Politics and Governance
2025 • Volume 13 • Article 10460
https://doi.org/10.17645/pag.10460

cogitatio

ARTICLE

Open Access Journal

Ruling the Data Flows: Data Cognition in Global Cross-Border Data Flows Governance

Jinhe Liu

School of Journalism & Communication, Peking University, China

Correspondence: Jinhe Liu (liujinhe@pku.edu.cn)

Submitted: 31 March 2025 **Accepted:** 10 July 2025 **Published:** 27 August 2025

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

Abstract

Noting the "awakening" of data cognition in the governance of global cross-border data flows over the past half-century, this article calls for a deeper understanding and exploration of the cultural dynamics underlying this phenomenon from a constructivist perspective. It identifies "cultural value" as one of the key driving factors in the governance approaches of four representative countries and regions: the US, China, the EU, and Russia. We extract "attribute cognition" and "value pursuit" from the core of data culture to the center of data governance under the concept of "evaluative cognition." By observing how policy stances change, we separate different evaluative cognitions from a complex game field through a historical and comparative analysis, and thus provide a theoretical understanding of the current intense geopolitical game around data.

Keywords

cross-border data flows; cultural value; data governance; evaluative cognition

1. Introduction

The global understanding of data is changing. In recent years, China's policy stance on cross-border data flows has changed, and the "data *developmentalism*" of data cognition behind it has been clearly expressed. In 2024, China issued the Provisions on Promoting and Regulating Cross-Border Data Flows and the Global Initiative on Cross-Border Data Flows, which shows its change from a strict data localization stance. At the same time, we have seen the US revise its claim of data free flows, showing a trend of advocating data localization to a certain extent. Also, in 2024, the US Department of Justice issued final rules prohibiting the cross-border transfer of sensitive personal data to some countries, starting the process of data decoupling for some countries, and establishing a cross-border data flows regime based on national security rationale.

Earlier in 2018, Brazil enacted the General Personal Data Protection Act, aligning with the EU's GDPR and amending the data localization initiative proposed in the Marco Civil da Internet in 2014.

How to understand this seemingly fickle policy stance, and how to analyze the complex and ever-changing regulatory system of cross-border data flows? This becomes an important challenge in the study of global cross-border data flows governance. There is often a systematic value system behind national policies, and data culture research is an effective theoretical approach to understanding data development and governance (Oliver, 2024), especially regarding the value propositions carried in data. The most typical example is the globally popular slogan "Data is Oil," as well as the highly concerning concept of "dataism" (Brooks, 2013; Harari, 2016), that have crystallized a prescriptive idea about how people should see data and the value it contains. It is necessary to analyze the cognition of the attributes of data and the value it carries in different countries and regions. This article takes an explicitly constructivist approach and adopts the theoretical perspective of cultural value theory to use the conceptual tools of evaluative cognition to analyze this inherent law. The history of regulating cross-border data flows holds rich philosophical implications that go far beyond the academic value of analyzing specific regulatory policies. A deeper epistemological contestation behind the global cross-border data flows governance should be recognized, and forces with more far-reaching effects should be identified.

2. Data Awareness: Three Historical Tracks of Global Development

The debates over the regulation of cross-border data flows have emerged even before the mass commercialization of the Internet. In Western countries, they go as far as the early 1970s. From a global perspective, the history of this regulation unfolds along three tracks and sparks three waves (see Figure 1). The first and second tracks, namely the American Track and the European Track, are rulemaking efforts led by the US and Europe, respectively, while the third track, namely the Emerging Economies' Track, is dominated by emerging countries, advocating new rulemaking through domestic legislation. The first wave of regulation of cross-border data flows was initiated by European countries. In the game with the US, the basic version of the European model was formed, which was marked by the 108 Convention, the General Exception Rules of the General Agreement on Trade in Services (GATS) under the WTO framework, and Directive 95. The second wave was led by the US, which changed its previous defensive posture toward Europe. For instance, the US took the Asia-Pacific Economic Cooperation (APEC) as the rule-building field and led the construction of the APEC Privacy Framework in 2004. Finally, the APEC Cross-Border Privacy Rules System (CBPRs) was formally formed in 2011. Since then, the American model has become an important international template for "data free-flowing."

Europe and the US had a clear understanding of electronic data at the beginning. The cross-border data flows had become the focus of the transatlantic competition since the early 1970s. Before the 1990s, Europe took the lead in establishing rules, and after 2000, the US took the initiative to construct the American version of cross-border data flows management norms. In the past decade, the global cross-border data flows regulation has entered its third wave. In the past 50 years or so of the history of cross-border data flows governance, the main value of Western countries in the first four decades had been the protection of personal privacy.

The third wave, which also marks the rise of the third track, began around 2010, when emerging economies such as China, India, and Russia started to put forward requirements for data localization (Chander & Lê, 2014).

Snowden's revelations in 2013 significantly accelerated this trend. But unlike the previous two waves, when Europe and the US focused on privacy legislation, this new stage presented a novel struggle of power and interests around data rules among Europe, the US, and the emerging economies. This game has gradually moved from domestic legislation to the negotiation of international trade rules, and the object of regulation has also expanded from personal information to almost all data circulating with commercial value (Wang, 2018).

In the later decade, as emerging economies began to "wake up" to this issue, one after another, they joined these "construction of rules" from the perspective of their own national interests. The problem of cross-border data flows regulation became no longer a problem of personal privacy, but also a competition for national economic interests. In the global rise of digital trade, a new round of global debate on the governance of cross-border data flows has emerged, among which various understandings of data attributes have been manifested. The most typical countries that regard data as wealth are China and India. China proposed that "data is a basic strategic resource of the country" (State Council of the People's Republic of China, 2015) in the Outline of Action to Promote Big Data Development in 2015, and it proposed data as a factor of production in 2019. Also in 2019, in response to the then US President Donald Trump's criticism of data localization policies at the G20 summit, Indian Foreign Secretary Vijay Gokhale asserted that "data is also needs to take into account the requirements of developing countries," and "it is a new form of wealth" ("Data 'new form of wealth,'" 2019). With the rapid development of data-based artificial intelligence, it can be foreseen that the cognition of data attributes will further develop.

