Stanford | Geopolitics, Technology, and Governance
Freeman Spogli Institute

DIGICHINA

Moving Data, Moving Target

Uncertainties remain in China's overhauled cross-border data transfer regime

BY
Samm Sacks
Krystal Chen Zeng
Graham Webster

October 25, 2024

digichina.stanford.edu

1. Introduction

On March 22, 2024, the Cyberspace Administration of China (CAC) unveiled the current version of China's rules governing outbound data transfers. The new "Provisions on Promoting and Regulating Cross-Border Data Flows" (or "2024 Provisions") took effect immediately and eased restrictions affecting many businesses, while still underscoring the strength of the CAC's authority over high-risk areas.[1] For companies conducting data transfers falling within new exempted categories, the regulations brought relief after years of daunting uncertainty. Long reporting cycles, extensive preparation of materials, and long wait times for audit results had created seemingly insurmountable obstacles for businesses relying on data flows, leading to deep pessimism about China's business environment.

The new rules, which eased burdens for some and pointed to possible solutions for others, were the latest chapter in a long story of regulatory uncertainty, and they won't be the last. When the Cybersecurity Law was finalized in 2016, it indicated that government approval would be needed before certain transfers of data out of China. The 2021 Personal Information Protection Law expanded these requirements, but specific regulations were left to regulators who had not yet provided details. In 2022, the CAC at last finalized regulations to fill the gap (the Outbound Data Transfer Security Assessment

[1] Chinese-language name: 《促进和规范数据跨境流动规定》. Original source: https://www.cac.gov.cn/2024-03/22/c_1712776611775634.htm Unofficial English translation: https://www.chinalawtranslate.com/en/Provisions-on-Promoting-and-Regulating-the-Cross--Border-Flow-of-Data/

Acknowledgements: The authors wish to thank Jamie Horsley for her generous comments and many others who shared their observations on these topics over the years.

Measures, or "2022 Measures"[2]), but as enforcement slowly moved forward, frustration was widespread. A year after the 2022 Measures took effect, it looked as if the government was listening, if not also experiencing the frustration of a high administrative burden themselves: In September 2023, the CAC issued draft Provisions that would replace the cumbersome Measures. As specialists from the international law firm Covington wrote in a representative commentary at the time, "[i]f adopted in the current form, the draft Provisions could significantly reduce the burden that companies have faced in the past few months." And that draft was mostly identical to the 2024 Provisions now in effect. (See, however, a potentially significant change below under "The importance of 'important data.'")

Prominent Chinese legal academics portrayed the revision as a move to ease cross-border business. Hong Yanqing, a professor at the Beijing Institute of Technology who has long been involved in China's cyberspace policy-making, interpreted the 2024 Provisions as the outcome of Beijing's effort to "rebalance" economic and security objectives. Zhou Hui of the Chinese Academy of Social Sciences wrote that the Provisions align with this year's State Council work report presented to the National People's Congress, which emphasized the need to align with high-standard international economic and trade rules. Peking University Law School Professor Wang Xixin noted the new rules' diplomatic message, pushing against the perception that China's data rules overemphasize data localization.

The 2024 Provisions indeed depart from the 2022 Measures in significant ways that signal an orientation toward greater openness. Yet there are significant areas of uncertainty that remain unresolved and will determine whether the changes prove meaningful in practice. First, the 2024 Provisions introduce new areas of ambiguity when it comes to so-called "*important data*." Second, at present, many domestic and foreign companies in China operate at a *scale of data transfers* too large to qualify for the Provisions' new openings, meaning these companies see limited relief and may face the choice of costly redesign of company systems or pulling business lines out of the Chinese market. Third, while *free trade zones (FTZs)* in China may establish rules that further ease restrictions for individual industries or extend relief to larger-scale operators, authorities have yet to fully clarify how companies may qualify for these benefits, for example by reincorporating or establishing data centers within a

[2] Chinese-language name: 《数据出境安全评估办法》. DigiChina English translation and original text: https://digichina.stanford.edu/work/translation-outbound-data-transfer-security-assessment-measures-effective-sept-1-2022/

given zone. Fourth, how bureaucrats interpret concepts such as the "*necessity*" of a data transfer remains unclear, and the outcome will determine the extent to which firms need to redesign global systems to isolate Chinese data and infrastructure. Finally, as companies seek approval for transfers, how permissive regulators are *in practice* could further lessen pessimism about cross-border business, or it could reinforce worst fears.

