How American Companies are Approaching China's Data, Privacy, and Cybersecurity Regimes

Antonio Douglas and Hannah Feldshuh

April 2022

THE US-CHINA BUSINESS COUNCIL
美中贸易全国委员会

Executive Summary

Over the last five years, China has constructed vast data, privacy, and cybersecurity regimes in the hopes of protecting personal data and strengthening national security. While many countries have also begun regulating data more tightly, the environment in China is uniquely restrictive. New laws, regulations, and standards are particularly challenging for multinational firms operating in China because their operations, products, and services rely on fast and fluid cross-border data flows. The US-China Business Council (USCBC) has spoken with over 30 American companies to better understand their data, privacy, and cybersecurity compliance challenges as well as their plans for dealing with policy uncertainty in this important market.

Core Challenges

- Data localization, prescriptive cybersecurity rules, and restrictions on cross-border data flows: A combination of data localization rules, prescriptive cybersecurity requirements, and cross-border data transfer security–review requirements makes China one of the most restrictive major economies in data and cybersecurity governance. Draft policies stand to further this trend, significantly increasing the cost of doing business in China, disrupting global systems, and limiting the types of goods and services foreign companies can bring to the country.
- Regulatory ambiguity: The practical details of several of the most consequential laws and regulations are unclear or undefined, including the definitions of key terms, the agencies of jurisdiction, whether rules are mandatory or voluntary, and the scope and thresholds of data localization and cross-border data transfer reviews. While USCBC expects these rules to be published in the future, companies are already experiencing associated enforcement challenges.
- Inconsistent regulatory enforcement: Companies increasingly report pressure to comply with regulations despite the lack of practical steps for doing so. The level and type of enforcement vary across both regions and industries, leaving companies unsure how to comply.

Companies' responses to this evolving legislative and regulatory landscape vary greatly depending on the industry and types of data they collect in China. At minimum, all interviewed companies indicated that they are mapping their data flows and assessing their business structure for any necessary adjustments.

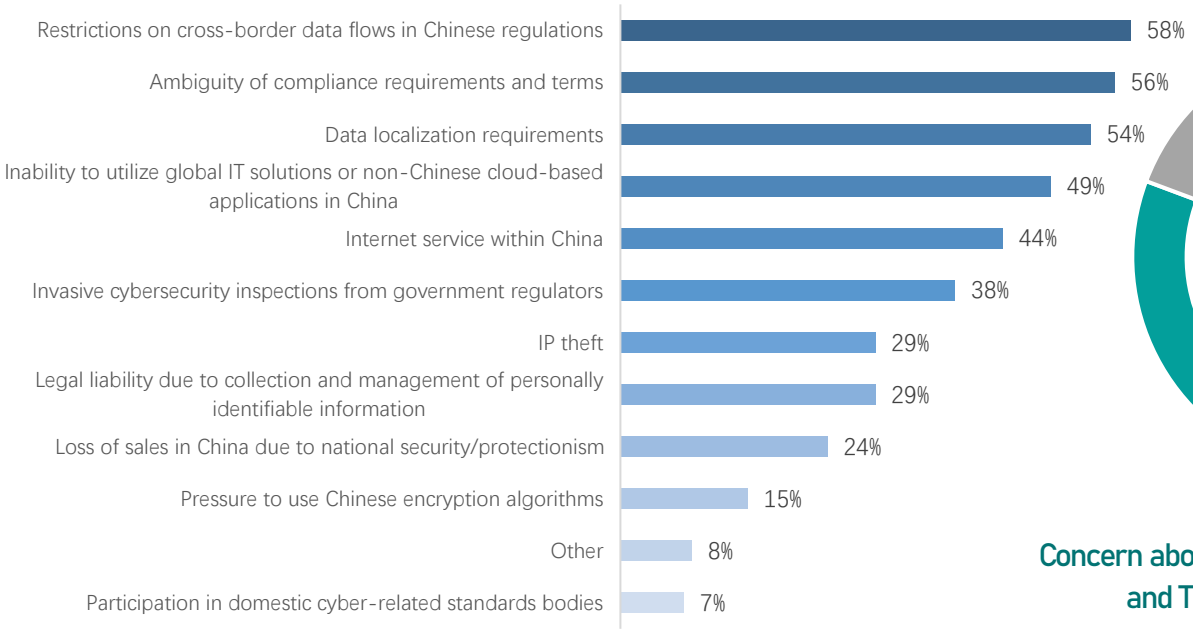
The long-term consequences of China's data, privacy, and cybersecurity regimes remain to be seen. If the policies are implemented rigidly, a possible outcome is the creation of data islands that force companies to localize technology, people, and processes, disconnecting them from global operations. This could force companies to make separate product offerings or conduct separate research and development in Chinese and global markets. This range of impacts might hurt the competitiveness of China's business environment to the detriment of Chinese consumers, corporate competitiveness in China, and the country's integration with the global economy.

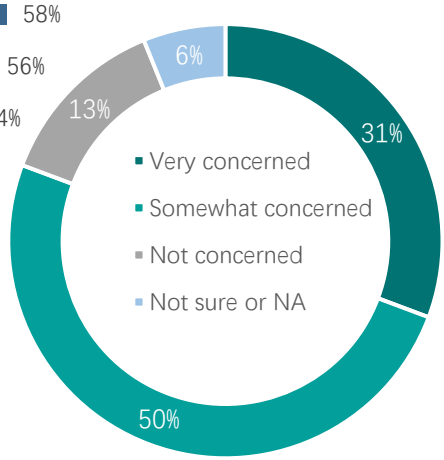
Table of Contents

Introduction

In an era when data are essential business resources, all countries are seeking to balance the need for legitimate data, privacy, and cybersecurity safeguards with the imperative to encourage economic dynamism and growth. China is no different. There, policymakers have exerted tremendous effort over a short period to tackle this complex balancing act. Since China's Cybersecurity Law (CSL) went into force in 2017, regulators from across departments have been closely examining needs regarding data, privacy, and cybersecurity, thereby articulating standards for the government, businesses, and individuals.