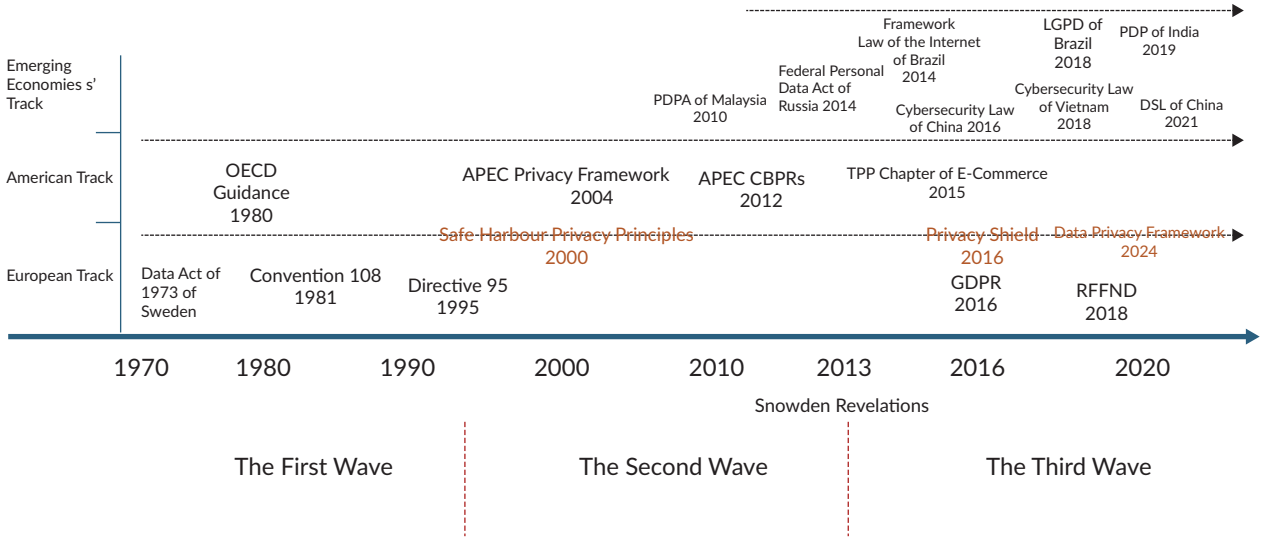

Figure 1. Three tracks of global cross-border data flows governance. Note: These represent significant historical milestones in global cross-border data flows governance, but do not encompass all the legislations and policies.

3. Cultural Value Paradigm of Data Governance Study

Governance, especially state decision-making, is highly complex and often involves multiple factors working together. There are multiple levels of research on the dynamics of cross-border data flows policies. Interest, power, and culture are all important analytical perspectives, and these three levels often jointly determine the formation of policies. Furthermore, the factors at these three levels also influence each other. A large number of research on the regulation game of cross-border data flows is mainly at the interest level,

assuming that countries are rational actors and try to select policies that maximize their national interests under existing international conditions, such as data localization theory (Chander & Lê, 2014) and data defensivism theory (Liu, 2020). Since cross-border data flows governance is often reproduced in the form of policies and rulemaking, a significant body of study has focused on material aspects, particularly rule analysis and policy recommendations (Xu, 2018). In contrast, there is a notable deficiency in analyses addressing the intrinsic cultural demands of data governance, as well as studies exploring historical depth and the underlying logic of contemporary realities.

Constructivism holds that society is largely constructed by human beings, and people's cultural value constantly influences decision-making in practice. Beyond the rationalist approach, this article advocates for further understanding and exploring of the cultural dynamics behind phenomena from a constructivist perspective, arguing also that cultural value should be taken as one of the most important driving factors of governance, which could be conceptualized as a cultural value paradigm (Liu & Cui, 2023). The relationship between cultural value and material society transpires in a process of mutual expression. However, through the accumulation of social history, culture has formed its own continuous logic and exerts a guiding role on the material society.

It should be noted that the cultural value paradigm is not an absolute cultural determinism, but rather a theory of the hierarchy of values. In other words, the cultural value paradigm holds that a series of values have an impact on real governance activities, but there are values that are given priority. The dominant values often run through the whole process of policy making, and even define the preconditions for policy makers to understand events and the perspective from which they view problems. Therefore, this study attempts to recognize the dominant values and analyze their impact on governance decision-making. At the same time, it aims to grasp the macro development laws, hoping to gain a more general understanding of the development context of global data governance.

Generally, data culture reflects and is influenced by people's values, attitudes, and behavior (Oliver et al., 2023). Actors conceptualize differently the meaning of data, the relevant stakeholder community, and the reasoning for their governance efforts, and these differences are directly related to whether data can be governed. (Obendiek, 2022) In fact, the objects pointed to by data culture are broad. This article selects "attribute cognition" and "value pursuit" as the core elements of data culture, which serve as key driving factors of data governance. I put the two elements under the concept of "evaluative cognition" as the operational tool of the cultural value analytical paradigm, which emphasizes human subjective initiative.

Evaluative cognition is an interdisciplinary concept, referring to the process in which, during cognition, not only the attributes of things are identified but also their values (such as good or bad, degree of importance, and legitimacy) are judged and asserted, which is a fundamental aspect of decision-making and planning. For instance, it is like recognizing the chemical properties of a certain drug (attribute cognition) and asserting that it has "therapeutic value" (value assertion). An important foundation of evaluative cognition is Richard Lazarus' cognitive appraisal theory in psychology, which emphasizes that emotions are not caused by events themselves, but by how these events are appraised in relation to personal goals (Lazarus, 1991, p. 135). Evaluative cognition is regarded as the core of attitudes, considering attitudes as the automatic association of "object-evaluation" (such as "apple → healthy → like"; see also Fazio, 2007). In the field of cognitive science, evaluative cognition is the computational process in which systems (humans or machines) compare

the values of options and prioritize them in decision-making, problem-solving, or goal-oriented behaviors. Typically, Herbert A. Simon proposed "bounded rationality," suggesting that the evaluative cognition of humans and machines is limited by information processing capabilities and tends to choose "good enough" options through the "satisficing" principle rather than the optimal solution (Simon, 1980). In summary, evaluative cognition is a value-driven information processing process.

