to establish stricter internal mechanisms for data security protection.

The regulatory crackdown on large digital platforms has been carried out since 2020 in the name of both anti-monopoly and protection of national security and personal data. The enormous power and regulatory authority of China's Anti-Monopoly Law has been fully demonstrated in the symbolic sky-high fine of 18.3 billion yuan on Alibaba in April 2021 (Associated Press 2021) for its practice of forcing merchants to sell exclusively on its platform (commonly known in China as "pick one from two"). The regulatory crackdown on ride-hailing giant Didi Chuxing was deemed as another example meant to showcase the state control over data, in particular tight control over cross-border data flows, after the DSL was passed in June 2021.

Didi infuriated the Chinese regulatory authorities in June 2021 by ignoring their warning and launching its initial public offering (IPO) in the New York Stock Exchange (NYSE). The CAC announced the launch of a "cybersecurity review" on Didi two days after the IPO and suspended Didi's new users' registration, which was a heavy blow for the company, and unfolded a one-year cybersecurity investigation, with Didi being forced to delist from the NYSE on June 10, 2022. One month after that, the CAC announced the final result of a security review on Didi: a huge fine of 8 billion yuan for Didi's illegal handling of 65 billion pieces of personal information and its "data handling activities severely negatively affecting national security" (CAC 2022b).

The CAC did not specify which data collected by Didi was security sensitive but claimed the company's data-handling behaviours had violated the CSL, the DSL and the PIPL and brought severe security risks on China's CII and data security. The CAC's announcement implied that the Didi platform belongs to CII, which is the concept defined in the DSL, and that any data of CII should go through security review before it can be exported outside of China. It appears that taking more control over data from the hands of large tech platform companies in the name of national security and protection of individual data was at the crux of CAC's crackdown on these tech companies.

Facing economic difficulties in the aftermath of the COVID-19 pandemic, China has again reversed course and taken measures to encourage and support the growth of the platform economy. A symbolic move was the announcement in January 2023 by the central bank at a news conference organized by the Information Office of the State Council that corrective actions against 14 large platform enterprises have been accomplished (China News Services 2023). Three days later, Didi announced it would resume its user registration after comprehensive corrective actions. Combined with the announcement of the Central Economic Work Conference in December 2022 that declared the government's support for platform companies to fully display their capabilities to lead economic growth, provide job opportunities and engage international competition, it is clear that the government has finished the regulatory crackdown on digital platform giants and is confident that these companies have been under proper government surveillance and regulations.

A crucial role of the powerful government has been seen in China's governance of digital platforms in terms of economic development, data security and personal data protection. A pro-business regulatory environment had helped boost the wild growth of the platform economy that contributed to economic development and creation of job opportunities while the unprecedented stress placed on data security and the resulting tight regulation to address concerns of national security and personal information had held back the big digital platforms' growth. Personal data protection has been incorporated into the broad sense of data security. With the key articles in the major laws in data governance, including the DSL and the PIPL, the government possesses mostly free rein to access all data including personal data held by large digital platforms in the name of protecting data security for the public interest and national security.

Regulations on Cross-Border Data Flows

Cross-border data flows are essential for the development of the global digital economy, which would create enormous economic wealth and add value in unleashing innovation potential and bolstering social benefits.[18] While recognizing these great potential gains and seeking solutions to relax restrictions on cross-border data flows, Chinese policy makers are more concerned about the possible significant negative impact cross-border data flows could bring on national security and are emphasizing the safe side of free flows of cross-border data.

The broad and strict rules on cross-border data flows can be found in China's current laws and regulations. These include:

- the CSL, effective June 1, 2017;
- the DSL, effective September 1, 2021;
- the PIPL, effective November 1, 2021;
- the Measures of Security Assessment for Data Export, released by the CAC on July 7, 2022, and effective September 1, 2022 ("the Measures"); and
- the Regulations on Network Data Security Management (draft for comments), released by the CAC on November 14, 2021 ("the Regulations").

These broad, strict regulations to limit cross-border data flows are made in the name of national security or public security. A major issue of China's regulations on cross-border data flows is that many key definitions in China's laws are loosely or vaguely defined, such as data classification categories and guidelines on what constitutes "important data" and "national core data" in its three data-related laws, the DSL, the PIPL and the CSL.