Concerns about Cyber-Related Issues





Concern about China's Information Flow and Technology Security Policies

Over time, US companies have grown increasingly concerned with the uniquely restrictive directions in which China's data, privacy, and cybersecurity regimes are moving. Since 2015, an average of more than 80 percent of respondents to USCBC's annual member surveys have expressed concern about Chinese policies and regulations on privacy, data, cybersecurity, and information flows. Businesses are particularly concerned with lingering ambiguity regarding data localization, cybersecurity requirements, and cross-border data transfer reviews. While Chinese regulators have devoted considerable time and attention to answering questions, key definitions and processes remain undefined. Against this backdrop, American businesses face increasing operational challenges as they navigate these still-evolving regimes.

Methodology

This report is derived from approximately 30 interviews with USCBC member companies across the information communication technology (ICT), hospitality, health care, energy, apparel, manufacturing, transportation, financial services, and automotive sectors. The breadth of industries demonstrates how widely these concerns are shared beyond just the ICT space. Company representatives were asked standardized questions that covered cybersecurity, privacy, data localization, and cross-border data flows.

The Data and Privacy Legal Landscape

The 2017 enactment of China's CSL raised many concerns around how the country's policies on data, privacy, and cybersecurity would impact foreign businesses. As various rules and standards were published over the following years, many concerns about the direction the CSL might take China's policy environment have come to pass.

These concerns are now compounded by the 2021 enactment of the Data Security Law (DSL) and the Personal Information Protection Law (PIPL). These laws expanded the scope of restrictions without providing companies the clarity needed to fulfill their obligations. Together, they provide the foundation of China's data and privacy regimes as well as its cybersecurity grading system, which is discussed later in this report. The Cyberspace Administration of China (CAC), the Ministry of Industry and Information Technology (MIIT), and the Ministry of Public Security (MPS) are the key regulators of all three laws.

The legislative landscape features numerous unfinalized regulations and implementing measures as well as hundreds of additional standards that inform companies' data management. A catalog of key legislation and regulations is available in the appendix.

Cybersecurity Law

Effective since June 2017

The CSL is the seminal law for all cybersecurity-related legislation in China. The law delineates the responsibilities of the state and companies for content control, privacy, IT security, and data.

Scope: The law applies to network operators, which are entities that construct, operate, maintain, or use networks in China.

Data localization and cross-border flow: Operators of critical networks known as critical information infrastructure (CII operators) in China must store personal information and important data locally and undergo a security review before these data are transferred abroad.

The Multi-Level Protection Scheme: All network operators must grade their systems on a five-level scheme known as the Cybersecurity Multi-Level Protection Scheme (MLPS 2.0). Systems graded at a higher level are subject to more stringent compliance requirements and external reviews.

Cybersecurity review: Critical networks must undergo government security reviews prior to purchasing products or services that could impact national security.

Personal information restrictions: Network operators should not collect information beyond the scope of their service and must obtain consent from individuals whose personal information is being collected.

Data Security Law

Effective since September 2021

The DSL imposes new obligations on the government's and industry's interactions with data. "Data" encompasses essentially all information in both electronic and nonelectronic forms.

Important data: The DSL empowers industry regulators at the central and local levels to create industry-specific catalogs of important data according to the risk those data pose to national security, economic security, and people's livelihoods if compromised. Despite the release of some sector-specific regulations, it is currently unclear what data will ultimately comprise the important classification.

Expanded cross-border restrictions: The DSL expands cross-border data transfer restrictions beyond CII operators, as required by the CSL, to include "general operators," which ostensibly include any company or organization that handles important data.

Data security review: The law establishes a data security review system for cross-border transfers that might impact national security.

Data classification: A comprehensive data classification system that categorizes data according to the harm that could be caused if they are tampered with, destroyed, leaked, etc., is to be established.

Geographic scope: While the DSL primarily applies to organizations and individuals inside China, it also includes an extraterritorial component granting limited authority to penalize those outside mainland China when they are found to engage in data activities that harm the country's national security interests.

Personal Information Protection Law

Effective since November 2021

The PIPL establishes privacy rights and obligations for users, regulators, and data processors. Of the three primary cyber laws, the PIPL is arguably the most fleshed out, likely due to inspiration drawn from the European Union's General Data Protection Regulation (GDPR).

Volume-based thresholds: The PIPL introduces low volume thresholds that trigger data localization and cross-border transfer-security review requirements.

Cross-border data flows: The PIPL also expands conditional restrictions on the cross-border transfer of personal information and allows a transfer if operators meet one of three circumstances: 1) have a standard contract with data recipients, in-line with government regulations, 2) undergo certification from qualified agencies, or 3) undergo a cross-border security review conducted by government agencies. It further expands the scope of CAC-led security assessments of cross-border data transfers from just covering critical networks to companies with a certain volume of personal information.

Consent: The PIPL specifies that consent is the primary legal foundation for collecting personal information, and the law lacks exceptions for "legitimate interests" present in other jurisdictions.

