Nigel Cory

Director, Crowell Global Advisors; Nonresident Fellow, National Bureau of Asian Research

Testimony before the U.S.-China Economic and Security Review Commission

Hearing: "Taking a Bigger Byte: China's Expanding Strategy for Data Dominance"

April 30, 2026

Table of Contents

Overview

This testimony builds on an extensive body of published research on China's data governance strategy, cross-border data flows, and digital trade. The works on which it directly draws are: "Testimony Before the U.S.-China Economic and Security Review Commission Regarding China's Cloud Computing Market" (ITIF, 2021); "Testimony to the U.S. Senate Subcommittee on Trade Regarding Censorship as a Non-Tariff Barrier to Trade" (ITIF, 2020); "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them," co-authored with Luke Dascoli (ITIF, 2021); "Writing the Rules: Redefining Norms of Global Digital Governance," in *China's Digital Ambitions: A Global Strategy to Supplant the Liberal Order*, National Bureau of Asian Research (NBR, 2022); "The Case for U.S. Leadership on Global Data Governance," co-authored with Akanksha Sinha (NBR, 2025); and "House Ways and Means Subcommittee on Trade Testimony: Maintaining U.S. Innovation and Technology Leadership through Digital Trade" (2026).[1]

Taken together, these works establish the foundation on which this testimony builds: China's data governance strategy is not a discrete set of policies but a sustained, state-directed campaign to control a foundational input of the digital economy, domestically through accumulation and restriction, internationally through norm-setting and institution-building.

The Central Analytical Problem

China has built, over the past decade, the world's most elaborate legal and regulatory architecture for governing data and simultaneously the world's least constrained system for state access to it. That juxtaposition is not a contradiction. It is the design.

The legislative foundation — the Cybersecurity Law (CSL), Data Security Law (DSL), Personal Information Protection Law (PIPL), the Data Twenty Articles, the Network Data Security Management Regulations, and the continuous stream of implementing rules documented throughout this testimony — creates an expanding perimeter of obligations on private actors, often relating to private sector involvement in strategic technologies and development interests. All the while it preserves maximum discretion for the state. The obligations run one way: firms must classify, protect, localize, and seek approval for moving data. The state faces no equivalent constraint. There is no independent judiciary capable of reviewing state data access. There is no transparency requirement that would reveal when access occurs. The National Intelligence Law's standing cooperation obligation and the Data Security Law's Article 36 asymmetry are not gaps in an otherwise well-designed system. They are features of it.

Against this domestic backdrop, Chinese digital firms are expanding globally at a pace and scale that has no historical precedent in the technology sector besides U.S. firms after the creation of the modern Internet. Chinese digital firms now hold dominant or near-dominant positions across multiple layers of the digital economy in Southeast Asia and beyond. In e-commerce and consumer platforms, they collectively account for approximately half of regional gross merchandise value across key Association of Southeast Asian Nation (ASEAN) economies. In physical digital infrastructure, Chinese firms have built the undersea cable networks, data centers, and 5G systems that form the transport and processing layer for a significant portion of

global data flows. In consumer applications, social media, short-form video, mobile payments, ride-hailing, logistics, and fast-fashion retail, Chinese platforms have rapidly captured market share across the world. In enterprise services, Chinese cloud providers are aggressively expanding data center footprints in emerging markets, competing primarily on price and leveraging state financing that Western commercial providers cannot replicate. Across all of these sectors, the pattern is consistent: rapid market penetration, pricing that reflects state subsidy rather than commercial cost recovery and competitiveness, and a governance architecture that makes the data generated by hundreds of millions of users in dozens of countries legally accessible to Chinese state actors upon demand.

There are a growing number of anecdotal stories and cases of Chinese tech firms making decisions in third-country markets that show they are not competing on commercial merit. The testimony documents all of this. What it cannot definitively resolve — and what no public evidence base fully resolves — is the intentionality question: is China's overseas digital expansion accompanied by a deliberate state objective of collecting and aggregating data from overseas, or is data acquisition incidental to commercial expansion that happens to be state-subsidized?

The structural asymmetry that distinguishes Chinese digital expansion from that of U.S. and other foreign firms is not primarily about commercial behavior — it is about the governance architecture within which commercial behavior occurs. American firms operating globally are subject to legal process under rule-of-law systems: warrants, subpoenas, court orders, independent judicial review, transparency reporting, and oversight by elected officials, civil society, and the media. They compete on commercial merit, bear the full cost of their overseas operations, and face the same data protection obligations as domestic firms in host countries. Chinese firms operate under a fundamentally different architecture — one in which state compulsion is always legally available, commercial and strategic objectives are deliberately intertwined, and the distinction between private enterprise and state instrument is a matter of political discretion rather than legal principle. They are additionally supported by state financing that allows them to compete on price and penetration terms that commercially driven firms cannot match.

The stakes extend well beyond which country's technology firms dominate global markets. The deeper question is which model of digital governance becomes the global default — and the answer is being determined now, in procurement decisions, regulatory drafting rooms, and bilateral digital agreements across the developing world. If Chinese digital infrastructure, platforms, and governance frameworks become the dominant model in Southeast Asia, Africa, and Latin America, it will not simply be a commercial loss for the United States. It will represent the normalization of a model structurally incompatible with privacy, rule of law, and democratic accountability. That contagion does not require deliberate ideological export. It happens through adoption, imitation, and the gravitational pull of market dominance.

The most difficult analytical question — whether China's overseas digital expansion is accompanied by a deliberate state objective of aggregating foreign data, or whether data access is incidental to commercially-motivated expansion — cannot be definitively resolved from the public evidence. But the legal architecture makes the distinction less consequential than it might appear. The National Intelligence Law creates a standing cooperation obligation. The Data

Security Law creates compulsory disclosure rights without specifying how they will be exercised. The military-civil fusion framework creates systematic pathways from commercial capability to military and intelligence applications. A Chinese firm does not need to be tasked with data collection for its overseas data to be accessible to Chinese state actors as the compulsion architecture is always on, regardless of whether it is being actively used. The critical difference from Western governance models is not behavioral but structural: there is no transparency mechanism that would reveal when state access occurs, and no independent judiciary capable of constraining it. That opacity is itself the problem, and no amount of corporate compliance investment can resolve it.

The Evolution of China's Data Governance Architecture

China recognizes data's critical role in economic development and national security and has built an evolving legal framework around this foundational point. In 2015, the 13th Five-Year Plan (2016–2020) described data as a "basic strategic resource." In 2020, China formally designated data as the fifth factor of production, after land, labor, capital, and technology.[2] Chinese President Xi has consistently used the phrase "data as a factor of production," placing data on equal footing with land, labor, capital, and technology as a basic input to economic output. He first said this in his October 2021 Politburo speech, stating that:

> "Data has become a new type of production factor, and has a major influence on the transformation of traditional production methods...The digital economy…is not only a new economic growth point, but also a supporting point for transforming and upgrading traditional industries…The healthy development of the digital economy benefits promoting the building of new advantages in national competition... [views data as] a critical force in reorganizing global factor resources, reshaping global economics structures, and changing global competition structures."[3]

Xi has repeatedly called national security "the bedrock of national rejuvenation" and said that "Cybersecurity affects the whole body and profoundly influences the security of politics, economy, culture, society, military, and other domains. Without cybersecurity, there is no national security."[4] Xi views the security of data, and the Chinese Communist Party's (CCP) ability to control it, as a critical step to maintaining public order and as a necessary precondition for development.[5] In 2022, the 20th National Congress report was the first to dedicate a special section specifically to national security, with the integration of development and security as a major throughline of the report.[6] Specifically, the chapter calls for building a "new security pattern" to aid in the creation of a "new development pattern," following what President Xi has said publicly about development being impossible without security.[7]

Key Institutions and Agencies

China's data governance framework involves multiple agencies whose authorities overlap, compete, and in some cases remain deliberately ambiguous. The lead regulator is not an administrative agency in any conventional sense.

The Cyberspace Administration of China (CAC)

The Cyberspace Administration of China traces its origins to the CCP propaganda system, not to the state administrative apparatus. Its predecessor, the State Internet Information Office, was established in 2011 as an internal sub-office of the State Council Information Office — itself a government nameplate for the CCP's External Propaganda Office — with a mandate to unify online content management and investigate website violations.[8] As Jamie Horsley (Senior Fellow, Paul Tsai China Center, Yale Law School) documented in her 2022 DigiChina analysis, the CAC is formally listed under the CCP Central Committee rather than the State Council — a "single institution with two nameplates" — meaning it is simultaneously a state enforcement agency and a party organ.[9] Xi Jinping chairs its governing commission, the Central Cyberspace Affairs Commission. Not a single meeting of that commission has ever been publicly reported. There is also no publicly documented direct bilateral engagement between the CAC specifically and any U.S. government agency.

That institutional design is not a technicality. Rogier Creemers of Leiden University describes the CAC as "the world's most powerful digital institution" precisely because of this dual structure.[10] It houses the secretariat of the Central Cybersecurity and Informatization Commission, meaning it sits at the junction of party policy and state regulation with no institutional separation between the two. Creemers identifies the CAC as having "several different roles, both political and regulatory" simultaneously — an observation that has direct implications for how foreign firms, foreign governments, and courts should interpret its enforcement actions. When the CAC acts, there is no reliable mechanism to determine whether a given decision reflects regulatory policy, party direction, or some combination of both. A November 2025 peer-reviewed analysis in the Journal of Chinese Political Science extended this institutional analysis to the municipal level, finding that local CAC branches are tasked with "often divergent mandates of digital innovation, regulatory enforcement, and political control" simultaneously, and that even Municipal Cyberspace Administrations (MCAs) within a single province vary significantly in how they prioritize these roles—with some emphasizing surveillance and others inverting the hierarchy to prioritize local digital economy development. This variation compounds the unpredictability that foreign firms already face at the national level, since enforcement priorities shift not just over time but across jurisdictions.[11]

Through the three foundational laws enacted between 2017 and 2021 — the CSL, DSL, and PIPL — the CAC's authority has been progressively codified and expanded. The CSL designated it as the body responsible for overall planning and coordination of cybersecurity regulation across all other agencies. The DSL tasked it with overall coordination of online data security and authorized it to regulate important data exports. The PIPL granted it overarching powers for comprehensive planning, coordination, and supervision of personal information protection work.[12] The CAC's direct rulemaking authority remains legally imprecise in some areas, as Horsley documents in detail — it has cited the Three Laws collectively as authority for specific regulatory actions while sometimes noting the need for State Council authorization in others, creating an inconsistent legal basis that gives regulated entities limited predictability and gives the CAC maximum discretion.[13] The September 2025 Dior enforcement action — penalizing the luxury firm for transferring personal information to its French parent without approval — demonstrates that the CAC's enforcement posture has sharpened considerably and now applies directly and assertively to foreign-invested enterprises.