Further specific regulations have been made in the Measures and the Regulations on the basis of these three data-related laws, to address some of the loosely or vaguely defined issues. On the crucial question of under what circumstances a national data security review should be applied before data could be exported, article 37 of the Regulations (CAC 2021a) and article 4 of the Measures (CAC 2022a), plus article 37 of the CSL (NPC 2016) and article 40 of the PIPL (NPC 2021b), say that a review would be needed for:

- any data handler that provides important data or more than 100,000 pieces of personal information or 10,000 pieces of sensitive personal information;
- any personal information and important data collected and produced by a CII operator;
- any export data that includes important data;
- any data handler that handles more than one million pieces of personal information; and
- other situations defined by the CAC.

Beyond these articles, the regulations and terms are otherwise not clearly defined. The definition and scope of "important data" described in the Regulations is still far more comprehensive, covering almost all walks of life in China's society (CAC 2021a). The definition of "core data" in the Regulations is also vaguely stated (ibid). Accordingly, restrictions on cross-border data flows are widely considered necessary in the name of supervision or public security and are applied. Furthermore, what is a "data processor" is defined differently in different laws and regulations.

To make these regulations on data export practicable for businesses, data processors and regulators themselves, Guidelines for Application for Security Assessment for Data Export was released by the CAC on September 1, 2022 (CAC 2022c), the same day the Measures was put in effect. Two months before this, the CAC (2022d) circulated Provisions on the Standard Contract for Exports of Personal Information (draft for comments). China's National Information Security Standardization Technical Committee on Information (SAC/TC 260) under the dual leadership of the SAMR and the SAC, issued the latest Information Security Technology-Guideline for Identification of Important Data (the "Guideline") on January 7, 2022 (SAC/TC260 2022).

The Guideline, which listed only six general principles and 14 factors used to identify what is important data (CAC 2022c), is still too expansive

18 This section relies in part on the author's CIGI opinion piece on China's cross-border data flows: www.cigionline.org/articles/trade-deals-might-induce-beijing-to-bend-on-data-restrictions/.

and comprehensive to recognize "important data." Too much data could still be classified into important data, and more detailed standards and specific guidelines for each region or province, each industry and each sector in society need to be made. Besides, both the Guideline and Regulations are drafts for comments, and are not coming into effect yet.

Clearly, safeguarding national security or public security stands as the prioritized goal of strict regulations on cross-border data flows, and specific regulations and measures are made for data processors, in particular, large digital platforms, for their handling export of data. At the same time, seeking means to facilitate cross-border data flows and unleash the value of data to promote trade and economic growth is being put in an equally important place.

In principle, China allows and even encourages the free flow of data across its borders. Article 11 of the DSL stipulates the principle of encouraging China to participate in international rulemaking and standard setting concerning data security and to "promote the safe and free flow of data across borders" (NPC 2021a). Article 41 of the PIPL (NPC 2021b) and article 36 of the DSL (NPC 2021a) both state that China's "responsible agencies" should adhere to relevant laws and international agreements or treaties China has signed or joined to provide data requested by law enforcement agencies from other countries.

These articles principally nudge open the door for China to take a flexible position on implementing international regulations on the free flow of data across borders. Article 38 of the Regulations further opened the door for China to compromise on its restrictions on cross-border data flows. It stipulates that China can follow the regulations of international agreements or treaties China has signed or joined to "provide personal information outside of the territory of the People's Republic of China" (CAC 2021a).

Reforms that would enable the free or more liberalized flow of data across China's borders are needed. They will need to be accelerated by external pressure, as shown by the often-cited logic of ushering in external pressure to push forward difficult domestic reforms, as China did in the 1990s when negotiating to join the World Trade Organization (WTO). This could be an important rationale behind China's submission to join the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the Digital Economy Partnership Agreement (DEPA), to which China officially submitted its applications to join in September and November 2021, respectively.

Given the announcements were made by President Xi himself, who enjoys absolute power and fully controls policy making, it seems China is determined to join these two agreements, each of which has considerable influence on international trade in the digital age. In a country where political calculation and economic considerations inevitably prevail over laws and regulations, the top leader's engagement likely would provide enough leeway to overcome the seemingly insuperable difficulties facing China's entry into the two treaties. Plus, the latest "data twenty measures" (see Table 1) contain detailed measures to establish safe, compliant and ordered mechanisms for cross-border data flows, which indicated China's recognition and determination to treat data as a factor of production to boost international trade and economic growth. If well established, these mechanisms for cross-border data flows could help reduce unexpected changes, even clampdowns in regulation, and other uncertainties that diminish incentives to invest.