Data evaluative cognition here refers to a country or a society's cognition of the attributes of data and their assertion of the value it carries. It is a kind of social epistemology in a broad sense. Lorraine Daston's historical epistemology (Daston, 1994, pp. 282–289; Daston & Galison, 2007) offers us significant inspiration that the nature, standards, and production methods of knowledge are not immutable but deeply rooted in specific historical, cultural, and social practices. Therefore, evaluative cognition helps to highlight the value expectations in a specific history and society from epistemology.

In terms of operational methods, this study takes evaluative cognition as the analytical variable and the more than half-century history of data cross-border flows regulation as the object, by observing the policy stance changes of major countries around the world. In the selection of case countries and regions, the US, China, the EU, and Russia were chosen because they all have a strong position tendency and relatively profound epistemological foundations. To some extent, these four countries/regions can be regarded as ideal types in Max Weber's sense, which have instrumental value for understanding the governance of global cross-border data flows. The other influential countries, such as India, Brazil, Japan, South Korea, and Iran, can be found in these four types accordingly or by similar logic. For example, India and Brazil hold a developmentalist stance similar to China's; Japan and South Korea follow a logic more like that of Europe and the US, and Iran aligns closer to Russia. Of course, it is difficult to match one individual country to one single position, and the situation of each country needs to be more accurately understood in the light of its history and reality. However, certainly, understanding each country's position from the perspective of cultural values is an effective approach. Data cognition is crucial for comprehending data governance on a global scale.

4. Starting Point and Development of Data Cognition

4.1. The Starting Point of Data Cognition

To accurately examine the data cognition, a historical perspective is needed. When examining the claims about data made by various countries and regions from the perspective of historical traditions, we can identify their starting point as the origin (see Table 1).

Table 1. The starting point for data cognition.

Country and region	Starting point of data cognition
US	Property carrier
China	Strategy carrier
EU	Rights carrier
Russia	Security carrier

The US views the Internet as a market product and as property that has been transferred from the state to private enterprises. Due to the Internet's "American-origin story," in the mid-1990s, the US privatized the

Internet and sold five access points of its backbone network to private enterprises, transferring the management of its root server system from the government to the private sector, to what is now well-known as the nonprofit corporation the Internet Corporation for Assigned Names and Numbers (ICANN; Leiner et al., 1997). Since then, the US has regarded the Internet as a market product, which became the fundamental logic supporting the later development of the American Internet industry. Under this kind of Internet cognition, the US generally regards data generated from the Internet as a market product and the property of enterprises. Moreover, the US believes that data is an indispensable element for the development of the Internet market; therefore, it has always supported the free flow of data along with the global market. In a transnational scenario, cross-border data is itself a kind of trade (Mueller & Grindal, 2018).

The EU has recognized the human rights embedded in data from the very beginning. During the Holocaust, in World War II, the Nazi German government identified and hunted the Jewish population by using census cards and other demographic statistics. This particular social memory has long raised deeply-embedded fears and concerns in Europe about the malign use of personal data. In the 1970s, the efficient data processing capabilities of large-scale computers in the US generated a sense of unease among Europeans (Fishman, 1980; Kirby, 1980; Novotny, 1980). The Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data, adopted in 1981, was a response to such concerns. Against this backdrop, the EU began to clearly define the rights and value of data itself (Kuner, 2011). The Charter of Fundamental Rights of the European Union, drafted in 2000 and enacted in 2009, clearly states the fundamental rights contained in the data under Article 8 on protection of personal data, and especially along with Article 7 on respect for private and family life. The GDPR, adopted in 2018, embodies the EU's claim to data rights, establishing data privacy and protection as a fundamental right. When it comes to digital technology, the EU emphasizes "European values." The EU's commitment to a safe, secure, and sustainable digital transformation that puts people first, aligning with the EU's core values and fundamental rights, is underlined in the *European Declaration on Digital Rights and Principles*, a high-level document signed by the Presidents of the Commission, the European Parliament, and the Council in 2022.

China has a tradition of technological nationalism, hoping that information technology can make the country rich and powerful, and treating data as a national development strategy (Liu, 2020). China sees the Internet as a force for national development and has put forward a "cyber power" (网络强国) strategy. In official statements, "big data" has been elevated to a national strategy. By 2020, China had officially proposed "data as a factor of production," raising expectations about the empowerment of data for national development to a new high (The Central Committee of the Communist Party of China & The State Council of China, 2020). To promote the development of data, China is working hard to build a "data factor market" (数据要素市场) and established, in 2023, the National Bureau of Data. The National Bureau of Data has released several definitions of data-related concepts, including data factor, data products and services, data assets, and market-based allocation of data factor, which have strong attributes of economic development and point to the market economy. For example, it defines "data resources" (数据资源) as "data with value creation potential" (National Data Administration of PRC, 2024). In this clear cognition, data is regarded as an element of national development and the carrier of development strategies. From the "big data strategy" to the data factor market strategy, we are constantly exploring the process of maximizing the energy of data.

China's expectation of a data development strategy also comes from earlier strategic propositions for national informatization and industrialization. Even we can see the logic behind China's pursuit of modernization since

the Reform and Opening Up program, which regards science and technology as the driving force of national development (Zheng, 2007, p.27). Therefore, data, as the basis of the latest information technology, is naturally regarded as the strategic carrier of national development.

In Russia, due to the Cold War, the understanding of Internet/cyberspace is dominantly based on national security, which is called "information security" instead. As early as 1998, in response to the international governance of the Internet, Russia put forward a proposal for an international information security aimed at the United Nations, calling on UN member states to pay attention to potential threats in the field of information security from a multilateral level. Since then, Russia has been firmly calling attention to the issue of international information security under the UN framework. In 2019, Russia promulgated the Federal Law No. 90-FZ, the so-called Sovereign Internet Law—with a set of amendments to existing Russian legislation—which lays out institutional arrangements for "autonomous and controllable sovereignty" over the Internet. Russia also has a strong tradition of control over content data (Zhuravlev & Brazhnik, 2018). In 2022, the Personal Data Act of the Russian Federation was amended to establish a strict management model for cross-border data both internally and externally.