The National Information Security Standardization Technical Committee

One regulatory body conspicuously absent from a lot of policy analysis of China's data governance framework is TC260, the National Information Security Standardization Technical Committee. Operating under the Standardization Administration of China in close coordination with the CAC, TC260 translates CAC policy into the binding and quasi-binding technical standards that determine how China's data laws are operationalized in practice. For example, its March 2024 data classification and grading standard (GB/T 43697-2024) is the technical backbone of the "important data" system, providing the reference framework that all sectoral regulators such as the Ministry of Industry and Information Technology (MIIT), National Financial Regulatory Administration (NFRA), and local data bureaus must follow when building industry-specific data catalogs.[14] In the AI domain, TC260 has sharply accelerated its output since 2023, publishing standards on generative AI security, AI training data, and data annotation, culminating in a comprehensive AI Safety Governance Framework in September 2024 that the CAC subsequently endorsed as authoritative policy guidance, making TC260, in effect, the technical standard-setter whose output the CAC then enforces.[15] That relationship matters strategically because TC260 holds China's seat on ISO/IEC JTC1/SC27, the principal international body for cybersecurity and privacy standards, and its 2025 work priorities explicitly instruct the committee to "leverage the hosting of the SC27 international conference to actively lead the development of international standards."[16]

The National Data Bureau (NDB)

In October 2023, the National Data Bureau (also see section below) was established. Its first director, Liu Liehong, came from the CAC where he had served as deputy director, and before that from MIIT and China Unicom. Tom Nunlist of Trivium China offered the most analytically precise characterization of the CAC/NDB division at the time of the NDB's establishment: "The security side will still firmly be [the domain of the] CAC. The NDB is expected to deal primarily with the development side of data governance."[17] That framing, security versus development — captures the intended institutional division but understates the jurisdictional tensions that have emerged since. For example, the January 2026 CAC draft on financial data classification, introducing a new "Sensitive General Data" subcategory that effectively supersedes the People's Bank of China's (PBoC) five-tier classification system, is evidence that the CAC is not content to cede the development agenda to the NDB where data security interests are at stake.[18]

Other Important Organizations

The CAC does not govern alone. The MIIT, MPS, the State Administration for Market Regulation (SAMR), and other industry regulators oversee law enforcement in their respective industries, with the CAC coordinating above them.[19] In practice, this coordination is imperfect. MIIT administers telecoms licensing and has driven the development of sector-specific important data identification standards, publishing draft guidelines for the industrial field in late 2024 that took effect April 2025.[20] MPS governs law enforcement data access and administers real-name registration requirements for online services. SAMR oversees anti-monopoly enforcement and consumer rights, including data-related market power abuses. In November 2024, CAC, SAMR, MPS, and MIIT jointly launched a special enforcement campaign targeting algorithm violations on online platforms, a multi-agency coordination that reflects a new pattern of cross-agency collaboration on emerging regulatory frontiers, though it also reveals how enforcement priorities can shift rapidly and without advance notice.[21]

The result is a structural tension at the heart of China's data governance architecture. The CAC's security-first mandate and the NDB's circulation-first mandate pull in opposite directions, with no institutional mechanism for resolution below the level of the CAC. The NDB's creation reflects the CCP's broader strategy of concentrating control over sectors it views as determinative of long-term political and economic power, which means the NDB's development mandate is ultimately subordinate to the party's security interests whenever the two conflict.[22] Foreign firms operating across financial services, telecoms, and data-intensive industries accordingly face overlapping and sometimes conflicting guidance from agencies whose jurisdictional boundaries are disputed among themselves.

Developments in China's Cybersecurity Review System

China's cybersecurity review regime is best understood not as a rules-based compliance system but as a discretionary tool of state power that has, in practice, preserved maximum regulatory flexibility. As Graham Webster and Rogier Creemers documented in their authoritative DigiChina analysis, the relevant laws "were drafted in full knowledge that technology and its context would develop rapidly." This language functions as a standing justification for regulatory adaptation without legislative amendment.[23] Over nearly a decade of continuous revision, the system has evolved from a narrow procurement review mechanism into a broad framework for state oversight of any technology activity deemed to touch national security.

The regime traces to Article 59 of the 2015 National Security Law and was operationalized through Article 35 of the 2017 Cybersecurity Law, which required critical information infrastructure operators to submit to security review before procuring network products or services that might affect national security. The current Cybersecurity Review Measures, finalized in December 2021, represent the third major iteration in five years.

Two triggers for mandatory filing are enumerated: CII operators procuring potentially sensitive network products, and firms handling more than one million users' data seeking a foreign IPO. But the Cybersecurity Review Office also retains authority to initiate reviews on its own initiative, drawing legal weight from the broad provisions of the NSL, CSL, and Data Security Law rather than from the Measures themselves.[24] The Micron case in March 2023 extended this pattern to a major U.S. semiconductor firm, on publicly stated CII security grounds whose specific factual basis was never disclosed.[25]

The October 2025 CSL amendments (the first major revision since enactment, effective January 1, 2026) substantially harden the enforcement architecture in two ways that directly affect foreign firms. First, penalties have escalated dramatically: general violation fines rose fivefold to RMB 500,000, while a new severe violations category carries fines up to RMB 10 million ($1.4 million), business suspension, and license revocation. Individual liability now extends to all directly responsible personnel, with personal fines reaching RMB 1 million.[26] Second, and more consequentially, the extraterritorial scope has been explicitly expanded from overseas activities harming Chinese CII to any overseas activity that endangers China's cybersecurity — potentially capturing foreign cloud providers, SaaS firms, and data analytics companies processing China-related data anywhere in the world. The February 2025 Compliance Audit Measures add a parallel mechanism of continuous state visibility: firms processing more than ten million individuals' personal information must conduct mandatory audits every two years, and the CAC

may require third-party audits of any firm it determines presents material risks — a threshold left undefined.[27] Both instruments operate through the CAC. A third parallel mechanism took effect November 1, 2025: the Administrative Measures for National Cybersecurity Incident Reporting, which consolidate previously dispersed reporting obligations into a structured framework requiring real-time disclosure to regulators when security incidents occur — adding continuous event-driven visibility to the ongoing audit visibility the Compliance Audit Measures create.[28]

How China Promotes the Accumulation of Data as a Strategic Asset: The Data Twenty Articles and the National Data Bureau

The Data Twenty Articles are a major new data initiative for China. China enacted these changes to not only ensure economy-wide integration of data into its economy but to create rules to "activate" the value of data.[29] China's "data element market" is a state initiative to commodify, trade, and circulate data as a new productive factor to drive digital economic growth.[30] In 2026, the initiative is now fully operational, having reached its "industrialization" phase. Per the Chinese government, this initiative is now in the last year of this phase, aiming to achieve an annual data industry growth rate of over 20 percent by the end of 2026.[31]

China created the NDB to accelerate the utilization of data to pursue economic growth and to create the digital infrastructure necessary to support the growth of a "digital China" via a unified national data market, moving away from prototype local markets, and seeks to build national-level data infrastructure and "industry databases" to provide training sets for artificial intelligence (AI) large language models (LLMs).[32] The NDB has focused on moving the Data Twenty Articles from principle to a structured economic ecosystem, by institutionalizing data as a "factor of production." It does this through four main pillars (below).[33] China has also launched the World Data Organization (WDO) to help export the "Data Twenty Articles" model as a global standard (see below).[34]

The four pillars:

1. Pillar 1: Data Property Rights: The document introduces a three-way structural separation of data rights: the right to hold data resources, the right to process and use data, and the right to operate data products. This applies differently to public, enterprise, and personal data, with the governing principle of "whoever invests, contributes, benefits." The framework is designed to allow commercial data circulation while preserving state control over sensitive categories.

2. Pillar 2: Data Circulation and Transaction: Covers compliance rules, standardized national data exchanges, and a data services ecosystem including brokers, auditors, and dispute arbitration. The cross-border subsection explicitly bases China's international engagement on the Global Data Security Initiative and calls for resisting what it terms "data hegemony, data protectionism, and long-arm jurisdiction in the data field" — direct references to U.S. export controls and sanctions policy embedded in China's foundational data governance document.

3. Pillar 3: Data Revenue Distribution: Market-based contribution assessment governs distribution, with explicit government redistribution mechanisms to address inequality.

The document links data revenue policy to common prosperity, calls for preventing monopolistic capital expansion in the data domain, and requires large data enterprises to bear social responsibility obligations alongside commercial interests.

4. Pillar 4: Data Governance: A multi-party governance structure involving government, enterprises, and society. Government sets the regulatory framework including a negative list of data that cannot be traded. Enterprises bear primary compliance responsibility and are prohibited from using data or algorithmic advantages to restrict competition. Anti-monopoly enforcement is an explicit component alongside data security oversight.[35]

China's data elements initiative has generated substantial institutional activity with more than 20 state-led data exchanges now operate nationwide. The NDB reports that China's data industry reached 5.86 trillion yuan (approximately $816 billion) in 2024, up 117 percent from 2020.[36] Yet trading volumes at the exchanges themselves remain marginal relative to that scale. China's first data exchange, the Guiyang Big Data Exchange established in 2015, had annual trading volume of less than 5 million yuan before its restructuring. This is a trajectory that prompted one widely cited internal Chinese analysis to describe the initiative's first six years as "idealism abundant, reality gaunt."[37] By mid-2023, the exchanges in Shenzhen, Guiyang, and Guangzhou had each crossed 1 billion yuan in trading volume, but this is still a fraction of the industry the government claims to be building.[38]

The gap between China's data policy ambition and reality reflects a structural contradiction that institutional restructuring will struggle to resolve. The security architecture Beijing built to control data — localization requirements, national security carve-outs, broad state access powers — is the same architecture that acts as a barrier to the commercial data circulation the Data Twenty Articles initiative was designed to create. A concrete illustration emerged in December 2024, when the first batch of digital asset public bidding projects in Fuling District, Chongqing, was suspended. Law firm analysis of that failure identified three unresolved barriers: no clear legal guidance on public data transfers, unclear data ownership rules and undefined privacy boundaries, and hidden compliance risks in government data transactions.[39] These are the predictable consequence of trying to build a data market under a governance framework whose primary purpose is control, not circulation.