Geographic scope: The PIPL primarily applies to entities that conduct personal information–processing activities within China but also includes an extraterritorial component that would allow Chinese authorities to penalize those outside the country who violate privacy rules in limited circumstances.

Key Data and Privacy Concerns

A 2021 Information Technology and Innovation Foundation report indicated that China has the most data-restrictive regime in the world, with 29 policies currently promoting de facto or forced data localization. Further, the World Bank's World Development Report 2021 found that China was among only 11 countries that have adopted a limited transfer approach to cross-border data flows.

Interviews with USCBC member companies echo these findings. Among issues related to data, privacy, and cybersecurity, companies across all industries have expressed the highest level of concern with China's requirements that they localize data and undergo security assessments to transfer data abroad. Members report that the resulting disruptions to normal global operations can often only be resolved by placing duplicative technology, people, and processes in China and making costly adjustments that make the companies less competitive vis-à-vis domestic Chinese competitors. In some cases, this prevents companies from bringing advanced or newer generation products to market in China.

For global companies, seamless cross-border data flows are essential to daily business operations, cybersecurity risk management, compliance in China and third markets, product safety and servicing, research and development, and due diligence (such as anti-money laundering and counterterrorism financing in the financial sector).

Cross-border data transfer restrictions

Cross-border data flow restrictions ranked highest among cyber-related issues of concern in USCBC's 2021 Member Survey, with 58 percent of companies indicating concern. Restrictions on cross-border data flows disproportionately harm the operations and competitiveness of foreign businesses in China that leverage global infrastructure with consistent, company-wide practices. As Chinese firms continue to grow and expand overseas, restrictions on data flows will similarly harm their development.

Current regulations stand to restrict cross-border data flows from China to other markets in a variety of ways, including by requiring government-authorized security reviews prior to transfer, directly prohibiting the transfer of certain data types, and requiring extraneous and separate consent from users. This level of government oversight over company operations is not common outside China. Uncertainty as to how these reviews will be implemented creates compliance ambiguity for companies across sectors.

Case study: Data transfer concerns prevent companies from bringing cutting edge technology to China

A leading medical device manufacturer indicated that it wanted to develop a remote program to manage its products in China, allowing for remote adjustment via 5G technology. The process of remote adjustment would have required the continual and free flow of data between China and engineers abroad. Ultimately, the company's headquarters determined that the likelihood of disruption to crucial cross-border data flows made offering this product too complex, costly, and potentially unprofitable. This unfortunate reality limits the ability of foreign companies to bring innovative products to market and deprives Chinese patients of leading health care technology.

At the time of USCBC's interviews, no respondent had yet undergone a government-led security assessment of its cross-border transfer of personal information and important data as legally required under the CSL, the DSL, and the PIPL, as the defining rules are still in draft form.

Additionally, most businesses indicated that they are waiting for further information regarding how "important data" will be defined in their sector. Government security reviews theoretically offer a suboptimal avenue for transfers abroad, though members report that the grounds, scope, frequency, and requirements of review remain unclear and that the reviews might raise privacy concerns over proprietary data. As regulators attempt to take on this new responsibility in the absence of transparent and predictable processes, businesses fear that they could be subject to arbitrary and sudden termination of their cross-border data transfers as well as fines, takedown notices, and public reprimands for unpredictable violations similar to the 2021 naming and shaming of top technology companies.

Duplicative systems and staffing caused by data localization

USCBC's 2021 Member Survey found that 54 percent of companies were concerned about data localization requirements. Global companies approach their data infrastructure as an integrated resource, using global data networks to innovate and provide top-quality services. Data localization requirements disrupt this process and often necessitate the duplication of these systems, significantly increasing the cost of operating in China while disconnecting a company's China operations from its global IT infrastructure. A 2021 Congressional Research Service study found that computing costs in markets with localization requirements are 30–60 percent higher than in open markets. Examples of these costs include investing in duplicative domestic data centers and research and development hubs as well as requiring additional IT, human resources, legal, and research personnel to staff these centers.

Cross-border data transfers limit product troubleshooting, which disadvantages foreign firms

According to USCBC's 2021 Member Survey, 49 percent of respondents are concerned with the inability to utilize global IT solutions or non-Chinese, cloud-based applications in China. Companies with globalized systems might face delays or restrictions due to cross-border data transfer requirements when updating operating systems or directly interfacing with customers. In comparison, domestic firms that are not concerned with cross-border restrictions are able to respond proactively to localized troubleshooting or demand. In terms of software, members also indicated that local troubleshooting and support are often unavailable as a result of data localization practices.

Data localization's impact on cybersecurity

Data localization could also negatively impact a company's ability to manage cybersecurity risks. Localization requirements stand to reduce the resiliency of platforms and applications as compared to spreading resources across multiple countries. These requirements also add to IT and data complexity given the up- and downstream impacts on interfacing systems and would make cybersecurity safeguards unscalable and less effective.