This essay takes up important data, the question of scale thresholds for data transfers, the FTZ situation, and the question of "necessity" to understand the knowns and unknowns in China's increasingly but not completely solidified cross-border data regime. It is a snapshot of China's outbound data transfer regime at the time of publication, both analyzing the regulatory text and chronicling expert opinion, especially inside China. It also notes remaining uncertainties and starts from the proposition that China's cross-border data regime is likely to continue to evolve, not least in the FTZs where new frameworks are just starting to emerge, but also through the actual exercise of regulatory discretion.

Read more:

This work builds on earlier DigiChina analysis over the last five years, tracing the evolution of China's data governance regime, from the uncertainty in the wake of the Personal Information Protection Law and the Data Security Law (2021) to the interplay between actions taken by Beijing and Washington in "Mapping Data De-Risking" (2024).

2. The importance of 'important data'

In China's regulation of cross-border data flows, "important data" (ID) is of the utmost importance. When the Cybersecurity Law took effect in 2017, it contained a provision in Article 37 requiring that ID gathered or produced by operators of "critical information infrastructure" (another novel term) be stored within China and that, before transferring such data abroad, a security assessment be undertaken in accordance with then-forthcoming regulations. The 2022 Measures and the 2024 Provisions are both in part designed to implement that general requirement.

It has therefore been more than seven years since what qualifies as ID became a crucial question for data handlers in China. Under the 2022 Measures, all data handlers had to undergo mandatory security assessment before transferring ID abroad. What constituted ID, however, was never totally clear, leaving individual organizations to make risk calculations, in some cases voluntarily refraining from transferring certain data abroad just in case it might be deemed ID.

That uncertainty seemed likely to decrease drastically with the 2023 draft Provisions, which suggested the government would notify data handlers if they

held any important data. In the final Provisions, however, the CAC introduced an added element of uncertainty. According to Article 2 of the 2024 Provisions: "Data handlers shall identify and declare important data in accordance with relevant provisions. Where relevant departments or localities have not issued notice or openly published that something is important data, data handlers need not file for an outbound data transfer security assessment for important data."[3]

It is possible to interpret Article 2 to mean that companies may be responsible for identifying and reporting on their own whether they have ID, even in the absence of notification by authorities. The CAC could be signaling that the understanding of ID has become a shared responsibility between data handlers and authorities. As Zhang Peng, author of the *Geotechnopolitics* newsletter, wrote: "The national security faction within China's policy circles evidently believes that if some institutions do indeed have important data that the relevant departments or regions have not notified, and if the enterprises themselves do not proactively identify and declare such important data, this could pose a significant national security risk."

It is also possible to read Article 2 to mean that, absent notification by authorities, data handlers don't need to worry about ID-related rules. The fact is that the two seemingly contradictory thoughts in Article 2 are equally present in the text, and government practice or guidance has not appeared to clarify matters.

The mixed message does not appear to be a mistake. Newly finalized Network Data Security Management Regulations, announced in September 2024 and effective in January 2025, include corresponding language in Article 29 that charges authorities with developing ID catalogs and notifying data handlers when ID is identified, while also requiring data handlers to identify and declare ID to authorities. Authorities may also be signaling that they will adopt a narrow and targeted interpretation of ID in these regulations, however. According to Zhang's analysis, the definition of ID in the Network Data Security Management Regulations emphasizes its "specificity" and "precision" in relation to national security.