Geopolitically, China needs to join these treaties to engage in international rulemaking in the digital economy. The country has lagged in this area. The status of rules collaborator would help Beijing become more relevant when competing in the global marketplace. In any case, continuing strict restrictions on cross-border data flows effectively prevents Chinese digital platforms, such as Alibaba or Tencent, from becoming large international internet firms like Google or Facebook.

More flexible measures and practices are needed to smooth the way for China to join the CPTPP and the DEPA. The pressure brought by the CPTPP and the DEPA is expected to push China to improve its data governance in terms of the level of precision and effectiveness of its regulations. Cross-border data flows are one challenge that has no obvious solution if China is serious about joining the CPTPP and the DEPA. Although the gap between China's existing obligations in the Regional Comprehensive Economic Partnership (RCEP) and the new obligations in both the CPTPP and the DEPA is not that wide (He and Fay 2023), China still needs to show enough flexibility on the difficult topic and try to bridge the gap in future negotiations to join the CPTPP and the DEPA. At present, China's exploration of solutions to relax cross-border data flows is basically theoretical or proceeding extremely slowly.

Chinese researchers and scholars in the area of cross-border data flows have suggested some ideas to make the data export workable. Two basic principles, precision and effectiveness in classification and restrictions of types of data on cross-border data flows regulations, have been put forward as a way of introducing several crucial reform measures to relax China's restrictions in this regard (Chen 2021).

The first recommended reform is to create multiple means or mechanisms to facilitate cross-border data transfer: for example, by establishing independent certification bodies to regulate cross-border data flows, similar to those defined in the GDPR, and by following the practice of the Standard Contractual Clauses adopted by the European Commission (tools designed to provide practical guidance on data transfer and efforts to comply with data protection laws), to build China's own standardized and pre-approved model data protection specifications (Chen 2021; Zhou and Yao 2021). In China's case, perhaps standards made by quasi-state trade associations in a certain industry could be applied to regulate cross-border data flows concerning this industry.

A second reform proposed is an improved data classification management system to expand the scope of general commercial data that can flow freely without national data security review. In this regard, a once-and-for-all solution is to establish a negative list that specifies "important data" and "data on national security" such as data pertaining to national defence, geography, oceans, finance and so forth. For any data not on the list, its free flow would be allowed (Peng 2020; Zhang 2020; Chen 2021; Zhou and Yao 2021; Wang 2021; Liang, Zhang and Yu 2022).

A third reform would be a streamlined national security review system for cross-border data flows, giving more weight to enterprises' self-review and providing for mutual recognition between certain countries in terms of data security review standards. Data would be allowed to flow freely between China and these recognized countries, which would be put on the "whitelist," a concept borrowed from the GDPR (Zhang 2020; Chen 2021; Zhou and Yao 2021).

If there is a road map for the possible easing of restrictions on cross-border data flows, it is likely to be China's past experiences in the decades of reform and opening-up policy commenced at the end of the 1970s. That is, drawing on these experiences, China might promote cross-border data flows in its free trade zones (FTZs) first, then spread these practices nationwide later. FTZs are defined as testing grounds, in which different policies and regulations are allowed in to promote economic growth. Indeed, pilot programs for cross-border data flows in the FTZs of Shanghai and Hainan are already under way. Trial programs in negotiating bilateral free trade talks with the United Kingdom or certain countries under the BRI framework are also being discussed (Peng 2020; Zhang 2020; Chen 2021; Zhou and Yao 2021).

For the requirement of data localization, China could also use the same logic adopted in FTZs to create a special supervision zone or "digital customs territory," in which entities such as data centres, cloud service providers and digital platforms could be treated with a "special supervision status" (Peng 2021). For example, a data centre, cloud service provider or digital platform located in a special FTZ or in a virtual location in cyberspace could be deemed as being outside traditional customs territory, and thus enjoy the free flow of data. In this way, a special supervision status could be created.