The data property rights system has not resolved this underlying legal ambiguity. A November 2025 academic analysis identifies four specific failures: ambiguity in the subject matter of data property rights, excessive exclusivity of those rights as constructed, insufficient protection of individual data rights, and inadequate data sharing.[40] The NDB's January 2025 consultation draft on common terminology in the data sector attempted to address definitional ambiguity by providing formal definitions for data property rights, data holding rights, data usage rights, and data operational rights, but a peer-reviewed assessment confirms that no concept of data property rights yet exists in Chinese laws and regulations, and the glossary's definitions have not resolved the underlying legal gap.[41] As the Journal of International Economic Law noted in its October 2024 comparative analysis of China's data property rights system and the EU Data Act, China creates new property rights for data processors rather than imposing obligations on them. This is a philosophically distinct approach that nonetheless leaves the same fundamental questions of ownership, valuation, and enforceability unresolved.[42] The cross-border dimension compounds these domestic challenges. The party-state's ongoing push to restrict foreign access to data about

China's economy, science, and technology actively undermines the cross-border data commerce that would be necessary for the data elements market to achieve its stated economic objectives.

Technology Specific Case Study: AI Robotics Data

The next competitive frontier in AI is not text generation but physical intelligence. AI systems that perceive, reason about, and act within the real world. Robotics is the primary arena. Training these systems follows a fundamentally different path from LLMs. Where LLMs are pre-trained on publicly available text and refined through human feedback, physical AI systems require thousands of hours of real-world operational data collected before any labeling process begins. That data is then annotated and structured to build Vision Language Action Models and once deployed, the systems generate further operational data that continuously improves their performance. The training bottleneck is not compute. It is the physical data itself, generated only through robots operating in real-world environments at scale.[43]

China's state-directed robotics data strategy rests on an interlocking set of policy instruments enacted at the national level. The USCC's March 2026 working paper "Two Loops: How China's Open AI Strategy Reinforces Its Industrial Dominance" identifies the core mechanism: China's open AI model strategy and its manufacturing dominance are mutually reinforcing, with open models enabling low-cost deployment across factories and logistics networks that in turn generate the real-world data feeding back into model improvement.[44] Ceding the robotics data layer to China is not an abstract technology policy concern, it is a potential critical infrastructure risk.[45]

In January 2023, the "Robotics+" Application Action Plan (co-signed by MIIT and seventeen other government departments) subsidizes robot deployment across manufacturing, logistics, healthcare, and consumer services.[46] The plan's data logic is straightforward: by subsidizing deployment at scale, Beijing simultaneously subsidizes the generation of real-world operational training data across every sector the plan touches. MIIT's October 2023 Guiding Opinions on the Innovative Development of Humanoid Robots established embodied AI as a national technology priority, setting a 2025 target for a preliminary humanoid robot innovation system and a 2027 target for a secure supply chain, with data infrastructure identified as a core enabling component.[47] The most technically specific instrument is MIIT's Intelligent Data Collection Standard 1.0, issued in November 2024. This is a unified, enforceable framework for synchronizing, formatting, labeling, and quality-grading multimodal robot training data across the industry, explicitly designed to ensure interoperability so that data generated across disparate deployments can be aggregated into shared training pools rather than remaining in proprietary silos.[48]

China industrialized data generation in a way the United States has not. China's January 2025 guidelines on the data labeling industry, issued jointly by the NDRC and the NDB, commit to establishing data labeling hubs nationwide and supporting the sector with favorable fiscal, financial, and tax policies.[49] This represents a general AI data infrastructure development program that has robotics training data as one of its priority applications.[50] In one government data collection center in Hubei province, close to 100 humanoid robots (controlled by human operators) practice movements like folding clothes, ironing, and wiping tables hundreds of times daily.[51] The data-sharing institutional architecture is equally deliberate. Beijing and Shanghai

have each established state-funded national humanoid robotics innovation centers whose explicit mandate includes aggregating training data and sharing it across the industry to reduce development costs for smaller firms. As of December 2025, more than 40 state-funded robot data collection centers had been announced nationwide, with approximately two dozen already in operation.[52] AgiBot's data factory generates approximately 50,000 data captures per day, which is a throughput that peer facilities also target, with at least one firm, Parsini, aiming an order of magnitude higher. Large real-world data factories operate in Shanghai, Beijing, and Shenzhen/Tianjin. Regional data consortia have been established in Hubei and Guangzhou. Open datasets including AgiBot World and RoboMIND supplement facility-based collection. The Robot Report describes this network as "a national data engine for multi-skill, multimodal robot learning."[53]

Leading Chinese robotics firms AgiBot and Fourier have released open training datasets as part of this strategy. This may appear to be a commercially counterintuitive move that RAND's "Full Stack: China's Evolving Industrial Policy for AI" report attributes directly to state pressure to build shared industry infrastructure rather than proprietary competitive moats.[54] The Chinese Academy of Sciences white paper adopted in March 2025 formalizes this as part of a three-stage roadmap: shared datasets and open middleware through 2027; scaled deployment in factories, logistics, and elder-care pilots through 2030; and mass-market generalization post-2030.[55] Taken together, these instruments constitute not a collection of sector policies but a coordinated national campaign to control the foundational data inputs of physical AI before the rest of the world has recognized the strategic stakes.

Cross Border Data Flows and Foreign Data Access

China has established a comprehensive legal framework for cross-border data transfers primarily though the CSL, the DSL, and the PIPL. CAC oversees the data transfer regime as the apex authority. CAC states that the current cross-border data transfer regime mainly regulates important data and personal information, and other types of data may be freely transferred overseas. There are currently three mechanisms to transfer such data abroad, including a Security Assessment performed by the CAC, Personal Information Protection (PIP) Certification issued by CAC-approved institutions, and filing Standard Contractual Clauses (SCC). Overall, the Chinese approach is considered one of the most restrictive, with strict data localization requirements and a government-led supervision regime over cross-border data flow. Although the CAC's recent policy developments and initiatives send a signal of liberalization of restrictive outbound data transfer, these changes have not yet proven substantive or commercially significant, especially compared to most other countries' data transfer frameworks.[56]

Recent regulatory changes related to cross-border data flows:

- In March 2024, CAC issued Provisions on Promoting and Regulating Cross-Border Data Flows. These regulations introduced the easing of select cross-border data transfer constraints such as for transfers of China-collected data related to international trade; necessary transfers for signing or performing e-commerce contracts; essential transfer of personal information to safeguard an individual's life in emergencies; and transfer of non-sensitive personal information, totaling fewer than 100,000 individuals by noncritical information infrastructure operators[57]. Guided by these Provisions, various industry sectors

actively followed up by issuing a series of industry-specific cross-border data guidelines. Key sectors such as finance, automotive, shipping, and biopharmaceuticals successively ended up releasing specific guidelines to promote cross-border data flows[58].

- In February 2025, CAC issued Measures for the Administration of Compliance Audits on Personal Information Protection (Audit Measures), which took effect on May 01, 2025. These Audit Measures require data processors to assess and quantify the scale of their personal information processing activities.[59]

- In April 2025, the CAC published an FAQ for cross-border data transfers reflecting its evolved position towards cross-border data transfers along with practical guidance for data processors. The FAQs clarified the concept of free trade zones (FTZs) as being permitted to develop "negative lists" for cross-border data transfers. This essentially implies that all data is exempted from the general legal framework and can be transferred cross-border from these FTZs without restriction, so long as the data is not contained on the "negative lists". Significantly, the FAQ confirmed that "negative lists" enacted by one FTZ will be automatically effective in other FTZs to ensure consistency across regions. As of June 2025, FTZs in Tianjin, Beijing, Hainan, Shanghai, and Zhejiang had released "negative lists" covering 17 industry sectors.[60] However, as DigiChina analysis documents, FTZ rules must be established "under the framework of the national categorized and graded protection system for data." This means FTZ flexibility is bounded by the national security classification architecture rather than operating independently of it.[61]

- In October 2025, the CAC and SAMR jointly issued the long-awaited Measures for Certification of Cross-Border Personal Information Transfer, effective January 01, 2026. The Measures clarified key aspects of the certification process, including scope and applicability, application procedures, certification body obligations, as well as supervision and enforcement. These marked a pivotal moment in China's data governance landscape as they completed the three-pathway framework for cross-border personal information transfers established under the PIPL[62].

- On November 1, 2025, an important new national standard took effect, "Data Security Technology – Security Requirements for Processing of Sensitive Personal Information (GB/T 45574 – 2025)". It further clarifies the scope of the sensitive personal information and sets out detailed security and compliance requirements for its processing. Overall, it adopts a more cautious and refined approach to identifying sensitive personal information than previous standards (e.g., GB/T 35273 – 2020).[63]

China's approach to cross-border data is structurally asymmetric. Its domestic framework imposes onerous restrictions on outbound data transfers while simultaneously having broad and vague legal authorities for Chinese government access to data held anywhere in the world by Chinese firms. That asymmetry is deliberate and long-standing, but it is becoming more consequential as Chinese firms expand. The operational expression of Beijing's data strategy appears to be: control the outflow, expand the inflow. The result is a system in which foreign governments, firms, and individuals that interact with Chinese platforms and infrastructure are subject to Chinese state access rights that have no transparency, no access to any independent judicial system for redress, and no equivalent reciprocal obligation.

The strategic value of foreign data to China operates across multiple dimensions. Consumer behavioral data from foreign markets, purchasing patterns, payment preferences, social graphs, location data, health and genomic information, feeds China's AI development ecosystem. China's ability to train and refine large language models and recommendation algorithms depends on data diversity and volume. Having access to hundreds of millions of people across highly diverse countries and demographics, such as in Southeast Asia, is valuable in ways that go well beyond any individual firm's business interests. Financial and transaction data from foreign markets provides intelligence on economic activity, supply chain relationships, and individual financial behavior that has both commercial value for Chinese fintech firms and intelligence value for the state. Geospatial and mapping data from overseas operations (collected through ride-hailing services, logistics platforms, and smart city projects) has potential national security applications. Genomic and health data, particularly from populations with different genetic profiles from the Chinese population, has pharmaceutical and other values.