A body of domestic standards in China may offer further information, if not total clarity, and a new standard this March from TC260, a body that develops standards related to IT security, provides one such reference. Section 6.5b and Appendix G of the "Rules for Data Classification and Grading" offer further

[3] Our translation. Chinese-language original: "数据处理者应当按照相关规定识别、申报重要数据。未被相关部门、地区告知或者公开发布为重要数据的，数据处理者不需要作为重要数据申报数据出境安全评估。"

information on identifying ID.[4] Appendix G postdates and may be seen as replacing TC260's 2022 Guideline on Important Data Identification.

Finally, there is the matter of when personal information, a category of data mostly regulated under the 2021 Personal Information Protection Law, may be categorized as ID. Article 5 of the 2024 Provisions identifies situations in which personal information will be "exempt" from pre-approval measures (i.e., security assessment, standard contracts, or personal information certification) prior to outbound transfer. But it states that the exemptions do not cover personal information that is deemed to be ID. In other words, if for any reason data is deemed ID, the fact that it is also personal information does not exempt it from restrictions targeting ID.

As the language and practice around ID evolves, businesses and other organizations may find relief in signals that authorities intend to implement these rules with an eye toward precision, especially as economic pressures loom. At this stage, what is clear is that regulators will have ample space to explore their own interpretations.

3. Little relief for large-scale data handlers

One of the significant differences between the September 2023 draft and the final version of the 2024 Provisions is that authorities increased the volume thresholds for personal information above which security assessments, standard contracts, or certifications are required before transfer out of China.

Since the 2022 Measures, China's outbound data regime has treated personal information differently depending on how many individuals' data is at issue. The 2022 Measures required a security assessment for transferring (non-sensitive) personal information of more than 100,000 people. The 2024 Provisions, on the other hand, only requires security assessment for data transfers covering over 1 million people. For transfers less than one million and greater than or equal to 100,000 individuals, a standard contract or certification is required. Non-sensitive personal information of less than 100,000 individuals is exempt from any required mechanism and can be freely transferred.

This change alleviates burdens for small and medium-sized companies, suggesting that authorities sought to allow more business data to flow out of China and indicating the authorities may have been responsive to some business concerns. Bureaucrats charged with processing security assessments would also

[4] Chinese-language name: GB/T 43697-2024《数据安全技术 数据分类分级规则》. Copy available at http://c.gb688.cn/bzgk/gb/showGb?type=online&hcno=F0C385EDC38CBF277AEC021F23126ADE

see relief. Compounding the relaxation of requirements embodied in the higher threshold, the 2024 Provisions also measure data volume over a shorter time frame, only counting data transfers since January 1 of the current year, for a maximum coverage of 12 months. The 2022 Measures, on the other hand, had counted from the beginning of the previous year, meaning a full 24 months of data transfer activity would count against the threshold by the end of any calendar year.

	2022 Measures (superseded)	2024 Provisions (in effect)	Requirements before transfer abroad
Scale of data	100,000 or more individuals since the beginning of the previous year	1 million or more individuals since the beginning of the current year	Security assessment
		100,000–9,999,999 individuals since the beginning of the current year	Conclude a standard contract or provide a certification.
	Less than 100,000 individuals since the beginning of the previous year	Less than 100,000 individuals since the beginning of the current year	None

While small and medium-sized operations are likely relieved, it is not hard to exceed 1 million users worth of data in a market where an estimated 1.09 billion people are online. For many major domestic and foreign companies who operate at million-plus scale, therefore, the specter of an uncertain security assessment process remains.

4. Freer trade in data, if you're 'in the zone'

The 2024 Provisions offered a new potential avenue for organizations to lower their cross-border data regulatory burden through "free trade pilot zones" (FTZs, 自由贸易试验区) around China that may establish regulations that differ from the standard national regime. The Provisions point to the use of "negative lists" and "positive lists" by FTZs to provide greater clarity. The concept of a negative list comes from foreign investment, in which certain sectors are restricted or closed for outside investors, while non-listed sectors are unrestricted. In other words, where a negative list governs investment, the default is openness unless listed. In the context of data flows, the idea is that local FTZ authorities can identify categories of data subject to transfer requirements (security assessment, standard contracts, or certification) and all other data would be generally permitted to flow. This marks a more liberal approach compared with a positive list (also called a whitelist)—which leaves restrictions in place except in sectors or under conditions enumerated on the list.