Furthermore, the Measures that came into effect on September 1, 2022, defined two scenarios that belong to "data export" (CAC 2022a) while the SAC/TC260 (2017) listed two case scenarios that are excluded as "data export." Combing the two rules together could help the operation of these data centres, cloud service providers and digital platforms in China to identify which data can or cannot be exported. The two excluded scenarios are "export via the territory of the People's Republic of China (PRC) of individual information and important data that are not collected and generated within the territory of the PRC and not changed or not processed," and "individual information and important data that are not collected and generated within the territory of the PRC but stored and processed within the territory of the PRC while not connected with individual information and important data that are collected and generated within the territory of the PRC" (ibid.). What is more, the Regulation does not explain what situation belongs to "collected and generated within the territory of the PRC" (Xue 2022), which would further open the door for Chinese or foreign-owned data centres, cloud service providers and digital platforms to operate within China and export data outside China without having to request permission for data export, as long as the data they processed is not concerning Chinese citizens' individual information and important data of China.

In sum, protecting data security or national security and promoting trade and economic growth are the two dominant goals in China's regulations and

the following reform measures on cross-border data flows. Compared to the GDPR, the PIPL's and the DSL's restrictions on cross-border personal information flows are stricter and have requirements for localization for processors (platforms) handling large amounts of personal data. More reforms are needed to unleash the power of data as a factor of production on cross-border data flows to boost China's foreign trade and deepen its engagement in global trade. However, again, the strict regulations on the cross-border export of personal data are aimed at the processors (platforms). They do not contain any essential constrictions on the government or state agencies' access to personal data. Governments have mostly unlimited access to all personal data based on the key articles in the PIPL and the DSL. In addition, the unclear definition of personal information processor in the PIPL also gives the government broad discretion to get access to personal data.

Implications of China's State-Centric Data Governance

The formation of China's data governance regime and its future development are expected to have a large impact on the data-based global digital economy. If China's government-dominated data regulation regime evolves into a gradually opening process and achieves balanced development among economic growth, national security and personal data protection, its global impact could be equivalent to the one brought by China's entry into the WTO two decades ago. However, if the country's strict regulation on cross-border data flows based on national security concerns continues, the ongoing "splinternet" trend underlined by the trade and technological decoupling between the United States-led West and China would be reinforced.

State-Centric Data Governance at the Expense of Personal Data Protection

How to balance economic growth, national security and individual data protection is a tricky issue that has long existed in data governance. China is pursuing the dual goal of bolstering national security and economic growth in its state-centric data governance system, while the government's access to all data including personal data is secured in the name of public security and criminal investigation. Concern over data security is prioritized. Particularly under China's top leader Xi's rule, security and ideological issues receive greater emphasis while, in practice, economic growth is an equally important goal being pursued under the Chinese government's top-level policy guidance. The stability-obsessed ruling style under President Xi's top-down approach probably would not help balance these different policy goals. The highly concentrated power and full control over policy making under Xi have generated new problems and aggravated the existing bureaucratic problems in China's policy execution (He 2020). For example, it could lead to inexplicable contradictions in policy implementation, as shown in China's policy toward foreign companies operating in the country in the post-pandemic era. While repeatedly "committed to promote high-standard opening up" and to "attract foreign investment," China's security officials are increasingly raiding and investigating foreign companies in the name of national security concerns and have raised panic among these companies.[19]

The protection of individual personal information against big companies and digital platforms is reinforced in data governance but so is the government's mostly unfettered access to all data, including personal data. There are no reasons to be optimistic that the government, in particular the governments at the local levels, will improve governance and build enough capacity to protect personal data, nor are there incentives for it to do so. There are not many restrictions on state power, and not enough impetus and capacity for the government to protect personal data, but more measures and means for the government to get access to personal data in the name of supervision. The characteristics of China's surveillance state equipped with increasingly advanced digital technologies would further compromise protection of personal data in the country.

Perhaps it is time for China to consider what the role of personal data protection means, ultimately, for its ability to harness data for economic growth and development. Is personal data protection a necessary condition for economic growth or is it more about human rights? It seems like allowing the trusted sharing of data with the private sector

19 See Wakabayashi, Swanson and Hirsch (2023).

is necessary for economic growth. Under China's current approach, personal data protection in businesses is gaining ground but is still vulnerable when facing the state power. China's state-centric data governance is achieving its national security objectives but at the expense of personal data protection, which could affect the goal of economic growth and trade development as well. Overstressed national security concerns and strict restriction on cross-border data flows would create uncertainty on data, including personal data protection, and scare off investment, competition, innovation and economic growth driven by businesses.