Data fully stored within one jurisdiction are at increased vulnerability to hacking, and the practice results in decreased systems resilience. A Georgia Institute of Technology study found that data localization creates negative cybersecurity risks in a variety of ways:

> *"First, data localization creates obstacles to integrated management of cybersecurity risk within a single organization, such as a corporation or government agency. Second, data localization creates obstacles for an organization in using cybersecurity-related services from outside of the organization. Third, apart from cybersecurity services, data localization creates obstacles to information sharing between organizations, and information sharing is an important tool for reducing cybersecurity risk."*

Conflating personal information with important data

China applies the same restrictions and controls to a set volume of collected personal information that it does important data, a trend that could impact companies with large amounts of personal information, especially consumer-facing companies. Personal information and important data are two distinct concepts with differing challenges. "Important data," while still not fully defined, is intended as a categorization of data that require the highest level of protection. These include national security-related information that stands to impact China's social, political, and economic integrity. In contrast, personal information has a sliding scale of sensitivity that is largely based on volume. Equating personal information with important data diverges from global practice and creates significant compliance challenges. Basic information, such as names and email addresses, is less damaging to the consumer if leaked than financial or biometric information.

The draft Network Data Security Regulation, published in November 2021, is among several policies that explicitly link rules regarding the treatment of 1 million sets of personal information with the treatment of important data. This draws an arbitrary connection between company management of mostly consumer data with company management of national security–relevant data. This approach also runs counter to the legislative precedent of managing both concepts separately, and it places an undue burden on businesses and regulators. Such correlation of personal information and important data essentially subjects all data collected by a reasonably sized corporation—regardless of the sensitivity level—to costly and

Personal information regulations increase compliance burden for hospitality industry

Equating personal information with important data is particularly problematic for sectors that process a large volume of it. For example, hospitality companies are particularly vulnerable to running afoul of increasingly stringent privacy regulations, as they constantly and intensively use customer data. Hotels have long faced requirements to register guest data with local security bureaus in China. Under new regulations regarding personal information, they now face additional scrutiny from regulators about their data practices due to the volume of personal information processed. As a result, virtually all large hotels are or will be subject to personal information volume thresholds, which impose obligations equivalent to important data requirements. These obligations include investing in costly hardware across hotels, undertaking new auditing practices, and hiring additional data governance personnel.

time-consuming practices without a clear rationale. Continuing this trend without resolving these contradictions will only obfuscate companies' compliance burdens and potentially lead to uneven enforcement by regulators.

Ambiguous legislation and regulatory enforcement

In USCBC's 2021 Member Survey, 56 percent of member companies highlighted ambiguity in China's data and privacy regimes as a concern. The conflicting regulations and lack of clear guidelines significantly hinder proactive compliance and might leave companies unable to understand their obligations until they face an enforcement action. Policymakers have yet to provide a final working definition for "important data," nor have they clarified cross-border data transfer rules or consistent volume thresholds for personal information, all concepts meant to undergird and guide the regimes. This is despite the fact that rules invoking these concepts are already in effect and enforceable. For example, Chinese authorities have conducted campaigns targeting companies that infringe on privacy rights, forcing hundreds of mobile apps to cease operations or reconfigure their structure. While most of the companies implicated so far have been Chinese, more than one foreign company has been impacted. The authorities' explanation of the companies' violations was vague, such as the "overcollection" or "abuse" of personal information, bringing little clarity to the confusion around compliance burdens.

Companies that have experienced compliance challenges related to personal information also note that voluntary standards are often enforced as mandatory. In particular, authorities reference the Notice on Minimum Personal Collection and the Personal Information Security Specification, which are voluntary standards. Companies also note that both documents are vague, exacerbating the issue of regulators treating them as mandatory. These companies indicated that even after consulting with the relevant regulator, they were unsure of how they could have anticipated or prepared for the scenario.

USCBC member experiences indicate that timelines to rectify offenses—at times, only 15 days—are often arbitrary and/or unworkable for a global business with engineers in multiple time zones who may need to translate regulator guidance. During app takedown requests, companies were often unable to reach regulators for additional clarification for days at a time.

Conflict with standards used in other markets

USCBC members operate across global markets with differing privacy requirements. Most companies are familiar and compliant with the European Union's GDPR and are able to compare their compliance preparation process between it and China's PIPL. However, China's framework does not fully align with the GDPR and other international frameworks and equivalents, particularly with regards to key definitions, cross-border data transfer requirements, and the blending of national security and privacy rules. This mismatch increases compliance costs and raises the risk of unnecessarily duplicating security measures.

Among the biggest discrepancies between China's privacy legislation and other market standards is a requirement for "separate consent." The PIPL requires separate consent, which effectively means that companies must obtain agreement from users every time their personal information is used for a different purpose, whereas the GDPR allows for consent to apply to several sub-processes if they serve the same purpose. It is unclear if the notion of purpose under the PIPL will allow for the same possibility. If a user in

China withdraws consent before the business completes their contractual obligations, it is unclear if those services can still be provided in China. For example, if a consumer uses a banking service that subcontracts with a third party to provide security or verification services, the consumer could opt to deny the third-party access to their data mid-transaction, preventing the transaction from being processed. At present, businesses say that they have not seen stringent privacy enforcement related to third-party vendors, but they anticipate disruptions once a standard contract for transfer of personal information overseas is released. While this feature does not solely impact foreign business, separate consent more directly limits multinational companies, which have complex operations, vast supply chains, and global footprints.

Sector-specific challenges

As do most countries, China regulates privacy and security in certain industries more heavily than other ones. Among the members interviewed, those operating in the automotive, hospitality, health care, and financial services sectors indicate that new data and privacy rules present a range of distinct challenges that go beyond their traditional work with regulators, further complicating cybersecurity and data compliance. Businesses in these industries have a history of working collaboratively with regulators to ensure compliance that predates recent developments in China's data, privacy, and cybersecurity regimes. Companies note that significant support from industry-specific regulators will be crucial to effectively enforcing the new rules given the volume of transfer requests and other administrative tasks involved.