4.2. Development/Adjustment of Data Cognition

Digital technology is developing rapidly, especially with the emergence of data-based AI. The tremendous energy released by data, as well as the continuous development of its functions, has exerted a strong influence on all aspects of society. People's understanding of the essence of data is constantly being updated. In recent years, as the regulation of global cross-border data flows has entered its third stage, the understanding and claims on data of various countries are undergoing obvious changes. At the same time, with the domestic development and the international pattern changing rapidly, information technology has become an important factor in the game among countries (Lang, 2021). To some extent, data cognition on a global scale is in a critical period of exploration.

People's understanding of the objective world is constantly being updated. In terms of data, it is in the development process from an emerging phenomenon to a social entity, which has only just begun. Therefore, people's understanding of the essential attributes of data is constantly evolving. For instance, in recent years, China has elevated the perception of data attributes to the level of production factors. As time goes by, the relative positions of different countries in the global landscape are also changing, and the expectations for the value carried in data are constantly evolving. For instance, the US increasingly emphasizes that there is national security value in exploring data. Overall, the understanding of data in societies of various countries has developed from a relatively simple single dimension to a complex multi-dimensional one. This can be ascribed to the fact that the demands of human society for data have become richer. We can observe this change in cognition from the change in policy propositions.

Based on the abovementioned considerations, the intention of this article is not to propose an absolute and static view of data cognition, but to construct a developing cognitive system for a more accurate grasp of history and reality. Below, several case countries and regions will be analyzed from this perspective (see Table 2).

Table 2. Data cognition and its development.

Country and region	Starting point of data cognition		Development/adjustment
US	Property carrier	⟶	privacy rights carrier, national security carrier
China	Strategy carrier	⟶	security carrier, economic carrier
EU	Rights carrier	⟶	societal (cultural, economic) carrier
Russia	Security carrier	⟶	national development carrier (domestic construction)

The understanding of data in the US has further evolved from "property carrier" to "carrier of privacy rights and national security." The "privacy rights carrier" refers to the personal rights value centered on privacy embodied in data, a concept that primarily stems from social developments within the US. The "national security carrier" lens regards data as a critical factor that may trigger national security risks, primarily arising from external threats.

After multiple rounds of interactive games with the EU, the US is paying more and more attention to the protection of personality rights, such as privacy in data. To a certain extent, due to the external pressure of the EU, the US began to revise the market concept of data *laissez-faire*, and constantly added elements of rights protection to its data governance regime (Voss, 2020). In addition to the external pressure, the rapid development of information technology itself and the increasing impact of data-based intelligent technology on people's lives will inevitably lead to the need for the US to respond to the issue of right protection in data. Historically, in the US, privacy rights are not equivalent to civil rights. However, in the digital environment, the call for privacy rights to be regarded as civil rights is gaining larger momentum (Allen & Muhawe, 2025). At the same time, the Clean Network Initiative launched by the US against China and the recent ban on TikTok both reflect a change in the US perception of data, which emphasizes national security and a protective national strategic orientation.

It is worth noting that the US has made progress in both legislation and judicial practice of data privacy protection. Since the enactment of the California Consumer Privacy Act in 2018, the number of comprehensive privacy bills proposed by US states, as well as the number of privacy laws passed, has largely increased (see Figure 2). Among the states that have enacted privacy laws that provide consumer data privacy rights, there is almost unanimous agreement that consumers should have the right to control their own data. The American Data Privacy and Protection Act, issued on June 3, 2022, served as the basis for the American Privacy Rights Act, a major legislative proposal at the federal level, which was proposed on April 7, 2024. In the draft text of the American Privacy Rights Act, it states that the congressional intent is to "establish a uniform national privacy and data security standard in the United States" (American Privacy Rights Act of 2024, 2024). The right to privacy has also gradually taken position in the US, where *Katz v. United States* (1967) pioneered the "reasonable expectation" standard of privacy, providing a theoretical basis for privacy protection. The *Carpenter v. United States* (2018) further adapted to the digital age, extending privacy protections to electronic data and records of long-term behavior. All these reflect the change in the understanding of the inherent attributes of data in the US.

China's evaluative cognition of data has further developed from "strategy" to multiple carriers of "security" and "economy." China is gradually transitioning from a single emphasis on data sovereignty to a more comprehensive framework of data developmentalism. Over the past decade, the emphasis on data cognition

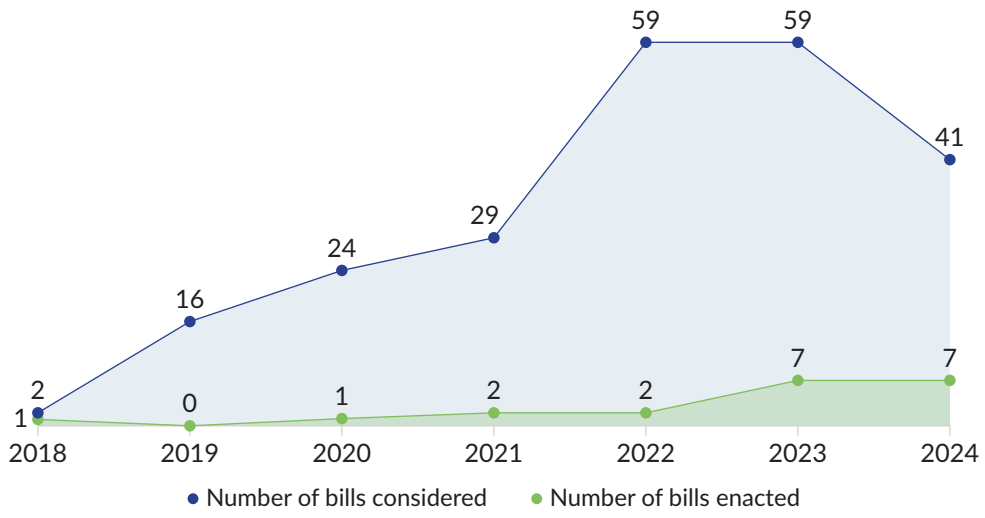

Figure 2. The growth of US state privacy legislation. Source: IAPP (2024).

in China has changed. After a period of excessive data defensivism, China has begun to shift its policy stance, representing a change in cognition as well. Shocked by Snowden's revelation in 2013, China embarked on a cybersecurity/data security as a stress response, elevating data security to a high priority. In this period, China is more inclined to recognize data as a security carrier, such as the investigation of Didi's IPO in the US in 2020. However, after the Sino–US trade war began in 2018, China began to recognize the overall beneficial role of data in the digital economy, putting forward the theory of "data as a factor of production," and starting to enrich its data cognition from the perspectives of market economy and industrial development. This shift is seen as a kind of "data developmentalism" (Meng, 2023). China has gradually transitioned from the proposition of data sovereignty to a more comprehensive data developmentism. The core of data developmentism is to regard data as a driving force for the all-round development of society, emphasizing that the priority value of data lies in promoting economic and social development. In fact, China has been developing its understanding of information technology and the Internet in a pragmatic way, and its governance methods have been constantly updated (Liu, 2023).