Catch-22? Tight Regulations on Large Digital Platforms Costing Economic Growth

A fundamental question that needs to be explored in data governance is how the enormous amount of data large internet companies (platforms) possess should be properly governed. In China's case, what has been revealed in the evolution of the state-centric data governance regime in recent years is a clear picture that data processors (platforms and other businesses) are facing stricter restrictions in dealing with data in their business practices while the government is capable of getting mostly free access to all data, including personal data in the name of national security and public interest.

China has passed national laws and regulation to oversee data governance on large digital platforms. However, the even trickier thing in China's state-centric data governance regime would be the implementation of these laws and regulations. The inconsistent regulatory environment caused by political and economic calculation in the government's policy and law implementation has had significant negative impact on the development of large digital platforms. Regulatory environments can change overnight due to political factors, as evidenced by the regulatory crackdown on China's big tech since 2020 and the dramatic end of Beijing's draconian zero-COVID policy in November 2022.

There is no guarantee that a similar regulatory crackdown would not happen again. The recent relaxation or adjustment of the tough regulations on platforms is mainly based on a short-term economic calculation instead of on platforms' performance on the protection of personal data. Chinese leaders and regulators prefer to adopt the dialectical thinking in striking a balance between the dual goal of bolstering national security and economic growth and justify their abrupt change of course in the state-centric data governance. The urgent need to boost economic growth in a particular period could lead to relaxation of implementation for data security compliance, and, vice versa, political calculus could generate tightened regulations on large digital platforms in the name of data security concerns. Yet the uncertainty created by ever-changing regulations is in and of itself one that would dampen economic growth.

Possible Compromises on the Regulation of Cross-Border Data Flows in China

Cross-border data flows are increasingly important in today's data-based digital economy, but a lack of consensus on approaches for governance of data flows that cross borders at national, regional and international levels is hampering the data-driven digital economy and likely imposing a significant negative impact on global economic growth. This is also likely the case in China.

China's official submissions to join the CPTPP and the DEPA and possible negotiations could generate changes to China's approach on cross-border data flows regulations in a way that is more in line with the United States and the European Union. China might gradually nudge the door open for less strict data regulations under the pressure brought by future negotiations for joining these treaties. Different from the RCEP, high-standard trade agreements such as the CPTPP and the DEPA are expected to play important roles in pushing China to seek creative approaches and possible solutions to compromises on crucial issues such as data localization and cross-border data flows in data governance. If progress on China's negotiations for joining these trade agreements could be made in the future, it could help promote new forms of global cooperation on data governance and include developing countries in global policy discussions on governing cross-border data flows. In the context of China's strict state-centric data governance model, any breakthrough on the regulation of cross-border data transfer could first happen in the experimental program such as the FTZs.

Convergence of Data Governance Regimes?

While the likelihood of fragmentation and competition among various governance regimes is increasing, a micro trend of convergence is happening among the main three governance approaches of the United States, China and the European Union. Seen from the Chinese perspective, the country has learned and is continuing to learn from the United States and the European Union and has developed its own rules, including laws, regulations on digital platform governance and personal information protection. In particular, China incorporated a lot from the GDPR for its regulation on personal data protection, which can be clearly seen from articles of the PIPL. Even in the difficult area of cross-border data flows, there is a glimmer of convergence in the main three governance approaches of the United States, China and the European Union, although there remains substantial path dependence that the data realms will continue to dominate. For instance, the suggestions in China's academic circle reveal many cases of China learning from the EU regulations on cross-border data flows such as the Standard Contractual Clauses, the "whitelist" and data classifications.

Certainly, the slight trend of convergence is more technical rather than essential. Blocking personal data flows on national security concerns is gaining strength in the United States, and the state's unfettered access to personal data in China is further guaranteed with the passing of the newly revised Counter-Espionage Law in April 2023, which expands the authorities of state organs in gaining access to any data, including personal data, in the name of anti-espionage investigation and cracking down on national security threats.

Works Cited

Associated Press. 2021. "E-commerce giant Alibaba fined $3.5B over China's anti-monopoly rules." CBC News, April 9. www.cbc.ca/news/business/alibaba-fined-anti-monopoly-1.5982642.

CAC. 2021a. "网络数据安全管理条例 (征求意见稿)" [Regulations on Network Data Security Management (Draft for Comments)]. November 14. www.cac.gov.cn/2021-11/14/c_1638501991577898.htm.