On outbound transfers, firms seeking to move data out of China must navigate three compliance pathways: mandatory security assessment for large-scale or important data; standard contract filing for mid-scale personal information; and certification for smaller volumes. The March 2024 CAC regulation introduced partial exemptions that left the core architecture intact. One of the regulation's most consequential changes was to the volume threshold triggering mandatory security assessment — raised from transfers involving more than 100,000 individuals under the 2022 Measures to more than 1 million individuals under the 2024 Provisions. This change provided meaningful relief for small and medium-sized firms, but as Sacks, Chen Zeng, and Webster note, it is not difficult to exceed 1 million users in a market of 1.09 billion internet users — meaning major domestic and foreign companies operating at that scale continue to face the security assessment process with all its attendant uncertainty.[64] The critical feature is the explicit exclusion of "important data" from all exemption categories, meaning that any data Beijing designates as strategically significant is subject to mandatory security assessment regardless of commercial rationale. The legal definition of "important data" remains insufficiently precise at the national level, giving regulators discretionary power to designate commercial data as subject to national security review after the fact.[65]

The 2024 Provisions compound this ambiguity rather than resolving it. Article 2 simultaneously requires data handlers to identify and declare important data themselves, while stating that absent regulatory notification, they need not file for a security assessment. As Sacks, Chen Zeng, and Webster document in their authoritative DigiChina analysis, "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" — leaving regulators with ample space to explore their own interpretations.[66] A further dimension of this ambiguity is the personal information/important data overlap: Article 5 of the 2024 Provisions makes explicit that even when personal information qualifies for a transfer exemption, that exemption does not apply if the data has been designated as important data. The national security designation can therefore strip away privacy-based exemptions after the fact, embedding the security classification architecture directly into the personal information protection regime.[67] A final unresolved area concerns the "necessity" standard embedded throughout the 2024 Provisions' exemption categories. Transfers for international trade, contract performance, and emergency purposes are exempt if "necessary," but neither the regulation nor subsequent guidance specifies who determines necessity or by what standard.[68]

Chinese Government Access to Data

On inbound state access to data, Article 36 of the DSL prohibits domestic organizations and individuals from providing data stored in China to foreign judicial or law enforcement authorities without government approval from competent Chinese authorities.[69] Crucially, this restriction applies to all data regardless of sensitivity level — not only "important data" or "core data." Jones Day's analysis of the provision notes that it appears to apply to all types of data and that the law does not specify what activity constitutes a transfer to a foreign authority or how approval may be obtained, giving Chinese regulators maximum discretion.[70] Entities providing data without approval face fines up to 5 million yuan and cancellation of business licenses.

The National Intelligence Law (2017) gets a lot of attention (understandably) from U.S. policymakers. It compounds this framework. Article 7 stipulates that "all organizations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with law."[71] Article 14 grants intelligence agencies authority to insist on this cooperation.[72] A December, 2020, U.S. Department of Homeland Security business advisory concluded that Chinese firms that own and operate data centers, both within China and abroad, "are subject to laws which require their secret cooperation with PRC intelligence services" and may be required to "secretly share data with the PRC government or other entities upon request, even if that request is illegal under the jurisdiction in which these firms operate."[73] China Law Translate's Jeremy Daum offers a more cautious reading of Article 7, noting it is far from clear the provision was intended to require active participation in information gathering.[74] This may well be the case, but the key point is not the outer boundaries of the legal obligation but the practical reality: there is no independent judiciary in China capable of constraining state access to firm data, and no transparency requirement that would allow the outside world to know when such access occurs.

Contrasting Chinese and U.S. Firms' Data Practices in Southeast Asia

The most analytically revealing theater for comparing Chinese and U.S. firms' data practices is not the United States or the European Union, where both sets of firms face meaningful regulatory constraints, but third-country markets — particularly Southeast Asia — where those constraints are nascent, enforcement capacity is limited, and the governance and behavioral gap between Chinese and U.S. firms is most consequential. It is in these markets that the structural asymmetry this testimony has documented throughout plays out with the fewest external checks. The asymmetry between Chinese and U.S. firms operating in Southeast Asia is legal, architectural, and operational.

Southeast Asia is a hugely consequential theater for Chinese commercial data acquisition outside China's borders. The scale is substantial. According to Bain & Company, Chinese platforms together held approximately 50 percent of the e-commerce market across Indonesia, Thailand, and the Philippines in 2024.[75] Momentum Works reported that Southeast Asia's total e-commerce gross merchandise volume reached $114.6 billion in 2023, more than double its 2020 level.[76] Beyond e-commerce, Chinese firms are major players in regional digital infrastructure. A Center for Strategic and International Studies report notes directly that China's control over optical fiber networks transports "huge amounts of personal, government, and financial data, which would presumably be shared with the Chinese government if controlled by Chinese companies."[77] The combination of consumer platform and physical infrastructure control creates a potential layered

data collection architecture. Chinese firms accumulate behavioral and transaction data through consumer platforms at the application layer while simultaneously positioning Chinese-controlled networks as the transport layer through which that data moves.

Chinese firms operating in Southeast Asia face a genuine structural contradiction: China's DSL requires Chinese firms to report data generated overseas to Chinese authorities upon request, while host country privacy and data protection laws may prohibit disclosure of that same data to foreign governments. Vietnam's Decree 53/2022 mandates local data storage for telecom and e-commerce platforms. Indonesia's Government Regulation 71/2019 similarly mandates domestic data storage for electronic systems operators.[78] These requirements directly conflict with Chinese state access obligations.

The starting point to compare U.S. and Chinese firm data management operations is the regulatory environment in which both sets of firms actually operate in the region. Southeast Asia does not have a unified data protection framework. Each country maintains its own regime at varying stages of development and enforcement. No Southeast Asian data protection authority has the investigative resources, technical capacity, or institutional independence of the Irish Data Protection Commission (DPC) or the U.S. Federal Trade Commission (FTC). This enforcement gap is the operating condition that makes the comparison between Chinese and U.S. firms in the region analytically significant. Both sets of firms are formally subject to local law when operating in these markets. The meaningful distinction is not the formal legal obligation but the behavioral constraints that operate independently of local enforcement, specifically, the extraterritorial obligations each set of firms carries from its home jurisdiction.

U.S. firms operating in Southeast Asia carry a set of home-country legal and reputational obligations that function as behavioral constraints regardless of local enforcement capacity. U.S. cloud firms publish detailed global transparency reports disclosing government data requests and their responses across all jurisdictions. They operate under the EU’s General Data Protection Regulation’s (GDPR) extraterritorial reach for any processing of EU residents' data, which imposes purpose limitation, data minimization, and consent requirements on their global data architectures. They are also subject to FTC oversight and to the reputational and litigation risk that flows from U.S. civil society, media scrutiny, and class action litigation. The World Benchmarking Alliance's 2025 Ranking Digital Rights Index, which for the first time included major Chinese firms in its assessment, found that while some scored near the middle of the pile on privacy and freedom of expression metrics, they lagged on governance transparency compared to the major U.S. platforms. This finding reflects the structural difference between firms operating under externally verified transparency obligations and those that do not.[79]

U.S. technology firms also face asymmetric regulatory and political scrutiny relative to Chinese competitors, even though U.S. firms tend to operate some of the world’s most sophisticated compliance systems for privacy, security, and lawful access. Yet in many third-country debates, scrutiny disproportionately fixates on U.S. legal authorities (often centered on the CLOUD Act), while comparatively little attention is paid to Chinese providers’ legal exposure, compliance, and transparency. The result in developing-country markets is a lopsided legal and operational risk conversation: policymakers may subject U.S. providers to intense legal scrutiny because U.S. processes are visible and contestable, while under-weighting the governance and legal constraints affecting Chinese providers—constraints that are often less transparent and harder for

customers to assess, particularly where sensitive government or critical-infrastructure data is involved.

There’s asymmetry in commercial data practices, which are most visible in behavioral targeting and algorithmic personalization. Chinese platforms dominating Southeast Asian e-commerce and social media accumulate behavioral data from hundreds of millions of users across markets with limited data minimization requirements, no meaningful purpose limitation enforcement, and no independent supervisory authority capable of auditing cross-border data flows at the technical layer. That data feeds recommendation and advertising algorithms that drive platform commercial performance. The more comprehensive the behavioral profile, the more effective the personalization; the more effective the personalization, the higher the engagement and conversion rates that generate advertising and transaction revenue. U.S. firms building equivalent systems in the same markets face their own governance obligations — extraterritorial GDPR reach where EU users are involved, FTC scrutiny for deceptive data practices, and the reputational constraints of operating under U.S. civil society and media oversight. Chinese firms do not face equivalent external constraints and, critically, face internal constraints from a home-country governance regime whose enforcement runs through the CAC.

The transparency asymmetry compounds the commercial one. None of China's major platform firms operating in Southeast Asia publish transparency reports disclosing government data requests and their responses across jurisdictions, despite operating at the scale of U.S. firms that do. No equivalent institutional pressure exists in Southeast Asia to require or verify such transparency from Chinese platforms, because no local regulator has the capacity to do so and no extraterritorial obligation from a home-country privacy regime requires it. U.S. firms' transparency reports are imperfect instruments, but they create a public record that enables independent verification, civil society scrutiny, and regulatory accountability. The absence of any equivalent from Chinese firms is not a compliance gap — it reflects a governance architecture in which transparency toward external parties is structurally disincentivized.

There’s also a clear difference in market preference. U.S. and other foreign firms operating in Southeast Asia actively oppose data localization requirements in the region on the grounds that such requirements create duplicative costs, undermine global service capabilities, and harm cybersecurity. Chinese platforms have actively embraced and promoted data localization as a competitive differentiator, accurately reading that some host country governments prioritize physical control over data regardless of the security consequences. As I documented in my 2021 USCC testimony, Alibaba Cloud's general manager for India explicitly described the Indian government's push toward data localization as "a big opportunity," and Alibaba Cloud President Simon Hu stated that "Indian data should be stored in India" as a matter of policy.[80]

The competitive consequence is a structural advantage in data-intensive markets that is also strategically valuable in ways that extend well beyond advertising revenue because the behavioral data, financial transaction records, and social information being accumulated by Chinese platforms in Southeast Asia is data that China's DSL and National Intelligence Law may access and use for targeted cybersecurity, industrial development, and other interests.

World Data Organization

On March 30, 2026, China held the founding assembly of its newly launched World Data Organization (WDO), which it is positioning as the first international organization in history dedicated specifically to data governance and development.[81] The WDO will be based in Beijing, but it aims to serve as a global, non-governmental, and non-profit platform for dialogue, rulemaking, and collaboration. It has a threefold mission of bridging the data divide, unlocking data's value, and powering the digital economy. The WDO ultimately aims to "break barriers" around different data policies in countries by promoting industry consensus and helping multinational enterprises reduce data compliance costs.[82] It also aims to build ecosystems through applying data in practical scenarios such as medical care, education, and energy to promote project implementation and industrial innovation. As of its first assembly, the organization had amassed more than 200 members from over 40 countries. Its membership includes companies, universities, think tanks, international organizations, and institutions across industries such as finance, medical care, energy, internet, and automobiles.[83]

Key policy considerations[84]:

- Even though the WDO will not establish binding rules, it will focus on policy coordination, standard-setting recommendations, and capacity building. It's unclear what it means by work on standards (whether technical standards akin to those from the ISO and IEEE) or it means general policy development, which may then form the basis for engagement in formal standards making at the ISO and other technical standards bodies. China clearly recognizes the role and value of taking leadership roles and being engaged in the development of technical standards. It's a matter of watching how it tries to leverage the WDO agenda to encourage other countries to adopt similar positions on standards.