Automotive sector

China's automotive sector is at the forefront of sector-specific government efforts to regulate data, and it is the subject of some of the most prolific policy activity. Some of these measures extend beyond current standards in other markets, principally, non-binding European regulations. In May 2021, the CAC released its draft Provisions on Security Management of Automotive Data for trial implementation, provisions which articulate proposed data security standards and work toward defining the nebulous concept of "important data." Within the automotive sector, the definition of "important data" is expansive, encapsulating information collected up and down the auto sector's physical supply chain. This includes audio-visual data, auto-charging station data, data on the flow of people and traffic, and survey and map data that are more precise than maps the state publicly issues.

The sheer number of auto sector guidelines makes them challenging to navigate. Moreover, many of the requirements are challenging to comply with while still fulfilling

The broad scope of "important data": An auto sector example

Important data includes:

1) Geographic information, data on flows of people, and vehicle flow volume in important sensitive areas, such as military control areas, organizations engaging in national defense science/technology and industry, and Communist Party and Chinese government organizations above the county level of government.
2) Data reflecting economic performance, such as vehicle flow and logistics.
3) Operational data of the automobile-charging grid.
4) Data on videos and images outside the vehicle, including human faces and license plates.
5) Personal information involving 100,000 or more individuals.

contractual obligations to deliver goods and services.

Though these rules are unfinalized, members indicate that important data provisions have already impacted automotive company operations, particularly their relationships with suppliers. As a result, they are adjusting and limiting product offerings in China with these changes in mind. When evaluating potential product developments, these impending data limitations are viewed as long-term barriers to investment.

Health care

Companies in the health care industry face unique challenges in China due to their reliance on clinical trials for innovation. Some members report that they are unable to offer certain new diagnostics or pharmaceutical products in China due to frustration and uncertainty with approvals of data collection or transmission. In addition to new obligations under the PIPL, separate rules from the Ministry of Science and Technology and the National Health Commission require approval for the cross-border transfer of data on human genetic resources, which are collected in some pharmaceutical and medical device clinical trials. This includes transfers to foreign parties, such as the US Food and Drug Administration, or similar foreign regulatory agencies, even if the transmission is intended for routine reporting purposes. This interpretation has created significant challenges and legal risks given requirements in other markets to report adverse effects or other elements of product information in a timely fashion.

The combination of additional approvals and restrictions on routine processes could significantly limit the ability of foreign companies to conduct clinical trials in China. While partnering with Chinese entities makes launching new trials in China easier, this arrangement may carry its own intellectual property protection and competition concerns.

Financial services

Financial services companies are subject to strict data localization requirements that predate the CSL. Starting in 2009, a range of financial sector–specific regulations have required data localization and prohibited most cross-border data transfers. Also in 2009, the China Banking and Insurance Regulatory Commission introduced guidelines that required banks to localize important systems. In 2011, the People's Bank of China expanded restrictions on the analysis, processing, and storage of personal financial information outside mainland China, allowing only limited exceptions for some data transfers to overseas headquarters or branches.

Early in 2019, additional regulations prohibited the cross-border transfer of all customer identification information and transaction information obtained when conducting due diligence related to anti-money laundering and counterterrorism financing obligations. These restrictions create ongoing challenges for international financial institutions using a global operating model as well as for financial institutions looking to enter the Chinese market and remain compliant with legal requirements in other markets.

Company Responses to Key Data and Privacy Concerns

Companies react to data, privacy, and cybersecurity challenges in different ways based on their risk tolerance, structure, and market exposure in China. For the most risk-averse companies, this has resulted in an "in China, for China" data strategy in which operations, products, after-sales services, and personnel are

disconnected from global structures. In turn, such companies have also reported that they are forced to remove more technically advanced elements of international products to comply with Chinese regulatory requirements that prevent overseas customer service representatives, engineers, and managers from processing data collected in China. As a result, the product is less competitive and less responsive to user demand. For small and medium-sized enterprises, the prohibitive cost of data localization and the complexity of navigating the policy landscape could disincentivize them from servicing the China market.

Due to the increasing challenges associated with China's data and privacy regimes, companies are finding it more and more untenable to simply wait and see what comes next. This has led to the following reactions:

- Revamping government affairs strategies: Many companies are working with regional regulators to navigate data, privacy, and cybersecurity concerns. They indicate that interactions with local authorities might offer greater clarity on the implementation of central policies, as these policymakers are better placed to provide an informal greenlight on company data governance strategies and practices. Some businesses also indicate that they are prioritizing government affairs outreach in new development zones based on the perception that there may be more room for advocacy to influence data practices in these areas. The Hainan Free Trade Zone and Shanghai Lingang Free Trade Zone were both highlighted as innovation centers of interest.
- Mapping company data: Many companies have taken or are currently pursuing the initial step of mapping their data to gain a preliminary understanding of which ones will be subject to the compliance requirements under data classification schemes and cross-border security reviews. Respondents often indicate difficulty in reaching a consensus on data residency strategies between companies' China offices and their headquarters as well as across their legal and executive functions.
- Adjusting structure and creating new plans: In order to mitigate concerns with China's data, privacy, and cybersecurity regimes, some companies have invested more resources in local teams to review compliance and evaluate whether their clients, vendors, partners, or customers will be subject to the most restrictive elements. Some companies report that these assessments have led to a conclusion that some of their domestic offerings will be cut off from upgrades available offshore and that they are planning accordingly.
- Evaluating data storage practices: Businesses are also evaluating their data storage practices, opting to localize either completely or partially or to continue communicating with regulators to understand if such steps are necessary. Regulators already require localization in the energy and financial services sectors, so some companies view wider enforcement of data localization requirements as inevitable. Many companies have already localized or plan to localize data and personal information gathered in China. Approaches to localization can include building local data infrastructure in China or storing data gathered in China with a local joint venture partner or cloud service provider. Businesses note that they are prioritizing the localization of data seen as the most essential to normal operations or product management. These include data types such as employee records, customer rewards programs, after-sales tracking, and product troubleshooting. Data localization trends are also visible in other markets today, including India and Vietnam.