———. 2021b. "十四五" 国家信息化规划" [The 14th Five-Year Plan for National Informatization]. December 27. www.cac.gov.cn/2021-12/27/c_1642205314518676.htm.

———. 2022a. "数据出境安全评估办法" [Measures of Security Assessment for Data Export]. July 7. www.cac.gov.cn/2022-07/07/c_1658811536396503.htm.

———. 2022b. "国家互联网信息办公室有关负责人就对滴滴全球股份有限公司依法作出网络安全审查相关行政处罚的决定答记者问" [Press Conference of responsible officials in the CAC on the decision of imposing administrative penalty related to cybersecurity review on Didi Global Inc.]. 国家网信办 [cac.gov.cn], July 21. www.cac.gov.cn/2022-07/21/c_1660021534364976.htm.

———. 2022c. "数据出境安全评估申报指南(第一版)" [Guidelines for Application for Security Assessment for Data Export (First Version)]. August 31. www.cac.gov.cn/2022-08/31/c_1663568169996202.htm.

———. 2022d. "个人信息出境标准合同规定(征求意见稿)" [Provisions on the Standard Contract for Exports of Personal Information (Draft for Comments)]. June 30. www.cac.gov.cn/2022-06/30/c_1658205969531631.htm.

China Academy for Information and Communications Technology. 2019. 互联网平台治理研究报告(2019年) [*Internet Platform Governance Report 2019*]. March. www.caict.ac.cn/kxyj/qwfb/bps/201903/P020190301352676530366.pdf.

China News Service. 2023. "央行: 蚂蚁集团等14家大型平台企业整改已基本完成" [Central Bank: Corrective actions against Ants Group and 14 large platform enterprises have been basically completed]. *中国新闻网* [Chinanews.com], January 13. www.chinanews.com.cn/cj/2023/01-13/9934611.shtml.

Chen, Hongna. 2021. "国际数字贸易规则谈判前景与中国面临的挑战" [Prospects of Negotiations on Rules of International Digital Trade and the Challenges Facing China]. *新经济导刊* [*New Economy Leader*], no. 1.

Congressional Research Service. 2020. "The Committee on Foreign Investment in the United States (CFIUS)." February 26. https://crsreports.congress.gov/product/pdf/RL/RL33388.

Council on Foreign Relations. 2021. *China's Belt and Road: Implications for the United States*. Independent Task Force Report No. 79. March. www.cfr.org/task-force-report/chinas-belt-and-road-implications-for-the-united-states.

DBAPPSecurity. 2021.《数据安全法》全面解读 [A Comprehensive Interpretation of the "Data Security Law"]. 安恒信息 [DBAPPSecurity]. www.iii.tsinghua.edu.cn/info/1058/2668.htm.

European Data Protection Board. 2019. *Government access to data in third countries*. Final Report. February 13. https://edpb.europa.eu/system/files/2022-01/legalstudy_on_government_access_0.pdf.

Fu, Wei. 2019. "全球数据治理体系建设与中国的路径选择" [Building of global data governance system and China's path selection]. In *Blue Book of China's Informatization: Analysis and Forecast on China's Informatization* (2018–2019)], edited by Secretariat of Advisory Committee for State Informatization, 267–82. Beijing, China: 社会科学文献出版社 [Social Sciences Literature Press].

He, Alex. 2020. *Top-level Design for Supremacy: Economic Policy Making in China under President Xi*. CIGI Paper No. 242. Waterloo, ON: CIGI. www.cigionline.org/publications/top-level-design-supremacy-economic-policy-making-china-under-president-xi/.

———. 2021. *China's Techno-Industrial Development: A Case Study of the Semiconductor Industry*. CIGI Paper No. 252. Waterloo, ON: CIGI. www.cigionline.org/publications/chinas-techno-industrial-development-case-study-semiconductor-industry/.

———. 2022. *The Digital Silk Road and China's Influence on Standard Setting*. CIGI Paper No. 264. Waterloo, ON: CIGI. www.cigionline.org/publications/the-digital-silk-road-and-chinas-influence-on-standard-setting/.

He, Alex and Robert Fay. 2023. *Digital Governance in China: Data, AI and Emerging Technologies, and Digital Trade*. CIGI Conference Report. Waterloo, ON: CIGI. www.cigionline.org/publications/digital-governance-in-china-data-ai-and-emerging-technologies-and-digital-trade/.