- It appears part of a long-term, methodical global Chinese strategy for creating a China-led or friendly global order for digital policy. China's creation of the WDO is clearly in part motivated by the U.S. governments withdrawal from many multinational institutions and forums. It also follows in the footsteps of other key policy initiatives, such as creating the National Data Bureau and the Global Cross-Border Data Flow Cooperation Initiative.

- The president of the UN Commission on Science and Technology for Development spoke at the inaugural assembly, signaling that the UN recognizes the WDO as a relevant forum for global discussions and potential rulemaking.

Overall, the WDO plans to achieve its mission through activities such as promoting member services and industry self-regulation; conducting policy research and compliance services; deepening industry studies and public interest initiatives; and providing a global platform for exchange and collaboration on data governance[85]. Through the WDO, China has essentially introduced a new actor with sufficient critical mass to shape agendas and build coalitions with the potential to shape the global data governance in its favor.

Trends to Watch

AI Distillation Attacks: A New Dimension to China's Data Acquisition Strategy

Adversarial AI distillation reveals something important about the evolution of China's data acquisition strategy. Knowledge distillation is a well-established and legitimate AI technique in which a smaller "student" model is trained on the outputs of a larger, more capable "teacher" model, acquiring capabilities at lower cost than training from scratch. Frontier AI labs routinely distill their own models to create smaller, cheaper versions for their customers. What Chinese labs did was weaponize this process: using fraudulent accounts, proxy services, and evasion infrastructure to circumvent geographic access restrictions, then systematically generating crafted prompts at industrial scale to extract training data they used to improve competing models. A China Business Law Journal analysis notes that if Chinese firms obtained output data through commercial APIs rather than stealing internal parameters or source code, determining that they used "deceptive means" or infringed trade secrets is legally complex. The more actionable claim is likely violation of terms of service rather than intellectual property theft under current frameworks.[86] These are legitimate caveats. However, the operational facts are not in dispute: the firms created fraudulent accounts, deliberately circumvented geographic restrictions, and used proxy services to disguise the source of their requests.[87]

This is data acquisition through the API layer, not the infrastructure layer. The Digital Silk Road strategy potentially acquires foreign data through physical infrastructure, such as undersea cables, data centers, and 5G networks. The distillation attacks described here acquire something more valuable: the synthesized intelligence embedded in U.S. frontier AI models, accumulated through billions of dollars of R&D investment and trained on vast datasets that Chinese labs do not independently possess. Joe Khawam in a Just Security article describes this as "free riding on the capabilities developed by OpenAI and other U.S. frontier labs."[88] This understates the strategic significance as what was extracted was not raw data, it was the distilled output of some of the most advanced AI research in the world. This implicates U.S. export controls. The Just Security analysis makes the connection explicit: "Distillation attacks therefore reinforce the rationale for export controls: restricted chip access limits both direct model training and the scale of illicit distillation."[89] If Chinese labs can extract frontier model capabilities through API access rather than through independent training, chip export controls are partially circumvented. The Institute for AI Policy and Strategy's March 2026 analysis estimates that successful distillation "lowers the compute threshold required to achieve near-frontier performance — meaning that even with restricted chip access, Chinese labs can close the gap faster than export controls were designed to allow."[90]

The World Data Organization as an Institutional Inflection Point

The WDO may become a major vehicle for Chinese data governance policy. As described above, it represents the institutional capstone of a decade-long Chinese strategy. The Commission should track WDO membership growth closely, particularly which developing countries join, under what terms, and whether WDO discussions produce outputs, and how those align or conflict with international standards, U.S. policy, and emerging global best practices relating to data policy. The stated goal of becoming "an internationally influential platform and trusted hub in the data field" by 2030 is Beijing's own benchmark.[91] The Commission should assess progress

against it annually. However, much like China's "Global Cross-Border Data Flow Cooperation Initiative" it may not turn into anything major (thus far, nothing further has happened).

China's 15th Five-Year Plan Data Infrastructure Buildout (2026–2030)

NDB Director Liu Liehong's March 2026 Qiushi article frames National Data Infrastructure as the defining priority of the 15th Five-Year Plan period, describing its purpose as to "open the aorta of data circulation" and enable large-scale movement of data resources across China's economy.[92] The institutional and technical architecture being built now (national data infrastructure, inter-agency data integration, provincial NDB networks linked to NDRC authority etc.) will define China's data capabilities in the years ahead. The Commission should track implementation of the 15th FYP data infrastructure commitments as a leading indicator of China's ability to realize its goals to make data a strategic asset.

AI and Data Governance Fusion

China's enforcement campaigns targeting large language models and algorithms signal that data governance and AI governance are formally merging in China's regulatory architecture. The CAC's November 2024 "Qing Lang" special campaign on algorithmic issues (jointly launched with three co-agencies) and subsequent enforcement waves through 2025 targeting LLM filing compliance, PIPL violations in AI services, and algorithm transparency violations collectively represent a significant intensification of AI governance that operates directly through the data governance framework.[93] The MIIT's Important Data Identification Guidelines in the Industrial Field, effective April 1, 2025, begins the process of defining important data at the sectoral level, covering high-technology data including integrated circuits, key software, and electronic components.[94] As AI competition intensifies, the classification of AI-related training and model data as important data, and thus subject to mandatory security assessment before any offshore transfer, will become an increasingly consequential policy tool, one whose asymmetric application could disadvantage foreign firms seeking to move AI-related data out of China. The Commission should monitor how China uses its data classification architecture in this emerging area.

Southeast Asia Data Governance Maturation

The United States should make Southeast Asia a priority for digital and technology policy engagement and development. Several ASEAN economies are developing or revising national data protection frameworks, but these can vary quite a lot.[95] How these frameworks develop and whether they are shaped by Global CBPR principles, GDPR-adjacent frameworks, or China's sovereignty model will determine whether Chinese data collection in the region will face meaningful constraint. The Commission should track ASEAN digital governance developments as an early indicator of whether this region, like many others around the world, converges toward or diverges from international data governance norms.

Personal Data and National Security Convergence

Both China and the United States are reclassifying certain personal data as national security matters, producing a convergence that is analytically important and practically consequential. China's March 2024 regulation explicitly excludes personal information designated as important data from all transfer exemptions, embedding a national security frame into what might

otherwise appear to be routine privacy regulation.[96] The United States' Executive Order 14117 and the Department of Justice final rule implementing it establish a parallel framework, designating bulk sensitive personal data flows to countries of concern as national security matters rather than trade or privacy issues.[97] As both countries tighten restrictions on each other's data access, third-country governments and firms may face pressure to choose sides. The Commission should monitor how this convergence affects allied and partner countries' digital trade and data governance frameworks, particularly in the Indo-Pacific.

China's Quantum Capabilities and the Post-Quantum Cryptography Imperative

Quantum-enhanced computing accelerates China's ability to derive analytical value from the vast data volumes its regulatory and commercial architecture is accumulating. The more immediate concern is the "harvest now, decrypt later" strategy — collecting encrypted data today for decryption when quantum computers mature. The U.S. National Institute for Standards and Technology (NIST) finalized three post-quantum cryptography standards in August 2024, and National Security Agency's Commercial National Security Algorithm Suite 2.0 framework requires full federal migration by 2035.[98] Congress should treat that deadline as an outer boundary: the harvesting is happening now, and the urgency of post-quantum migration across federal systems, defense contractors, and critical infrastructure operators should be calibrated accordingly.

Policy Recommendations

Pass the Digital Trade Promotion Act and Codify U.S. Digital Trade Priorities

China's asymmetric market access — open global markets for Chinese digital firms, a closed domestic market for foreign competitors — is a long-standing structural issue.[99] The Biden administration's October 2023 withdrawal from World Trade Organization (WTO) digital trade negotiations eliminated longstanding U.S. protections for cross-border data flows, prohibitions on data localization, and safeguards for source code at precisely the moment China was advancing its own competing governance model. As Samm Sacks and I wrote in Lawfare at the time, the U.S. Trade Representative (USTR) handed Beijing a victory and dealt a blow to longstanding U.S. support for an open internet and digital economy.[100] Without a statutory anchor, U.S. digital trade positions remain vulnerable to administrative reversal.

Congress should pass the Digital Trade Promotion Act, introduced by Senators Young, Coons, Moran, and Bennet, to codify those positions in statute and prevent future reversals.[101] The Act establishes a statutory process for addressing digital trade barriers; codifies cross-border data flows, bans on data localization and discriminatory digital taxes, protection for source code and algorithms, and support for interoperable privacy frameworks; empowers USTR with stronger monitoring and enforcement tools; and establishes congressional oversight over digital trade negotiations. Its most strategically significant feature is that it directly addresses regulatory contagion from both China's data sovereignty model and the EU's digital regulatory agenda by providing a durable legislative foundation that would remain operative even if EU courts again invalidate the EU-U.S. Data Privacy Framework, as they have twice before.

Re-Engage WTO Digital Trade Negotiations with a Clear U.S. Position

The Biden administration's October 2023 withdrawal from WTO Joint Statement Initiative (JSI) negotiations on data flows handed Beijing a victory and a blow to U.S. efforts to counter Chinese data policies. The WTO JSI concluded negotiations in July 2024 without meaningful U.S. input on data flow provisions. Allowing China (and the EU) to define the terms of global digital trade rules by default is not a neutral outcome. It is a concession of leadership at the most consequential moment in the development of global data governance.

Congress should direct the administration to re-engage WTO digital trade negotiations with a clear, affirmative U.S. position on cross-border data flows, prohibition of data localization, and narrow, well-defined national security exceptions that cannot be exploited as pretexts for digital protectionism. All of China's problematic laws and issues this testimony has documented are designed to exploit the absence of binding international rules that would constrain these practices. The USCC's 2024 Annual Report recommended that Congress urge USTR to pursue digital trade agreements with strong cross-border data flow provisions and prohibitions on data localization.[102] Given the WDO's March 2026 launch and China's accelerating international governance advocacy, that recommendation should be treated as urgent.