Regulatory Landscape for Cybersecurity: The Multi-Level Protection Scheme

Alongside China's piecemeal release of data and privacy legislation has been its steady rollout of a comprehensive cybersecurity regime. Unlike in the United States, where businesses have the flexibility to choose cybersecurity frameworks that best suit their sector and operational model, China has developed a prescriptive and mandatory cybersecurity framework: the Multi-Level Protection Scheme (MLPS). While the MLPS initially focused on the protection of network and information systems, an update to the regime—what this report refers to as the "MLPS 2.0"—has expanded its scope to cover cybersecurity protection for basic infrastructure, network operations, data, and information, with specific data protection provisions.

At its core, the MLPS 2.0 is a system for ranking companies' computer information systems in China, and it places different compliance requirements on the operators of those systems according to the damage that their failure would pose to China's national security and economic stability. At a basic level, all companies are required to take technical and operational measures to ensure the resiliency and security of their information systems, including the use of cryptography, data risk classification, and incident response measures. The MPS, along with its local counterparts, is the leading agency responsible for implementing, supervising, and enforcing the MLPS 2.0.

The Five Grade System

Level 1	Damage to the information system results in harm to the legal rights of citizens, legal persons, and other organizations but does not harm national security, social order, or public interest.
Level 2	Damage to the information system results in serious harm to the legal rights of citizens, legal persons, other organizations, social order, or public interest but does not harm national security.
Level 3	Damage to the information system results in serious harm to social order, public interest, and national security.
Level 4	Damage to the information system results in very serious harm to social order, public interest, and national security.
Level 5	Damage to the information system results in very serious harm to national security.

While compliance with the MLPS 2.0 is mandatory for all companies based in China, the Cybersecurity Multi-Level Protection Regulation, which undergirds the scheme, is unfinalized and remains in draft form. Other aspects of the regime are built out in PIPL and DSL provisions as well as through a patchwork of separate mandatory and voluntary standards, making it difficult to decipher companies' exact compliance obligations.

There are intrusive and burdensome requirements on systems that are rated as MLPS 2.0 level 3 or above. Those requirements include local maintenance, connecting company systems to the public security bureau's systems, and procurement requirements for secure and controllable products (often synonymous with domestic products). These requirements can have a far-reaching impact on global companies' operations in China.

Compliance Burden Examples

Level 1

- Using cloud computing providers that are compliant with "relevant national regulations." In practice, this can mean working with domestic cloud providers.
- Filing with government not required.

Level 2

- Using cloud computing providers that are compliant with "relevant national regulations."
- Self-scanning for systems vulnerability.
- Promptly responding to supply chain security incidents and threats from the cloud service provider.

Level 3

- Selecting cloud computing providers that are compliant with "relevant national regulations."
- Testing external system penetration points.
- Promptly responding to supply chain security incidents and threats from the cloud service provider.
- Requiring designated personnel to manage system security and environment.

Level 4

In addition to level 3 requirements, examples of level 4 systems requirements include:

- More stringently restricting the number of personnel allowed to access data storage areas.
- Providing a higher level of cybersecurity protections to a wider range of facilities and products, including all restricted areas.
- Greatly improving inspection to verify safety certification of component systems.

Level 5

- Not publicly available.

MLPS 2.0 Classification Grading Steps

Step 1: Confirm grading subject. The business determines which information systems and network infrastructure require internal cybersecurity evaluation.

Step 2: Initial grading confirmation. The business provides an initial cybersecurity risk self-classification to the MPS. If the self-classification is level 2 or above, it proceeds to step 3.

Step 3: Expert assessment. An expert or certification body assesses the initial self-classification.

Step 4: Approval. The relevant industry regulator approves or rejects the business's internal assessment.

Step 5: Filing audit. The business formally files its cybersecurity assessment and audit results with the MPS.

Key Concerns with the MLPS 2.0

- **Market access:** The MLPS 2.0 can operate as a market access barrier to foreign ICT technology suppliers in China because qualifying for certain security standards as a foreign company is difficult and the security certification itself is cumbersome. Additionally, potential clients ranked at higher MLPS 2.0 levels face limits regarding which suppliers they are allowed to use in their systems. American cloud service providers, for example, must navigate a complex licensing regime and security standards to provide cloud services to companies. This cost has to be weighed against the likelihood that Chinese clients may choose a domestic provider due to potential mistrust of American cloud service providers, an issue that is exacerbated by bilateral tensions.
- **Intellectual property concerns:** There are concerns the MLPS 2.0 framework gives the Chinese government excessive access to companies' proprietary information. Risks to intellectual property protection include requirements to link level 3 systems with the local public security bureau as well as routine auditing and system checks. Some companies have had to provide detailed information to government authorized auditors on their system/infrastructure design and simply trust that this information will be kept confidential and their intellectual property secure.
- **Trustworthiness of testing agencies:** The MPS maintains a list of hundreds of qualified third-party evaluation agencies that help companies test the security of their network systems according to their MLPS 2.0 grading level. Companies harbor concerns about some evaluation agencies' professionalism and impartiality, as some are reported to have pushed companies to purchase the testing agencies' own proprietary software or hardware in order to be certified. As these third-party agencies are state-affiliated, it is also unclear to what degree they can serve as impartial assessors and protect the proprietary information businesses share with them.
- **Local maintenance:** The MLPS 2.0 requires companies with level 3 systems to carry out maintenance on domestic systems locally. If a company requires overseas professionals to provide additional remote support, they must first undergo risk assessments. These requirements create challenges for

foreign businesses' global operations and negatively impact their ability to leverage global resources and expertise.