The EU has further extended its evaluative cognition of data from the carrier of rights to the carrier of cultural values, while separating the economic carrier, and generally placing the data in the position of societal comprehensive carrier, as the societal (cultural, economic) carrier. After the promulgation of GDPR, the data rights protection system has been basically established. Followed by the Regulation on a Framework for the Free Flow of Non-Personal Data in the European Union, it is a timely recognition of the economic value of data. In 2015, the European Commission published the European Digital Single Market Strategy, which aims to create an EU digital market to facilitate data flows. In 2020, the European Commission launched its European Data Strategy, which aims to make the EU a "world model" for better data-driven decision-making by businesses and the public sector, thereby creating an open data market for the world. The common data spaces proposed by the EU as the cornerstone of the European data strategy play a key role in combining the necessary infrastructure with data governance mechanisms. The ongoing Digital Fairness Act, the so-called "law of everything" for the digital economy and the digital world as a whole (Zhu, 2024), has heightened expectations for the social value that data carries.

Although Russia still regards national security as the primary value of data, it is increasingly focusing on the development value of data. In the context of Russia, this new evaluative cognition can be called "the carrier of national development," shifting from an overly emphasis on external threats to an internal construction perspective. Especially after the war began between Russia and Ukraine, under strong external sanctions, the external development of Russia's digital economy has been greatly challenged and even stalled. From the perspective of national security, Russia has implemented data localization more thoroughly, which also leads to Russia's attention on data being more focused on the development of its national economy. In other words, Russia is more concerned about how these local data can serve a social and economic utility. Although the legislation is strict, there is room for maneuver in judicial enforcement (He, 2016; Sun & Haritonova, 2022). The Russian courts have punished companies for not complying with relevant laws; although the amount of penalties is negligible for companies, it also shows the logic of Russian justice: to balance the dual goals of personal data protection and industrial development, and not to take an overly biased attitude (Sun & Haritonova, 2022). Under this cognition, Russia is actively promoting the compilation of the Digital Code, which is also an effort to actively promote the construction of a domestic digital economic development system.

5. The Choice of Governance Tools Under Data Cognition

Decision making and action are important aspects of evaluative cognition. Supported by the different evaluative cognitions of data, to realize their inherent value expectations, different countries and regions choose the corresponding governance tools, and each forms a complete set of governance propositions.

5.1. US: Market + Ideology: Advocating the Establishment of a Global System of Free Data Flows

Starting from the data property cognition, the US often puts cross-border data flows in the context of the Internet economy, and regards the data flows as an indispensable part of the market economy, including the internal business data flows of transnational corporations, the optimal configuration of data of Internet companies, and the free transaction of data itself as a product, etc. This proposition is embodied in the CBPR system under the APEC framework in 2012, which adheres to the principle of supporting data free-flow under the free market law. Therefore, the market is the basic tool for the governance of cross-border data flows for the US. This logic of taking the market economy as a governance tool has developed into a liberal ideology to a certain extent, with a strong color of exclusivity. In American logic, data free-flow is the proper meaning of a market economy: Opposing it represents a rejection of the market economy, and opposing the market economy means rejecting freedom.

With their two pillars of governance—market and ideology—the US advocates the establishment of a global system for the free flows of data. Taking the APEC privacy framework as the basic model, the US tried to build a competing global data governance system on the basis of the global digital economy by updating the TPP proposal (which was later withdrawn) and the trans-Atlantic data flows framework as its core component.

However, based on the continuous understanding of the carrier of privacy rights and the carrier of national security, the US began to pay attention to the data privacy protection system, promote the development of privacy rights in legal rules, and construct national security exceptions for data flows in the international system. Meanwhile, in the face of the international competition system, the US has introduced data

"decoupling" policies against "adversary" countries like China and even established a global export control regime for AI.

5.2. China: Sovereignty + Trade: Advocating a Global System of Secure and Orderly Data Flowing

China has taken an attitude of "Internet sovereignty" from the beginning of participating in the formulation of rules on cross-border data flows, and it has long advocated for its absolute sovereignty over data produced in China and requires data localization (Liu, 2020). This is based on China's original strategic cognition of data—a simple logic of "my data is mine." The most typical evidence is the provision on data localization in Article 37 of the Cybersecurity Law passed in 2016. However, as China's understanding of data has further shifted into a factor of production, the adoption of cross-border data flows governance has begun to pay more attention to the dimension of international trade. China is also paying increasing attention to participating in the negotiation and rulemaking of international digital trade-related agreements (He, 2022). It has actively participated in the World Trade Organization's e-commerce negotiations and signed the Joint Statement Initiative on e-commerce in 2021. At the same time, by advocating rules in multilateral international trade negotiations, it has joined the Digital Economy Partnership Agreement, the Regional Comprehensive Economic Partnership, and actively applied to join the Comprehensive and Progressive Agreement for Trans-Pacific Partnership.

In 2024, China stated that: "Cross-border data flows are crucial to the e-commerce, digital trade and even the economy, science, technology and culture of various countries…and realize a new type of globalization driven by data flows" (Cyberspace Administration of China, 2024). It further proposed to "encourage cross-border data transmission through electronic means for the needs of normal commercial and social activities, so as to realize that global e-commerce and digital trade will provide new impetus for economic growth and sustainable growth of all countries" (Cyberspace Administration of China, 2024).