Support an Ambitious ASEAN Cloud and Digital Governance Engagement Strategy

The United States has an established foundation for digital engagement with the Association of Southeast Asian Nations (ASEAN) through the U.S.-ASEAN Digital Work Plan 2023–2025 and the six U.S. priority areas confirmed at the 6th ASEAN Digital Ministers' Meeting in January 2026.[103] Congress should direct the State Department and Commerce Department to significantly deepen this engagement, backed by U.S. International Development Finance Corporation (DFC) financing and the American AI Exports Program established under Executive Order 14320 (Promoting the Export of the American AI Technology Stack), both of which should explicitly prioritize Southeast Asia as a priority.

A comprehensive strategy should pursue three specific initiatives. First, active U.S. financial and technical support for the ASEAN Trusted Data Corridor which pairs corridor-specific rules limiting data localization with binding government data access safeguards modeled on OECD trusted government access principles.[104] Second, an accelerated campaign to expand Global CBPR membership across the region as it is the most effective accountability mechanism available. The U.S. should provide financial and technical support for each country's certification process. Third, the DFC should support U.S.-backed data center and cloud infrastructure investments in Indonesia, Vietnam, and the Philippines as credible alternatives to Chinese offerings. Ideally, a fourth initiative would be a U.S.-ASEAN digital trade agreement to provide a common, high-standard set of provisions on data and digital trade.

Promote the Global Cross Border Privacy Rules (CBPR) System

The Global CBPR System, officially launched in June 2025, is the most credible rules-based mechanism currently available for building trusted cross-border data flows among like-minded countries. Its thirteen current members include major U.S. trading partners (e.g. Japan, Canada, and Australia) and partners critical to AI and technology leadership (e.g. Singapore and Taiwan). Congress should direct the administration to make Global CBPR expansion a top-tier trade and technology policy priority, integrating it explicitly into U.S. trade negotiations, the AI Action Plan's international pillar, and bilateral technology dialogues. Congress should also explicitly

recognize Asia Pacific Economic Cooperation CBPR and Global CBPR certifications as valid data transfer mechanisms in U.S. law, providing domestic legal certainty that would accelerate both U.S. firm participation and partner country interest in joining.

The Global CBPR framework is at an inflection point. Its credibility and network effects depend on achieving critical mass in the near term. The United Kingdom is actively considering membership; India has engaged the question in both government and private-sector channels; Indonesia would be a transformative addition. Congress should direct USTR and the State Department to prioritize securing Indian and Indonesian membership as the immediate diplomatic objective, using trade negotiations, bilateral technology dialogues, and the AI Action Plan as leverage. Global CBPR provides something no bilateral agreement can replicate: a certifiable, multilateral accountability standard that distinguishes firms operating under rule-of-law data governance from those subject to Chinese state compulsion obligations.

Operationalize OECD Trusted Government Access Principles

The Organization for Economic Cooperation and Development (OECD) Declaration on Government Access to Personal Data, adopted December 2022, establishes the clearest available multilateral differentiation between democratic and authoritarian approaches to government data access: "We reject any approach to government access to personal data held by private sector entities that, regardless of the context, is inconsistent with democratic values and the rule of law, and is unconstrained, unreasonable, arbitrary or disproportionate."[105] That declaration describes China's model precisely. China's broad, arbitrary, and opaque ability to compel private firms to disclose data to the state is the structural mechanism that makes Chinese digital firms categorically different from their U.S. and European counterparts, regardless of where they operate. The problem is that most jurisdictions — including key U.S. partners — lack the legal mechanisms, frameworks, or diplomatic coordination to act on that conclusion systematically.

Congress should direct the administration to do three things. First, operationalize the OECD declaration by developing concrete compliance tools — legal checklists, certification criteria, risk assessments and risk indices for specific jurisdictions, and government access transparency standards — that allow partner countries to formally distinguish trusted from untrustworthy jurisdictions in their data transfer frameworks, using the U.S. experience implementing Executive Order 14117 as a practical template.[106] Second, launch a dedicated multilateral dialogue on trusted government access to data running in parallel to the Global CBPR Forum. The latter addresses commercial privacy, while this new forum would address government access, with the goal to attract non-OECD countries in Southeast Asia and the Global South that are grappling with exactly these questions and currently lack any multilateral framework to help answer them. Third, integrate trusted government access standards explicitly into U.S. bilateral technology dialogues with Australia, the EU, Japan, and the UK, developing common tools that make data flows to China and other problematic jurisdictions addressable through coordinated policy rather than unilateral restrictions.

Establish a Trusted Cloud Initiative with Key Allies and Partners

Cloud infrastructure is the foundation on which data governance either succeeds or fails. The threat of governments compelling cloud providers to surrender customer data is not hypothetical.

The United States has addressed this domestically through the CLOUD Act and the EU-U.S. Data Privacy Framework. Meanwhile, Chinese cloud firms are aggressively expanding in Southeast Asia and the Global South, competing primarily on price in markets where governments recognize the importance of security and trust in cloud services but lack the tools to evaluate and differentiate providers in practice. That gap is a strategic vulnerability the United States has not closed.

Congress should direct the administration to establish a trusted cloud initiative with Five Eyes partners, Japan, the EU, and others to develop a common, risk-based framework defining cloud trustworthiness that can be applied across allied and partner country procurement decisions. The initiative should produce a shared toolkit of technical controls, audit standards, and certification criteria that allow governments and commercial buyers to distinguish trusted from untrustworthy cloud providers on grounds beyond price. It should cover incident response requirements, configuration management, government access transparency obligations, and data handling safeguards.[107] A common catalog of trustworthiness criteria endorsed by the United States and its partners would serve three simultaneous purposes: it would protect sensitive data from Chinese state compulsion; it would give U.S. and allied cloud firms a credible, verifiable competitive advantage over Chinese providers in third-country markets; and it would directly operationalize the Trump administration's interest in ensuring that allies buying U.S. AI do so on approved, trusted cloud infrastructure.[108]

Establish a National Industrial Robotics Data Foundry

The United States has no institutional equivalent to what China has built at the physical AI data layer. Individual U.S. firms generate operational robotics data in proprietary silos. SMEs — the majority of U.S. industrial capacity — lack the deployment scale to generate meaningful training data independently. Meanwhile, China's response is centralized and systematic.

The Commission should recommend that Congress and the Administration direct the establishment of a National Industrial Robotics Data Foundry — a federated, IP-protecting infrastructure to aggregate, standardize, and share physical AI training data across U.S. manufacturers. The ARM Institute, with its 450+ member consortium, existing DoD relationships, and Manufacturing USA co-location, is the natural institutional anchor. Its mandate should be expanded to include standardized data formats — a direct U.S. answer to MIIT's Data Collection Standard 1.0 — and a federated governance architecture modeled on the EU's Catena-X automotive data space, where raw data never leaves participants' systems but model weights and anonymized derivatives are shared.

NIST should simultaneously be directed to develop a national robotics data interoperability standard through its proven voluntary multi-stakeholder process — replicating the twelve-month Cybersecurity Framework model — to position U.S.-originated formats at ISO before Chinese standards consolidate global adoption. Congress should authorize 5–8 regional testbed hubs co-located with Manufacturing USA institutes to give SMEs access to shared robotic systems and data collection infrastructure that no individual firm can build alone.

Institutionalize a Systematic BIS Chokepoint Assessment Framework

The U.S. government's connected vehicles rulemaking demonstrated that Bureau of Industry and Security (BIS) can develop targeted, technically credible national security rules for complex technology supply chains, but only when it has the time, industry engagement, and analytical discipline to distinguish core control functions from ancillary components. That process, which began with everything on the table and ended with a focused rule targeting operating systems and primary control software rather than entire vehicle systems, is the right model for addressing Chinese components in other critical technology infrastructure. Congress should direct BIS to institutionalize that chokepoint identification framework — systematic, technology-by-technology, proportionate, and in sustained engagement with U.S. industry — and apply it across critical technology sectors in a disciplined and sequenced manner.

The connected vehicles process is the right model precisely because of how it evolved. BIS began with everything on the table, then through sustained formal and informal industry engagement learned to distinguish the operating system and core control functions — the Advanced Driver Assistance Systems, the primary vehicle management software — from ancillary hardware and software that feeds into those systems without controlling them. The final rule was considerably more targeted than the proposed rule, reflecting BIS's receptiveness to technical information sharing during development. That process produced a rule with a defensible legal basis, a clear scope, and industry buy-in that would not have been achievable through a top-down prescriptive approach.

The Department of Commerce's proposed Information and Communications Technology and Services (ICTS) rulemaking targeting Chinese components in U.S. cloud services and data centers is at an earlier, less structured, and stalled stage. BIS has conducted some industry outreach covering data center market structure, customer and vendor profiles, traffic management, access control, and supply chain composition down to the component level. But unlike connected vehicles, BIS has not provided a clear statement of its objective, a defined timeline, or guidance on how it is thinking about the distinction between critical core functions and non-critical ancillary services.

Congress should direct BIS to apply the connected vehicles analytical framework across a defined set of critical technology sectors on a rolling basis. Two additional conditions are necessary for this framework to function. First, interagency coordination must be embedded in the process from the outset. The current cloud and data center rulemaking appears to be proceeding without adequate coordination with the U.S. Trade Representative on trade implications, with State on ally and partner impacts, or with the National Security Council on its relationship to the broader AI and supply chain strategy. These are gaps that risk producing rules that conflict with trade negotiating objectives or that disadvantage U.S. firms in third-country markets without corresponding security benefits. Second, the framework should explicitly distinguish between prohibitions on foreign adversary control of core functions and broader restrictions that would effectively require domestic sourcing of ancillary components

[1] Nigel Cory, "Testimony Before the U.S.-China Economic and Security Review Commission Regarding China's Cloud Computing Market," Information Technology and Innovation Foundation (ITIF), April 15, 2021, https://itif.org/publications/2021/04/15/testimony-us-china-economic-and-security-review-commission-regarding-chinas/; Nigel Cory, "Testimony to the U.S. Senate Subcommittee on Trade Regarding Censorship as a Non-Tariff Barrier to Trade," Information Technology and Innovation Foundation (ITIF), June 30, 2020, https://itif.org/publications/2020/06/30/testimony-us-senate-subcommittee-trade-regarding-censorship-non-tariff/; Nigel Cory, "Writing the Rules: Redefining Norms of Global Digital Governance," in *China's Digital Ambitions: A Global Strategy to Supplant the Liberal Order*, NBR Special Report No. 97, National Bureau of Asian Research, March 1, 2022, https://www.nbr.org/publication/writing-the-rules-redefining-norms-of-global-digital-governance/; Nigel Cory and Arjun Sinha, "The Case for U.S. Leadership on Global Data Governance," *Asia Policy*, Vol. 20, No. 4, National Bureau of Asian Research, October 2025, https://www.nbr.org/publication/the-case-for-u-s-leadership-on-global-data-governance/; Nigel Cory, written testimony before the House Committee on Ways and Means, January 2026, https://waysandmeans.house.gov/wp-content/uploads/2026/01/Nigel-Cory-Written-Testimony.pdf.