- Opaque standards: Members note the scoring system used by the MPS to rate MLPS 2.0 compliance frequently changes and is not publicly available. This leaves companies subject to seemingly arbitrary changes within a nontransparent system.

The MLPS 2.0 and Cybersecurity Enforcement Trends and Concerns

To date, the majority of interviewed members report having at least completed an internal MLPS 2.0 systems evaluation. It is notoriously difficult to track MLPS 2.0 scoring given the lack of public-facing documentation on assessment standards from the government. Moreover, the MLPS 2.0 is enforced by the public security bureaus at the district level of government, making it susceptible to disparate regional enforcement.

It has been widely acknowledged by industry that since new standards went into effect in 2019, MLPS 2.0 certification has been enforced most rigorously in Shanghai, China's largest commercial center. Some companies have reported proactive inquiries from the public security bureau on compliance status. Interviewees indicate that Beijing-based companies are also experiencing increased proactivity from regulators, and some businesses indicate that they were encouraged to undergo assessment. Geographic differences in MLPS 2.0 enforcement suggest that local officials have a degree of autonomy. Local discretion in enforcement creates unpredictability for businesses registered in multiple regions and cities, as they may be subject to differing regulatory approaches.

In addition to regional variance, businesses face uncertainty regarding the precedent set by an assessment of one system in their network. Some companies expressed concern that the assessment of a single system in one location could create a domino effect when looking to evaluate other systems. If precedent in other regions contributes to local evaluation, that could mean that companies are unnecessarily evaluated at a higher compliance level, contributing to costs and procurement requirements across their network.

Intersection of MLPS 2.0 requirements and privacy regimes

Companies in the hospitality sector report pressure to comply with the MLPS 2.0 in Beijing and Shanghai specifically. Members suspect that this is simply due to the large amount of personal information generated by users and guests. While regulators are still articulating privacy obligations, MLPS 2.0 implications are more immediate and direct. At level 3 and above, certification would prove onerous and costly due to the need for an expanded IT management budget as well as the need to purchase new hardware and software. One member expects level 3 compliance to impose new costs on each of the 1,000 hotels it operates in China.

The Road Ahead

China's data, privacy, and cybersecurity regimes are unfolding in real time. There is a growing sense that security concerns are prevailing over practical commercial realities. As the policy landscape takes clearer shape, the costs and legal risks of doing business in China are going up. Limiting cross-border data flows, requiring data localization, and mandating duplicative or vague system requirements could broadly impact the competitiveness of China's business and investment environments in a number of ways. The question of how to balance unintended impacts to the business and investment environments with legitimate needs for improved cybersecurity and privacy remains open, both in China and globally.

At minimum, the one-off costs of acquiring local servers will reach several million dollars for many companies, not accounting for any ongoing budget items for people, support, and maintenance. Restrictions on data flows create a diverse range of challenges. These include undermining risk management, cybersecurity, and anti-money laundering practices; increasing IT and data complexity; and reducing access to service offerings. Relying on globalized structures and backups offsets risk and allows for strengthened data supply chains.

At worst, components of current regulation could result in "in China, for China" data islands that make portions of global businesses essentially inaccessible by headquarters or offices in other markets. This would not only hinder the operations and competitiveness of foreign businesses, but it would limit the capacity for Chinese firms to go global. It could stifle the way foreign and Chinese companies innovate, limit which products are brought to market in China, and change how companies conduct research and development, all of which could ultimately impact investment decisions. Further, the uptick in compliance burdens is likely to impact foreign companies unevenly, particularly because smaller companies are less able to keep pace with increasingly far-reaching compliance demands.

As China works to grow its digital economy, ambiguously scoped and far-reaching data, privacy, and cybersecurity policies might prevent foreign businesses from helping advance its development. An approach that more practically balances commercial realities with legitimate security concerns would lead to both greater economic benefits and stronger security protections.

Appendix: Catalog of Key Policies

Laws

Cybersecurity Law	Passed by the National People's Congress in November 2016, the CSL is the seminal cybersecurity law in China, covering content control, IT security, privacy, and data. The law went into effect in 2017.
Personal Information Protection Law	The PIPL defines the individual rights of persons over the processing of their personal information as well as the obligations of personal information processors when handling personal data. Following several rounds of revision, the final version of the law was implemented on November 1, 2020.
Data Security Law	The DSL calls for a comprehensive data classification and grading scheme along with a data security system based on national security concerns, and it mandates that important data catalogs be established at the central and local levels. The final version was implemented on September 1, 2021.