5.3. EU: Moral + Market: Advocating a Global System With Data Rights Protection at Its Core

From the very beginning, the EU has been concerned about human rights embedded in data. When it comes to cross-border data flows, its code of conduct is more of a moral proposition. The GDPR provides a solid foundation for the free flow of data in line with European values. The European Data Strategy and the Shaping Europe's Digital Future initiative have repeatedly mentioned that "the EU is a global leader" and "the EU is setting global norms for the digital economy," which indicates that the EU has begun to utilize its regulatory capabilities to promote European rules and establish global standards (Xia, 2023). Later, the EU began to attach importance to the material value contained in data, advocating the market-oriented development of data to empower Europe's digital development, which is enacted in the Regulation on the Free Flow of Non-Personal Data, the European Data Act, and other later legislation.

5.4. Russia: Sovereignty, Advocating Independent and Controlled Data Flows

Russia sees data from the perspective of security, which still remains its core perspective. Russia faces an international landscape that has long been dominated by the Western bloc, so this demand for security is relative to that of the US and its allies. It is natural for Russia to choose sovereignty as the starting point of governance, from the service mode to the sovereign mode (Martynova & Shcherbovich, 2024). In the face

of an international system governing cross-border data flows, Russia advocates for the orderly flows of data under autonomy and control. By imposing legal obligations on enterprises, Russia has achieved comprehensive government control over data storage, cross-border transmission, processing, and other links, thereby taking the initiative in the cross-border flow of domestic data (see also He, 2016).

6. Changes in the Global Governance Landscape Under the Development of Data Cognition

The global pattern of cross-border data flows is not static, and it is not always solidified by ideology; it is a state of flows driven by cognitive changes. In terms of historical stages, the first phase was basically a transatlantic game between Europe and the US, about how data flowed from Europe to the US, and no other countries were involved. The second phase, based on the American data free market cognition and taking APEC as its starting point, tried to construct a global data free flow market system. In the third phase, in the "awakening" of developing countries to data, the rise of cognition theories—national security, privacy rights protection, and national strategy empowerment—the global pattern of cross-border data flows witnessed a trend towards data localization, fragmentation of rules, and strong institutional competition.

The US transitioned from a political system characterized by consistent freedom and openness to one that emphasizes defense and regulation. On 25 October 2023, during the WTO's Joint Declaration on e-Commerce Initiative meeting, the office of US Trade Representative Catherine Day announced that the US would abandon some of its long-held digital trade propositions, including the requirement for the free flow of cross-border data—indeed, the US is reviewing its current approach to trade rules in sensitive areas such as data and source code (Trachtenberg, 2025). In July 2024, the WTO officially issued the Joint Declaration on e-Commerce Initiative: WTO members negotiated on e-commerce rules and published the latest text of the agreement, requiring negotiating parties to prohibit tariffs on cross-border data transfers; the US did not support this initiative. "The current text falls short and more work is needed, including with respect to the essential security exception," the US ambassador to the WTO said in a statement (US Mission Geneva, 2024). With the profound realignment of global strategic competition, the US data regulatory policies have gradually shifted toward a model of "limited free flow under the premise of security" (Zhou & Yan, 2025). In the US, this policy shift also has its domestic political motivations; however, the shift towards cross-border data flows is closely related to the country's evaluative cognition of data, which aligns with the US' greater concern for the security value contained in data. Outside the international trade arena, the US has issued regulatory policies for data and artificial intelligence from a political perspective and has started to build a pan-national security political system that is different from what the free market had previously advocated.

China is moving from passive defense to integration into the global market system—from isolation to integration. Having gone through a strict data localization policy, China is moving from a passive defensive posture to a more active attitude of openness and integration into the international system. In 2024, China issued the Global Cross-Border Data Flow Cooperation Initiative, which sets out China's position and proposition on the issue of cross-border data flows, echoing the concerns of all parties in the international community about cross-border data flows and expressing a common willingness to promote cooperation. In March 2024, the Cyberspace Administration of China formulated the Regulations on Promoting and Regulating Cross-Border Data Flows—a move regarded as an important shift in China's policy stance on data localization and a practical measure to be actively integrated into the international system. It is worth noting

that China is now promoting mechanisms for cross-border data flow and exchanges between China and the EU for the second time in 2025. Such a shift makes China likely to gradually become one of the most dominant players in data transfer (Chen & Gao, 2024).

The EU is mining the economic benefits from the value of data rights, moving from a moral system to a comprehensive system of digital society. The EU attaches more and more importance to the economic and social value created by data. While insisting on the protection of data rights, the EU is also actively seeking the construction of a comprehensive governance system based on data. With GDPR at its core, the EU has set a global moral benchmark for data rights protection with the construction of a more comprehensive and more basic legal system in the digital field, such as the Digital Market Law, the Digital Services Law, and the Artificial Intelligence Act. The Digital Fairness Act constitutes the last piece of the "jigsaw puzzle" of digital society legislation. The EU's new claims on data are not only about the protection of information privacy rights, but also reframed itself at a level of a comprehensive governance system for the digital society. The EU is striving to become a "good global actor" in data governance (Chen & Gao, 2022) and intends to be the leader of the world's basic regime construction, playing an important leading role in the development of human digital civilization.

Russia is further seeking a way out of isolation for security and development. The Russia–Ukraine war is producing an impact on Russia's domestic politics and economy, and directly affecting Russia's cybersecurity. To deal with this situation, Russia has made detailed provisions on information legislation and the cross-border flows of information data in its national security strategy (Wen & Tan, 2024). In July 2022, the National Parliament of the Russian Federation made extensive amendments to the Law on Personal Data of the Russian Federation, adding the pre-procedure for cross-border transfer of personal data, limiting the range of countries in which cross-border transfer of data can be carried out, and adding the circumstances in which such transfer is prohibited or restricted, requiring the operators to inform the supervisory authorities of the intention to carry out the cross-border data transfer.

The digital sanctions imposed on Russia by Western countries have brought many challenges to Russia in the field of digital technology, but those pressures have also prompted Russia to accelerate the pace of independent innovation in digital technology. Russia has fundamentally reduced the risks associated with the adoption of foreign programs, computer technology, and telecommunications equipment, and has done its best to protect the digitalization process of the public administration system and the economic sector from any potential negative external influences, turning to build its domestic equipment, technologies, programs, and products. Data-based domestic development has therefore become an important strategic choice for Russia.