[2] Central Committee of the Communist Party of China and State Council, "Opinions on Building a More Complete Market-Based Allocation System for Production Factors" (中共中央 国务院关于构建更加完善的要素市场化配置体制机制的意见), March 30, 2020, https://www.gov.cn/zhengce/2020-04/09/content_5500622.htm. Even earlier, the 13th Five-Year Plan (2016–2020) described data as a "basic strategic resource."

[3] Graham Webster and Rogier Creemers, trans., "Translation: Xi Jinping's Speech to the Politburo Study Session on the Digital Economy (Oct. 2021)," DigiChina, Stanford University, January 19, 2022, https://digichina.stanford.edu/work/translation-xi-jinpings-speech-to-the-politburo-study-session-on-the-digital-economy-oct-2021/.

[4] Xi Jinping, "Hold High the Great Banner of Socialism with Chinese Characteristics and Strive in Unity to Build a Modern Socialist Country in All Respects," report to the 20th National Congress of the Communist Party of China, October 16, 2022, Section XI, Xinhua English translation, https://english.news.cn/20221025/8eb6f5239f984f01a2bc45b5b5a0ad5d/c.html.

[5] Cyberspace Administration of China, General Secretary Xi Jinping's Introduction to Important Ideology Regarding China as a Cyber Powerhouse, Chapter 5: "Building a Durable National Cybersecurity Barrier" (Beijing: People's Publishing House, July 2023), translated by Dakota Cary, Interpret: China, Center for Strategic and International Studies, https://interpret.csis.org/translations/general-secretary-xi-jinpings-introduction-to-important-ideology-regarding-china-as-a-cyber-powerhouse-chapter-5-building-a-durable-national-cybersecurity-barrier/.

[6] Chen Xiangyang, "What is the Deeper Significance of the Phrase 'Leverage the New Security Pattern to Ensure the New Development Pattern'?" *Theory Weekly* (理论周刊), February 14, 2023, translated and annotated by the Center for Strategic Translation, China Open Source Observatory, https://chinaopensourceobservatory.org/articles/what-is-the-deeper-significance-of-the-phrase-leverage-the-new-security-pattern-to-ensure-the-new-development-pattern.

[7] Ibid.

[8] Jamie P. Horsley, "Behind the Facade of China's Cyber Super-Regulator: What We Think We Know — and What We Don't — about the Cyberspace Administration of China," DigiChina, Stanford University, August 8, 2022, https://digichina.stanford.edu/work/behind-the-facade-of-chinas-cyber-super-regulator/.

[9] Ibid.

[10] Rogier Creemers, "In a League of Its Own: The Cyberspace Administration of China," *The Diplomat*, November 28, 2023, https://thediplomat.com/2023/11/in-a-league-of-its-own-the-cyberspace-administration-of-china/.

[11] Yi Ma and Chunrong Liu, "Three Faces of the State in Local Cyberspace Administrations: Development, Regulation, and Surveillance in China's Internet Governance," Journal of Chinese Political Science (published online November 10, 2025), https://doi.org/10.1007/s11366-025-09923-8.

[12] Chambers and Partners, "Data Protection and Privacy 2025 — China," March 2025, https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2025/china.

[13] Horsley, DigiChina, 2022 (above).

[14] TC260, "Data Security Technology — Rules for Data Classification and Grading" (GB/T 43697-2024), March 21, 2024, https://www.tc260.org.cn/upload/2024-03-21/1711023239820042113.pdf. Sectoral significance also in James Gong, "China Data Protection and Cybersecurity: Annual Review of 2024 and Outlook for 2025 (II)," Bird & Bird, February 2025, https://www.twobirds.com/en/insights/2025/china/china-data-protection-and-cybersecurity-annual-review-of-2024-and-outlook-for-2025-(ii).

[15] TC260 AI Safety Governance Framework, September 9, 2024, and CAC endorsement in SESEC V China Standardisation Newsletter, January–February 2025, https://sesec.eu/wp-content/uploads/2025/03/SESEC-V-Newsletter-January-February-2025.pdf. TC260 generative AI standards output in CSET translation series, https://cset.georgetown.edu/publication/china-safety-requirements-for-generative-ai-final/.

[16] James Gong, Tanya Luo, and Michael Dong, "China Cybersecurity and Data Protection Monthly Update — May 2025 Issue," Bird & Bird, May 2025, https://www.twobirds.com/en/insights/2025/china/china-cybersecurity-and-data-protection-monthly-update-may-2025-issue; TC260's role on ISO/IEC JTC1/SC27 (Information Security, Cybersecurity and Privacy Protection) confirmed via JTC1 Information, "SC 27 – Information Security, Cybersecurity and Privacy Protection," Standing Document 2: History of JTC1, https://jtc1info.org/sd-2-history/jtc1-subcommittees/sc-27/.

[17] Tom Nunlist (Senior Analyst for Tech and Data Policy, Trivium China), quoted in "China's Proposed National Data Bureau to Become a Powerful Tool for Beijing to Ratchet Up Development of Digital Economy, Analysts Say," South China Morning Post, March 8, 2023, republished on Yahoo Finance, https://finance.yahoo.com/news/chinas-proposed-national-data-bureau-093000914.html.

[18] Kendra Schaefer, Tom Nunlist, Zeng Chen, Jamie Horsley, DigiChina Discussion Group thread on CAC draft financial data classification guideline, January 26–27, 2026. CAC draft directly accessed at https://www.cac.gov.cn/2026-01/24/c_1770812246428118.htm. National Financial Regulatory Administration, "Measures on the Administration of Data Security in Banking and Insurance Institutions," December 2024, https://www.gov.cn/zhengce/zhengceku/202412/content_6995081.htm.

[19] Chambers and Partners, "Data Protection and Privacy 2025 — China," March 2025, https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2025/china.

[20] Ministry of Industry and Information Technology, "Important Data Identification Guidelines in the Industrial Field," effective April 1, 2025; Reed Smith, "China's Key Data and Privacy Developments in the First Eight Months of 2025," https://www.reedsmith.com/articles/chinas-key-data-and-privacy-developments-in-the-first-eight-months-of-2025/.

[21] Global Investigations Review, "China: Legal and Enforcement Shifts in a New Era of Assertiveness," 2026, https://globalinvestigationsreview.com/review/the-asia-pacific-investigations-review/2026/article/china-legal-and-enforcement-shifts-in-new-era-of-assertiveness. James Gong, "China Data Protection and Cybersecurity: Annual Review of 2024 and Outlook for 2025 (II)," Bird & Bird, February 2025, https://www.twobirds.com/en/insights/2025/china/china-data-protection-and-cybersecurity-annual-review-of-2024-and-outlook-for-2025-(ii).

[22] Rogier Creemers, "China's National Data Bureau and Global Data Governance," Internet Policy Review, May 2, 2023, https://policyreview.info/articles/news/chinas-national-data-bureau-and-global-data-governance.

[23] Graham Webster and Rogier Creemers, "Micron and China's Cybersecurity Review," DigiChina, Stanford University, May 2023, https://digichina.substack.com/p/micron-and-chinas-cybersecurity-review; All characterizations of the DiDi case, CRO discretionary authority, and regime timeline are drawn directly from this analysis. Cybersecurity Review Measures (2022 edition), China Law Translate, https://www.chinalawtranslate.com/en/17598-2/.

[24] Graham Webster and Rogier Creemers, "Micron and China's Cybersecurity Review," DigiChina, Stanford University, May 2023, https://digichina.substack.com/p/micron-and-chinas-cybersecurity-review.

[25] Lexology, "China's Cybersecurity Review Regime: Framework and Latest Trends," April 2023, https://www.lexology.com/library/detail.aspx?g=dd7d2c5a-b301-4f0c-a72b-226423ec9a74.

[26] Arnold & Porter (John Tan, Sheena Thomas, Siyi Gu), "China Data Privacy and Cybersecurity: 2025 Year in Review," February 13, 2026, https://www.arnoldporter.com/en/perspectives/advisories/2026/02/china-data-privacy-and-cybersecurity-2025-year-in-review.

[27] Arnold & Porter (John Tan, Sheena Thomas, Siyi Gu), "China Data Privacy and Cybersecurity: 2025 Year in Review," February 13, 2026, https://www.arnoldporter.com/en/perspectives/advisories/2026/02/china-data-privacy-and-cybersecurity-2025-year-in-review.

[28] Covington & Burling, "China Amends Cybersecurity Law and Incident Reporting Regime to Address AI and Infrastructure Risks," Inside Privacy, October 29, 2025, https://www.insideprivacy.com/cybersecurity-2/china-amends-cybersecurity-law-and-incident-reporting-regime-to-address-ai-and-infrastructure-risks/.

New Zealand Ministry of Foreign Affairs and Trade, "China's Data Governance Framework Takes Shape: Implications for New Zealand Businesses," MFAT Market Reports, https://www.mfat.govt.nz/en/trade/mfat-market-reports/chinas-data-governance-framework-takes-shape-implications-for-new-zealand-businesses.

[30] Li Sanxi, "Data Elements Market Critical to Growth," China Daily, July 8, 2024, https://www.chinadaily.com.cn/a/202407/08/WS668b4709a31095c51c50ced9.html.

[31] "China Unveils Action Plan to Promote High-Quality Development of Data Sector," The State Council of the People's Republic of China, January 5, 2024, https://english.www.gov.cn/news/202401/05/content_WS65973ab3c6d0868f4e8e2c44.html.

[32] Fan Feifei, "'Digital China' the Priority for 2026," China Daily Hong Kong, January 5, 2026, https://www.chinadailyhk.com/hk/article/626571; Rogier Creemers, "China's National Data Bureau and Global Data Governance," Internet Policy Review, May 2, 2023, https://policyreview.info/articles/news/chinas-national-data-bureau-and-global-data-governance.

[33] Jingjing Li, Limei Gao, and Jiayou Shi, "Too Good to Be True? China's New Conceptual Scheme for Data Property Rights," Telecommunications Policy 50, no. 3 (2026): 103145, https://doi.org/10.1016/j.telpol.2025.103145.

[34] "China Establishes Data Organisation Aimed at Global Industry Consensus," Reuters, March 31, 2026, https://www.reuters.com/business/media-telecom/china-establishes-data-organisation-aimed-global-industry-consensus-2026-03-31/.