Implementing Regulations

Information Security Multi-Level Protection Regulation	Released by the MPS in June 2007, these are the original MLPS measures and are still referenced by regulators.
Draft Personal Information and Important Data Cross-Border Security Review Measures	Released in April 2017 to implement the CSL, these draft measures expand cross-border security reviews beyond CII operators (as per the CSL) to general network operators under certain circumstances, including 1) when the transfer involves more than 500,000 records of personal information, 2) when the transfer surpasses 1,000 gigabytes of data, and 3) when a CII operator transfers either personal information or important data. The draft remains unfinalized.
Trial Security Review Measures for Network Products and Services	Issued by the CAC in May 2017, these trial measures implement the CSL by mandating security reviews for the procurement network of products and services that may affect China's national security and information infrastructure. The reviews assess the "security and controllability" of goods and services. The measures were replaced by the 2019 Cybersecurity Review Measures.
CII Protection Regulations	Released by the CAC in July 2017 as a draft, these regulations implement the CSL by broadly defining CII industries and the obligations of CII operators and regulators. A finalized version of the measures was released in July 2021, providing further clarity, and it went into effect September 2021.

Draft Cybersecurity Multi-Level Protection Measures	Released by the MPS in June 2018, these unfinalized measures outline the overall scope, obligations, and grading principles of the MLPS 2.0.
Cybersecurity Review Measures	Implementing measures of the CSL and the DSL, the Cybersecurity Review Measures were originally released by the CAC in May 2019 and require cybersecurity reviews for procurement of network products and services by CII operators if they might affect national security. A revised draft was released in 2021 proposing cybersecurity reviews be conducted on companies possessing over 1 million records of personal information when they make initial public offerings abroad and that the offerings be assessed to determine if they would lead to the compromise of important data, core data, personal information, CII, etc., by a foreign power. A final version of the measures maintaining these revisions was released in January 2022 and came into force in February 2022.
Draft Data Security Administrative Measures	Issued by the CAC in May 2019 as an implementing measure of the CSL to regulate operators that conduct data activities (transfer, storage, collection, processing, etc.) in China, this draft is notable for requiring domestic users to use the "domestic internet." It mandates that operators publicly publish the rules guiding their collection and use of personal information and data, prohibiting discrimination against users who do not provide consent for their personal information to be processed and providing a definition of important data.
Children Personal Information Data Protection Measures	Originally released by the CAC in May 2019 as implementing measures of the CSL and Minor Protection Law, these measures regulate the limits and abilities operators have when processing children's personal information. An updated version went into effect in October 2019.
Draft Cross Border Security Review Measures for Personal Information	Released by the CAC in May 2019 as an implementing measure of the CSL, this draft governs the cross-border data flow activities of all operators in China and is notable for solely governing personal information and including no volume-based thresholds.
Cloud Computing Security Assessment Measures	Released by the CAC in July 2019, these assessment measures mandate security reviews for the procurement of cloud computing services by CII operators. Among many factors, reviews assess the security and controllability of the service provider, especially if they have access to operational data and client data or if those data will be migrated to the cloud service platform. The measures went into effect in September 2019.
Several Measures on Vehicle Data Security Management (Trial)	Released by the CAC in August 2021, these trial measures implement the DSL and are sector-specific data regulations notable for providing specific examples of important data for the automotive sector.

Draft Data Security Administrative Measures for the Industry and Information Technology Sector	Released by the MIIT for public comment in September 2021 and February 2022, this draft implements the DSL for the industry and information technology sector and introduces the concept of "general data," a new classification encompassing low-risk data.
Draft Outbound Data Security Assessment Measures	Released by the CAC in October 2021, this draft formalizes the details of the cross-border security review process and mandates that any operator that possesses 100,000 records of personal information or 10,000 sets of sensitive personal information undergo a cross-border security assessment.
Draft Network Data Security Regulations	Released by the CAC in November 2021, this draft is the most comprehensive implementing regulation for all three laws underpinning China's cybersecurity regimes. The draft proposes cross-border security reviews for companies that possess over 1 million records of personal information.

Standards

Personal Information Security Specification	The TC-260 released this voluntary standard in 2017. It is a seminal standard for regulating processors who collect, store, and use personal information, and it limits the harm that could be caused by that information's abuse, illegal access, and leakage. The final version went into effect in October 2020.
Draft Guidelines for Data Cross-Border Transfer Security Assessment	The TC-260 released this draft voluntary standard in 2017. It outlines the scope and procedure for cross-border security assessments and is notable for explicitly identifying important data across 28 industries, including financial services, mapping, and foodstuffs. The draft remains unfinalized.
MLPS 2.0 Testing and Evaluation Requirements	The TC-260 released this voluntary standard in May 2019. It outlines requirements for evaluating information systems under the MLPS 2.0. It came into effect in December 2019.
MLPS 2.0 Security and Design Technical Requirements	The TC-260 released this voluntary standard in May 2019. It outlines basic security design requirements for systems under the MLPS 2.0. It came into effect in December 2019.
MLPS 2.0 Basic Requirements	The TC-260 released this voluntary standard in May 2019. It outlines general requirements for compliance with the MLPS 2.0. It came into effect in December 2019.
MLPS 2.0 Implementing Guidelines	The TC-260 released this voluntary standard in August 2019. It provides guidance for appropriately providing security for systems covered under the MLPS 2.0. It came into effect in March 2020.

MLPS 2.0 Grading Guidelines	The TC-260 released this voluntary standard in April 2020. It provides guidance for appropriately grading systems under MLPS 2.0. It came into effect in November 2020.
Draft Important Data Identification Guide	The TC-260 released this draft voluntary standard in January 2022. It provides a framework for industry regulators and players to identify important data. It explicitly excludes personal information from the definition of important data but notes that statistics and other data derived from large volumes of personal information can be counted as important data.