The pattern of cross-border data flows in the world demonstrates a new trend. The construction of a global data political system has accelerated, with the US becoming a strong leader in this system and constantly incorporating elements of privacy protection. China's shift has led to the further improvement of the global digital trading system and the strengthening of the national security element of the international trading system (Kalin, 2024, pp. 77,132). The EU has further evolved from a value system to a social system, transcending physical competition, and is likely to be a leader in the development of human right-based digital civilization. Russia's inward turn is a constant warning to countries that are unpopular with the West to pay more attention to data security, which turns to be the driving force of global Internet fragmentation rather than positive factor for global digital development.

The changes in China, the US, the EU, and Russia are naturally important forces for the change of the world, but other countries and regions are also in the overall trend of change and are equally important factors. However, for the reasons mentioned above, this article cannot analyze each country individually. However, from the theoretical perspective of cultural values, we can roughly witness such trends: The developing countries, represented by Brazil and India, actively advocate data developmentalism, and the developed countries are strengthening the pursuit of value leadership while maintaining the economic leadership; what's more, and the countries deeply involved in geopolitical conflicts, including the countries in the Middle East and Eastern Europe, are trapped in a growing security struggle. Under these trends, the global cross-border data flows governance has generally entered a period of comprehensive institutional construction of economy, politics, and culture. In addition to the realistic interest game, we must see the value proposition and the most fundamental epistemological changes in this system construction process.

7. Concluding Remarks

The demands and claims on data have been constantly changing, and the global consensus and rules for regulating cross-border data flows are still lacking. The lack of trust has seriously hindered the global circulation and sharing of data (OECD, 2023). The data flows that enable the Internet to function as a global network are increasingly adhering to geographical national boundaries, thereby delineating a map of cyberspace segregated by national territorial boundaries. This phenomenon has given rise to persistent concerns regarding the fragmentation of the Internet (Drake et al., 2016; Mueller, 2017). In this sense, ruling cross-border data flows becomes an important way for states to compete for control of cyberspace, as well as a challenge of the times for global Internet governance.

Data is the foundation of AI development, and understanding data inevitably shapes our understanding of AI. A theoretical path of data cognition can be extended to encompass the overall cognition of internet-data-AI-technology across different countries and regions. Since Martin Heidegger, philosophers and social theorists have been discussing how people should understand modern technology. The discussion of data cognition may contribute some new ideas to that question. This article attempts to present a timely overview of the development of the global data governance landscape from the perspective of evaluative cognition. However, the complex reasons driving the changes in evaluative cognition have not been fully studied. The ruling of cross-border data flows is not only a practical public policy issue but is also related to the future of digital civilization, requiring further exploration of its philosophical and historical significance.

Acknowledgments

Thanks are due to the thematic issue's editors Xinchuchu Gao and Xuechen Chen, as well as the reviewers for their valuable comments. The reasoning this article is based on was initially presented at the CAICT symposium in 2023—I thank Dr. Bo He for the invitation. Also, I would like to thank Letian Cheng and the editors for their meticulous proofreading.

Conflict of Interests

The author declares no conflict of interests.

References

Allen, A. L., & Muhawe, C. (2025). Is privacy really a civil right? *Berkeley Technology Law Journal*, *40*, Article 541. https://doi.org/10.15779/Z38KK94D6R

American Privacy Rights Act of 2024, § 118U.S.C. (2024).

Brooks, D. (2013, February 4). The philosophy of data. *New York Times*. https://www.nytimes.com/2013/02/05/opinion/brooks-the-philosophy-of-data.html

Cyberspace Administration of China. (2024). *Global cross-border data flow cooperation initiative*. https://www.cac.gov.cn/2024-11/20/c_1733706018163028.htm

Carpenter v. United States, 138 S.Ct. 2206 (2018).

Chander, A., & Lê, U. P. (2014). Data nationalism. *Emory Law Journal*, *64*, Article 677. https://scholarlycommons.law.emory.edu/elj/vol64/iss3/2

Chen, X., & Gao, X. (2022). Comparing the EU's and China's approaches in data governance. In E. Fahey & I. Mancini (Eds.), *Understanding the EU as a good global actor* (pp. 209–225). Edward Elgar Publishing.

Chen, X., & Gao, X. (2024). Norm diffusion in cyber governance: China as an emerging norm entrepreneur? *International Affairs*, *100*(6), 2419–2440. https://doi.org/10.1093/ia/iiae237

Daston, L. (1994). Historical epistemology. In K. Chandler, I. Davidson, & D. Harootunian (Eds.), *Questions of evidence: Proof, practice, and persuasion across the disciplines* (pp. 282—289). University of Chicago Press.

Daston, L., & Galison, P. L. (2007). *Objectivity*. Princeton University Press.

Data 'new form of wealth,' take it into account of developing nations' needs: India. (2019, June 28). *The Economic Times*. https://economictimes.indiatimes.com/tech/internet/data-new-form-of-wealth-needs-to-take-into-account-developing-nations-needs-india/articleshow/69988888.cms?from=mdr

Drake, W. J., Vinton, C. G., & Kleinwächter, W. (2016). *Internet fragmentation: An overview*. World Economic Forum.

Fazio, R. H. (2007). Attitudes as object–evaluation associations of varying strength. *Social Cognition*, *25*(5), 603–637. https://doi.org/10.1521/soco.2007.25.5.603

Fishman, W. L. (1980). Introduction to transborder data flows. *Stanford Journal of International Studies*, *16*(Summer 1980), 1–25.

Harari, Y. (2016). *Homo Deus: A brief history of tomorrow*. Vintage.

He, B. (2016). Legislation and enforcement of cross-border data flows rules in Russia. *Big Data Research*, *2*(6), 129–134.

He, B. (2022). Challenges and countermeasures for China's participation in international rules of the cross-border data flows. *Administrative Law Review*, *4*, 89–103.

IAPP. (2024). *Comprehensive US state privacy legislation in 2024*. https://iapp.org/resources/article/us-state-privacy-laws-overview

Kalin, R. P. (2024). *Digital trade and data privacy*. Springer Nature.

Katz v. United States, 389 U.S. 347 (1967).

Kirby, M. D. (1980). Transborder data flows and the basic rules of data privacy. *Stanford Journal of International Studies*, *16*, Article 27.