Hong, Yu and Jian Xu. 2019. "Toward Fragmented Platform Governance in China: Through the Lens of Alibaba and the Legal-Judicial System." *International Journal of Communication* 13: 4642–62. https://ijoc.org/index.php/ijoc/article/view/12025/2804.

Huang, Daoli, Hao Yuan and Wenhua Hu. 2020. "数据安全法(草案)的立法背景, 立法定位与制度设计" [The legislative background, legislative intent and legal system design for the Data Security Law (draft)].信息安全与通信保密 [*Information Security and Communications Privacy*], no. 8.

Hungerland, Nils and Kenddrick Chan. 2021. "Assessing China's Digital Silk Road: Huawei's engagement in Nigeria." LSE Ideas Digital IR Working Paper Series no. 11. https://eprints.lse.ac.uk/112588/1/LSE_IDEAS_assessing_chinas_digital_silk_road_huaweis_engagement_in_nigeria.pdf.

Liang, Zheng, Dong Zhang and Yang Yu. 2022. "数据出境安全治理国际经验比较与启示" [Comparison and Implication of International Experiences on Security Governance of Data Export]. *中国信息安全* [*China Information Security*], no. 3.

Lu, Yiwen, 2022. "Hackers claim they breached data on 1 billion Chinese citizens." *The Washington Post*, July 6. www.washingtonpost.com/business/2022/07/06/china-hack-police/.

MIIT. 2015. "工信部解读促进大数据发展行动纲要" [Interpretation of the Action Outline for Promoting the Development of Big Data]. September 11. www.cac.gov.cn/2015-09/11/c_1116538239.htm.

———. 2021. "十四五" 大数据产业发展规划" [The Outline for Big Data Development in the "14th Five-Year" Period]. November 30. www.gov.cn/zhengce/zhengceku/2021-11/30/5655089/files/d1db3abb2dff4c859ee49850b63b07e2.pdf.

Ministry of Foreign Affairs of China. 2020. "2020年9月8日外交部发言人赵立坚主持例行记者会" [Foreign Ministry's Spokesperson Zhao Lijian's Regular Press Conference on September 8, 2020]. www.fmprc.gov.cn/web/wjdt_674879/fyrbt_674889/202009/t20200908_7816630.shtml.

———. 2023a. "中国—中亚峰会西安宣言(全文)" [Xi'an Declaration of the China-Central Asia Summit (Full text)]. May 19. www.fmprc.gov.cn/web/wjb_673085/zzjg_673183/xws_674681/xgxw_674683/202305/t20230519_11080194.shtml.

———. 2023b. "China's Positions on Global Digital Governance (Contribution for the Global Digital Compact)." May 25. www.fmprc.gov.cn/eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/202305/t20230525_11083607.html.

NPC. 2016. 中华人民共和国网络安全法 [Cybersecurity Law of the People's Republic of China]. *中国人大网* [npc.gov.cn], November 7. www.npc.gov.cn/npc/c30834/201611/270b43e8b35e4f7ea98502b6f0e26f8a.shtml.

———. 2021a. 中华人民共和国数据安全法 [Data Security Law of the People's Republic of China]. *中国人大网* [npc.gov.cn], June 10. www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml.

———. 2021b. 中华人民共和国个人信息保护法 [Personal Information Protection Law of the People's Republic of China]. *中国人大网* [npc.gov.cn], August 20. www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml.

Nussipov, Adil. 2020. "How China Governs Data." Center for Media, Data and Society, CEU Democracy Institute, April 27. https://medium.com/center-for-media-data-and-society/how-china-governs-data-ff71139b68d2.

Peng, Lei. 2020. "数字关境对我国数字市场开放的意义及政策涵义" [The Significance and Policy Implication of Customs Digital Territory to the Opening of China's Digital Market]. *国际贸易* [Intertrade], no. 9.

Que, Tianshu and Ziyue Wang. 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]. *国际安全研究* [*Journal of International Security Studies*], no. 1.

SAC/TC260. 2017. "信息安全技术 数据出境安全评估指南(草案)" [Information Security Technology-Guideline for Data Cross-Border Transfer Security Assessment (draft)], August 30. www.tc260.org.cn/front/bzzqyjDetail.html?id=20170830211755&norm_id=20170221113131&recode_id=23883.