According to Zhao Jingwu, a law professor at Beihang University, this development is an extension of a 2023 State Council Opinion calling for a "list of general data that can freely flow" (可自由流动的一般数据清单)—essentially a

positive list. He also notes the upcoming rules in free trade zones might inform further exemptions at the central level. Hong Yanqing writes that the data list system aims to advance China's participation in international trade negotiations, allows the government to adjust policy more quickly than in laws or broadly applicable regulations, and seeks to streamline compliance for both regulated entities and government departments. Amidst broad and still vague legal provisions, the combination of negative lists and FTZs could present a more welcoming face to those who need to transfer data across borders.

Reflecting a longstanding Chinese governance pattern of local experimentation and delegation of some powers to localities, the ability of FTZs to create their own rules for cross-border data transfers (with the approval of provincial cyberspace and informatization authorities) provides considerable potential for variation and specialization of zones. These localized rules are also likely to be dynamic, with the Shanghai FTZ Administration Committee's for instance giving its list a one-year period of validity. Any novel arrangements could be renewed—or not.

FTZs are now actively issuing new rules, moving away from a one-size-fits-all volume threshold toward a more nuanced, contextualized approach with specific regulations for different scenarios, types, and volumes of data. So far in 2024, Beijing, Shanghai, Tianjin, and Fujian have been at the forefront of releasing their data lists. Tianjin led on May 9 with the first negative list, followed by Shanghai's positive list on May 17. August 26 saw simultaneous developments: the Beijing FTZ released a negative list and rules for identifying ID, while Fujian Pingtan FTZ issued a positive list. Already there is significant variation. For instance, among the four FTZs that have published their lists, Beijing has set the most favorable volume thresholds for cross-border transfers of sensitive personal information in retail and pharmaceutical industries. In contrast, Shanghai and Pingtan have not adjusted their data export volume thresholds, instead simply enumerating specific types of general data that can be freely transferred across borders.

Even as FTZ data-transfer rules have begun to roll out, there are a variety of uncertainties as to how this kind of flexibility will unfold. First, it is unclear in what ways FTZs will be able to deviate from nationwide policies. The 2024 Provisions note that FTZ rules must be established "under the framework of the national categorized and graded protection system for data," a broader effort to categorize data by type and level of sensitivity, suggesting that the motivations of

data transfer rules should be aligned, even if the modalities are not the same.[5] Moreover, the level of autonomy enjoyed by FTZs overall is developing in recent years, with the 2023 revision of China's Legislation Law specifically naming Shanghai and Hainan as areas where local officials have regulatory power (see Art. 84). In both of these localities, there may be more room for deviation from the national regime, but that flexibility is not total and the mechanisms for central supervision or review of these local regulations can be opaque and remain an area of active study among Chinese scholars. It is also unclear to what extent other FTZs can look to Hainan and Shanghai as examples or whether their freedom of action will be comparatively limited.

Second, what a business or other data handler will have to do to qualify for advantageous data transfer rules set by an FTZ remains an open question. The positive lists in Shanghai and Pingtan may only require companies to register and conduct business activities within the FTZ, without restricting where in China the data originates. Could foreign firms registered elsewhere transfer data to subsidiaries or third-party companies incorporated in the FTZs to enjoy a relaxed outbound data regime? Will every FTZ treat the location of data centers or offices the same? The answers are not yet known and the practical implications are significant: Moving corporate registrations or administrative offices might be feasible for some, but large-scale data centers are not so simple to relocate.

Third, while FTZs generally appear motivated to attract business activity by making rules that ease burdens, the localized regulations can also create procedures or obligations that present their own uncertainties. For instance, while signaling specific areas of increased openness through positive lists, Pingtan also established additional risk assessment procedures and Shanghai also noted other "managerial requirements" to be met.