Kuner, C. (2011). *Regulation of transborder data flows under data protection and privacy law* (Digital Economy Paper No. 187). OECD Publishing. http://doi.org/10.1787/5kg0s2fk315f-en

Lang, P. (2021). How the internet changes international relations. *International Political Science*, *2*, 90–121.

Lazarus, R. S. (1991). *Emotion and adaptation*. Oxford University Press.

Leiner, B., Cerf, V., Clark, D., Robert, K., Kleinrock, L., Lynch, D., Postel, J., Roberts, L., & Wolff, S. (1997). *Brief history of the internet*. Internet Society. https://www.internetsociety.org/internet/history-internet/brief-history-internet

Liu, J. (2023). Rethinking Chinese multistakeholder governance of cybersecurity. In I. Johnstone, A. Sukumar, & J. Trachtman (Eds.), *Building an international cybersecurity regime: Multistakeholder diplomacy* (pp. 185–200). Edward Elgar Publishing.

Liu, J., & Cui, B. (2023). On the paradigm innovation of global governance in cyberspace. *Journalism & Communication Research*, *30*(7), 75–91.

Liu, J. (2020). China's data localization. *Chinese Journal of Communication*, *13*(1), 84–103. https://doi.org/10.1080/17544750.2019.1649289

Martynova, E., & Shcherbovich, A. (2024). Digital transformation in Russia. *Computer Law & Security Review*, *55*, Article 106075. https://doi.org/10.1016/j.clsr.2024.106075

Meng, Q. (2023, March 18). The establishment of the National Data Bureau will accelerate the construction of digital China. *IFENG NEWS*. https://cq.ifeng.com/c/8NzaXQDPi6m

Mueller, M. (2017). *Will the internet fragment?* Polity.

Mueller, M., & Grindal, K. (2018). *Is it "trade?" Data flows and the digital economy* [Paper presentation]. TPRC 46: The 46th Research Conference on Communication, Information and Internet Policy, DC, United States. http://doi.org/10.2139/ssrn.3137819

National Data Administration of PRC. (2024). *Explanations of common terms in the field of data (first batch)*. https://www.nda.gov.cn/sjj/zwgk/zcfb/1230/20241230160715745237413_pc.html

Novotny, E. J. (1980). Transborder data flows and international law: A framework for policy-oriented inquiry. *Stanford Journal of International Studies*, *16*, Article 141.

Obendiek, A. S. (2022). What are we actually talking about? Conceptualizing data as a governable object in overlapping jurisdictions. *International Studies Quarterly*, *66*(1), Article sqab080. https://doi.org/10.1093/isq/sqab080

OECD. (2023). *Moving forward on data free flow with trust: New evidence and analysis of business experiences* (Digital Economy Papers No. 353). OECD Publishing. https://doi.org/10.1787/1afab147-en

Oliver, G., Cranefield, J., Lilley, S., & Lewellen, M. (2023). Data cultures: A scoping literature review. *Information Research an International Electronic Journal*, *28*(1), 3–29. https://doi.org/10.47989/irpaper950

Oliver, G., Cranefield, J., Lilley, S., & Lewellen, M. J. (2024). Understanding data culture/s: Influences, activities, and initiatives: An Annual Review of Information Science and Technology (ARIST) paper. *Journal of the Association for Information Science and Technology*, *75*(3), 201–214. https://doi.org/10.1002/asi.24737

Simon, H. A. (1980). Cognitive science: The newest science of the artificial. *Cognitive Science*, *4*(1), 33–46.

State Council of the People's Republic of China. (2015). *Outline of action to promote big data development*. https://www.gov.cn/gongbao/content/2015/content_2929345.htm

Sun, Q., & Haritonova, Y. (2022). Legislative characteristics and trends of cross-border data flow in Russia in the context of data sovereignty. *Russian Studies*, *2*, 87–107.

The Central Committee of the Communist Party of China, & The State Council of China. (2020, March 30). *Opinions on building a more complete market-based mechanism for the allocation of factors* [Government document]. https://www.gov.cn/zhengce/2020-04/09/content_5500622.htm

Trachtenberg, D. (2025). *Digital trade and data policy: Key issues facing congress*. Congressional Research Service. https://crsreports.congress.gov/product/pdf/IF/IF12347

US Mission Geneva. (2024, July 26). *Statement by Ambassador María L. Pagán on the WTO e-Commerce Joint Statement Initiative*. https://geneva.usmission.gov/2024/07/26/statement-by-ambassador-maria-l-pagan-on-the-wto-e-commerce-joint-statement-initiative

Voss, W. G. (2020). Cross-border data flows, the GDPR, and data governance. *Washington International Law Journal*, *29*(3), Article 485. https://digitalcommons.law.uw.edu/wilj/vol29/iss3/7

Wang, R. (2018). Cognition and recommendations of cross-border data flow policies. *Information Security and Communications Privacy*, *3*, 41–53.

Wen, M., & Tan, R. (2024). Regulatory cooperation on cross-border data flows under the threshold of data sovereignty and China's response. *International Trade*, *6*, 5–14. https://doi.org/10.14114/j.cnki.itrade.2024.06.003

Xia, H. (2023). EU Progress in Legislation for Data Governance and Implications for China. *Wuhan University International Law Review*, *7*(4), 106–118.

Xu, D. (2018). International pattern of personal data cross-border flow regulation and China's response. *Legal Forum*, *33*(3), 130–137.

Zheng, Y. (2007). *Technological empowerment: The Internet, state, and society in China*. Stanford University Press.

Zhou, H., & Yan, W. (2025). The shift in U.S. cross-border data regulation: From free flow to secure flow. *Chinese Review of International Law*, *3*, 100–114.

Zhu, Y. (2024, November 21). Oumeng shuzigongping faan qianzhan. *Legal Weekly*. http://m.legalweekly.cn/whlh/2024-11/21/content_9089351.html

Zhuravlev, M. S., & Brazhnik, T. A. (2018). Russian data retention requirements: Obligation to store the content of communications. *Computer Law & Security Review*, *34*(3), 496–507. https://doi.org/10.1016/j.clsr.2017.11.011

About the Author

Jinhe Liu is an assistant professor at the School of Journalism and Communication, Peking University. He earned his PhD at Tsinghua University, focusing on Internet governance, medium governance, and communication theory. He has an interdisciplinary background in journalism and communication, law, and management, and is recruiting doctoral students.