———. 2022. "信息安全技术重要数据识别指南(草案)" [Information Security Technology-Guideline for Identification of Important Data (draft)]. January 7. www.tc260.org.cn/file/2022-01-13/bce09e6b-1216-4248-859b-ec3915010f5a.pdf.

Sacks, Samm, Graham Webster and Mingli Shi. 2019. "The evolution of China's data governance regime: A timeline." DigiChina, Stanford University. February 8. https://digichina.stanford.edu/work/the-evolution-of-chinas-data-governance-regime-a-timeline/.

Sodiq Omolaoye, Abuja. 2022. "Doubts, queries over China's interest in Nigeria's telecom sector." The Guardian Nigeria, March 1. https://guardian.ng/features/doubts-queries-over-chinas-interest-in-nigerias-telecom-sector/.

State Council. 2015. "国务院关于印发促进大数据发展行动纲要的通知" [Notice of the State Council on Issuing the Action Outline for Promoting the Development of Big Data]. September 5. www.gov.cn/zhengce/content/2015-09/05/content_10137.htm.

———. 2021. "国务院关于印发 '十四五' 数字经济发展规划的通知" [Notice of the State Council on Issuing the Plan for Development of the Digital Economy During the "14th Five-Year" Period]. December 12. www.gov.cn/zhengce/content/2022-01/12/content_5667817.htm.ua

———. 2022. "中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见" [Opinions of the CPC Central Committee and the State Council on Establishing a Basic System for Data to Maximize a Better Role of Data Elements]. December 19. www.gov.cn/zhengce/2022-12/19/content_5732695.htm.

Tiezzi, Shannon. 2020. "China's Bid to Write the Global Rules on Data Security." The Diplomat, September 10. https://thediplomat.com/2020/09/chinas-bid-to-write-the-global-rules-on-data-security/.

Wakabayashi, Daisuke, Ana Swanson and Lauren Hirsch. 2023. "In China, the Police Came for the Consultants. Now the C.E.O.s Are Alarmed." *The New York Times*, May 15. www.nytimes.com/2023/05/12/business/china-anti-espionage-law.html?_ga=2.191998953.2121840535.1684265051-1956752967.1542218591.

Wang, Zhongmei. 2021. "跨境数据流动的全球治理框架: 分歧与妥协" [Global Governance on Cross-border Data Flows: Diversity and Compromise]. *国际经贸探索* [*International Economics and Trade Research*], no. 4.

Wong, Chun Han. 2020. "China Launches Initiative to Set Global Data-Security Rules." *The Wall Street Journal*, September 8. www.wsj.com/articles/china-to-launch-initiative-to-set-global-data-security-rules-11599502974.

Xinhua. 2014. "习近平: 坚持总体国家安全观 走中国特色国家安全道路" [Xi Jinping: Maintaining a holistic approach to national security and walking the path of national security with Chinese characteristics]. 新华网 [xinhuanet], April 15. www.xinhuanet.com/politics/2014-04/15/c_1110253910.htm.

———. 2020. "全球数据安全倡议 (全文)" [Full text: Global Initiative on Data Security]. 新华网 [xinhuanet], September 8. www.xinhuanet.com/world/2020-09/08/c_1126466972.htm.

———. 2021. "中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要" [The 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035 of the People's Republic of China]. 新华网 [xinhuanet], March 13. www.gov.cn/xinwen/2021-03/13/content_5592681.htm.

Xue, Annie. 2022.《数据出境安全评估办法》解读 [Interpretation of Measures of Security Assessment for Data Export]. *己任律师事务所* [GEN Law Firm], July 11. www.lexology.com/library/detail.aspx?g=e7d379b1-4345-4167-ac2e-690ecb06945b.

Zhang, Monan. 2020. "跨境数据流动: 全球态势与中国对策" [Cross-border Data Flows: Global Situation and the Countermeasures for China]. *开放导报* [*China Opening Journal*], no. 2.

Zhou, Nianli and Tingting Yao. 2021. "中国自由贸易试验区推进数据跨境流动的现状、难点及对策分析" [Analysis on the Current Saturation, Difficulties and Countermeasures of Promoting Cross-border Data Flows in Free Trade Zones of China]. *国际商务研究* [*International Business Research*], no. 3.

Centre for International
Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

@cigionline