Finally, although the 2024 Provisions provide increased room for experimentation in FTZs, there remain certain cross-border data transfer activities in gray areas that the data lists and CAC regulations cannot fully address or exempt. These include national security-related activities such as international criminal investigations and co-regulated areas like medical and financial data transfers, which all involve powerful parts of the bureaucracy outside the CAC.

In the months since the 2024 Provisions were announced and implemented, FTZs have begun to develop differential data transfer regimes, but the real

[5] DigiChina's translation. See the 2021 Data Security Law: https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/#_ftn9

operational implications for businesses and other organizations are yet to be seen as local regulations roll out and the realities of the policy become clear through practice.

5. Who decides what is 'necessary'?

Since the inception of China's outbound data transfer regime as captured in Article 37 of the Cybersecurity Law, organizations have been envisioned as having legitimate grounds to transfer covered data only when "truly necessary" (确需). In the 2024 Provisions, the exceptions in Article 5 that suggest significant relief for normal business operations similarly apply if the transfer is "necessary." Who decides what is necessary, and how?

Will authorities defer to companies and organizations definition of what constitutes "necessary" transfers for their global operations, or will they make their own determination based on a weighing of national security, economic, or other factors? The answer to this question remains unknown. Similarly, it will take time for companies, law firms, and eventually the public to get a sense of how authorities are generally processing outbound data transfer cases. Businesses will be happier if they see timely and relatively permissive practices, and they will be more pessimistic if they hear stories of drawn out processes or a tendency to deny. The reality of bureaucratic discretion limits how predictable China's outbound data transfer regime can be.

6. Conclusion

While China's cross-border data regulatory regime has evolved significantly over the last year, providing relief from burdensome requirements for some, this narrow area of policy and the broader field of data governance in China is not standing still. The questions discussed above—about how ID as a category will shape data flows, how regulators will treat large amounts of data, policy innovation in FTZs, and the role of "necessity" in allowing data transfers—are all areas that businesses and scholars will continue to watch. How regulators operate in practice will gradually provide concrete insight.

China's broader data governance framework is also evolving with the introduction of the National Data Administration, a new office under the powerful National Development and Reform Commission whose role in shaping regulations or enforcement is not yet clear. Local data management bureaus are also cropping up in different forms and with different levels of authority. Legal

scholars and practitioners in China are meanwhile studying potential conflicts between the texts of different national and local laws and regulations.

The salience of data in developing artificial intelligence and the intense drive from industry and government to unlock the economic value of data are powerful currents in China today. So too are the consciousness that China faces security challenges at home and abroad, and the sense that unprotected data could be a national vulnerability. In outbound data flows and other policy areas, Chinese government actors will continue to adapt to these and other drivers of action. Releasing the 2024 Provisions so soon after the 2022 Measures had proven problematic was a strong signal that officials believed the data gates had closed too far. In the coming months, we will find out how far open, and to whom, they will be for the time being.

About the Authors

SAMM SACKS is a Senior Fellow at New America and Yale Law School's Paul Tsai China Center. She is also a Senior Fellow for China with the Cross Border Data Forum.

KRYSTAL CHEN ZENG is a Research Associate of the Paul Tsai China Center at Yale Law School based in Beijing. She is concurrently pursuing her Ph.D. at China's University of Political Science and Law (CUPL).

GRAHAM WEBSTER is a Research Scholar in the Program on Geopolitics, Technology, and Governance at Stanford University and Editor-in-Chief of the DigiChina Project.

About DigiChina

The DigiChina Project is a collaborative effort to analyze and understand Chinese technology policy developments through direct engagement with primary sources, providing analysis, context, translation, and expert opinion. It is based at Stanford University, housed within the Program on Geopolitics, Technology, and Governance at the Freeman Spogli Institute for International Studies. More at digichina.stanford.edu.

Stanford | Geopolitics, Technology, and Governance
Freeman Spogli Institute