[35] CPC Central Committee and State Council, "Opinions on Building a Data Fundamental System to Better Play the Role of Data Elements" (关于构建数据基础制度更好发挥数据要素作用的意见), adopted December 2, 2022, published December 19, 2022, https://www.gov.cn/zhengce/2022-12/19/content_5732695.htm. All translations by the author.

[36] Liu Liehong, head of the National Data Administration, press conference remarks, August 2025, reported by Xinhua, https://english.news.cn/20250814/de3dbd5115d04306a0e0ead082de425f/c.html.

[37] Luo M. and Tian M., "Idealism Abundant, Reality Gaunt: The Six Years of Guiyang Big Data Exchange," cited in Xueting Fu, "The Dilemma and Resolution of Data Circulation in China," *Computer Law and Security Review*, ScienceDirect, November 2024, https://www.sciencedirect.com/science/article/abs/pii/S0267364924001407. Note: original Chinese-language article not directly accessed; cited via secondary reference.

[38] Centre for International Governance Innovation (CIGI), "Data Marketplaces and Governance: Lessons from China," https://www.cigionline.org/articles/data-marketplaces-and-governance-lessons-from-china/.

[39] James Gong, "China Data Protection and Cybersecurity: Annual Review of 2024 and Outlook for 2025 (II)," Bird & Bird, February 2025, https://www.twobirds.com/en/insights/2025/china/china-data-protection-and-cybersecurity-annual-review-of-2024-and-outlook-for-2025-(ii).

[40] Shaokun Huang and Le Cheng, "Experiences, Challenges, and Improvements in the Construction of Data Property Rights in China," *Computer Law & Security Review*, Vol. 59, Elsevier, November 2025, https://www.sciencedirect.com/science/article/abs/pii/S2212473X25001002.

[41] Ibid.

[42] "The Rise of Data Property Rights in China: How Does It Compare with the EU Data Act and What Does It Mean for Digital Trade with China?" *Journal of International Economic Law*, Vol. 27, No. 3, October 2024, https://academic.oup.com/jiel/article/27/3/462/7750423.

[43] Max Fenkell, Global Head of Policy and Government Relations, Scale AI, testimony before the House Committee on Homeland Security, "DeepSeek and Unitree Robotics: Examining the National Security Risks of PRC Artificial Intelligence, Robotics, and Autonomous Technologies, and Building a Secure U.S. Technology Base," 2026, https://homeland.house.gov/hearing/deepseek-and-unitree-robotics-examining-the-national-security-risks-of-prc-artificial-intelligence-robotics-and-autonomous-technologies-and-building-a-secure-u-s-technology-base/.

[44] Ngor Luong, "Two Loops: How China's Open AI Strategy Reinforces Its Industrial Dominance," USCC Research Working Group Paper, March 23, 2026, https://www.uscc.gov/sites/default/files/2026-03/Two_Loops--How_Chinas_Open_AI_Strategy_Reinforces_Its_Industrial_Dominance.pdf.

[45] Max Fenkell, Global Head of Policy and Government Relations, Scale AI, testimony before the House Committee on Homeland Security, "DeepSeek and Unitree Robotics: Examining the National Security Risks of PRC Artificial Intelligence, Robotics, and Autonomous Technologies, and Building a Secure U.S. Technology Base," 2026, https://homeland.house.gov/hearing/deepseek-and-unitree-robotics-examining-the-national-security-risks-of-prc-artificial-intelligence-robotics-and-autonomous-technologies-and-building-a-secure-u-s-technology-base/.

[46] MIIT and 17 co-signing agencies, "Robotics+ Application Action Plan," January 2023, China Briefing, "The Chinese Humanoid Robot AI Market," July 10, 2025, https://www.china-briefing.com/news/chinese-humanoid-robot-market-opportunities/.

[47] MIIT, "Guiding Opinions on the Innovative Development of Humanoid Robots," October 20, 2023, via Jamestown Foundation, "Embodied Intelligence: The PRC's Whole-of-Nation Push into Robotics," November 17, 2025, https://jamestown.org/embodied-intelligence-the-prcs-whole-of-nation-push-into-robotics/.

[48] Georg Stieler, "China Experiences Physical AI Surge — and How the U.S. Should Respond," The Robot Report, September 10, 2025, https://www.therobotreport.com/china-experiences-physical-ai-surge-how-u-s-should-respond/.

[49] Xinhua, "China Promotes Data Labeling to Spur AI Development," State Council of the People's Republic of China, January 14, 2025, https://english.www.gov.cn/news/202501/14/content_WS67859ba1c6d0868f4e8eeca1.html.

[50] State Council of the People's Republic of China, "Implementation Opinions on Promoting the High-Quality Development of the Data Labeling Industry," December 2024, reported via english.www.gov.cn, January 14, 2025, https://english.www.gov.cn/news/202501/14/content_WS67859ba1c6d0868f4e8eeca1.html.

[51] Viola Zhou and Kinling Lo, "In Chinese Data Factories, Workers Teach Humanoid Robots Boring Tasks," Rest of World, January 7, 2026, https://restofworld.org/2026/china-robots-training-centers-workers/.

[52] Kyle Chan, Gregory Smith, Jimmy Goodrich, Gerard DiPippo, and Konstantin F. Pilz, Full Stack: China's Evolving Industrial Policy for AI (RAND Corporation, June 26, 2025), https://www.rand.org/pubs/perspectives/PEA4012-1.html, citing Xinhua, "China Pools Efforts to Fuel Development of Embodied AI Robotics," State Council of the People's Republic of China, October 11, 2024, https://english.www.gov.cn/news/202410/11/content_WS67092284c6d0868f4e8ebb88.html; Shanghai center general manager quote via U.S.-China Economic and Security Review Commission, Humanoid Robots, October 2024, https://www.uscc.gov/sites/default/files/2024-10/Humanoid_Robots.pdf.

[53] Georg Stieler, "China Experiences Physical AI Surge — and How the U.S. Should Respond," The Robot Report, September 10, 2025, https://www.therobotreport.com/china-experiences-physical-ai-surge-how-u-s-should-respond/.

[54] Kyle Chan, Gregory Smith, Jimmy Goodrich, Gerard DiPippo, and Konstantin F. Pilz, Full Stack: China's Evolving Industrial Policy for AI (RAND Corporation, June 26, 2025), https://www.rand.org/pubs/perspectives/PEA4012-1.html, citing Xinhua, "China Pools Efforts to Fuel Development of Embodied AI Robotics," State Council, October 11, 2024, https://english.www.gov.cn/news/202410/11/content_WS67092284c6d0868f4e8ebb88.html.

[55] Georg Stieler, "China Experiences Physical AI Surge — and How the U.S. Should Respond," The Robot Report, September 10, 2025, https://www.therobotreport.com/china-experiences-physical-ai-surge-how-u-s-should-respond/.

[56] ScienceDirect, “Developing China’s Approaches to Regulate Cross-Border Data Transfer: Relaxation and Integration,” September 2024, https://www.sciencedirect.com/science/article/abs/pii/S0267364924000645

[57] IAPP, “China’s new cross-border data transfer regulations: What you need to know and do,” April 03, 2024, https://iapp.org/news/a/chinas-new-cross-border-data-transfer-regulations-what-you-need-to-know-and-do

[58] James Gong and Yiting Wang, "China Data Protection and Cybersecurity: Annual Review of 2025 and Outlook for 2026 (II)," Bird & Bird, April 2026, https://www.twobirds.com/en/insights/2026/china/china-data-protection-and-cybersecurity-annual-review-of-2025-and-outlook-for-2026-(ii).

[59] Arnold & Porter (John Tan, Sheena Thomas, and Siyi Gu), "China Data Privacy and Cybersecurity: 2025 Year in Review," Advisory, February 13, 2026, https://www.arnoldporter.com/en/perspectives/advisories/2026/02/china-data-privacy-and-cybersecurity-2025-year-in-review.

[60] John Tan and Siyi Gu, "China Clarifies Cross-Border Data Transfer Rules: Practical Guidance for Compliance," Arnold & Porter Advisory, June 6, 2025,

https://www.arnoldporter.com/en/perspectives/advisories/2025/06/china-clarifies-cross-border-data-transfer-rules.

61 Samm Sacks, Krystal Chen Zeng, and Graham Webster, "Moving Data, Moving Target: Uncertainties Remain in China's Overhauled Cross-Border Data Transfer Regime," DigiChina, Stanford University, October 25, 2024, https://digichina.stanford.edu/work/moving-data-moving-target/

62 China Briefing, "China Releases Certification Measures for Cross-Border Data Transfers – The Last Piece of the Regulatory Puzzle," October 24, 2025, https://www.china-briefing.com/news/china-cross-border-data-transfer-certification/

63 Arnold & Porter, "China Data Privacy and Cybersecurity: 2025 Year in Review," February 13, 2026, https://www.arnoldporter.com/en/perspectives/advisories/2026/02/china-data-privacy-and-cybersecurity-2025-year-in-review

64 Samm Sacks, Krystal Chen Zeng, and Graham Webster, "Moving Data, Moving Target: Uncertainties Remain in China's Overhauled Cross-Border Data Transfer Regime," DigiChina, Stanford University, October 25, 2024, https://digichina.stanford.edu/work/moving-data-moving-target/

65 Reed Smith, "China's Key Data and Privacy Developments in the First Eight Months of 2025," February 2026, https://www.reedsmith.com/articles/chinas-key-data-and-privacy-developments-in-the-first-eight-months-of-2025/.

66 Samm Sacks, Krystal Chen Zeng, and Graham Webster, "Moving Data, Moving Target: Uncertainties Remain in China's Overhauled Cross-Border Data Transfer Regime," DigiChina, Stanford University, October 25, 2024, https://digichina.stanford.edu/work/moving-data-moving-target/

67 Samm Sacks, Krystal Chen Zeng, and Graham Webster, "Moving Data, Moving Target: Uncertainties Remain in China's Overhauled Cross-Border Data Transfer Regime," DigiChina, Stanford University, October 25, 2024, https://digichina.stanford.edu/work/moving-data-moving-target/

68 Ibid.

69 Standing Committee of the National People's Congress, "Data Security Law of the People's Republic of China" (中华人民共和国数据安全法), Article 36, effective September 1, 2021, https://www.gov.cn/zhengce/2021-06/11/content_5616919.htm; Jones Day, "China's New Data Security Law Restricts Cross-Border Transfers of Data," August 2021, https://www.jonesday.com/en/insights/2021/08/chinas-new-data-security-law-restricts-crossborder-transfers-of-data; DLA Piper, "China's Emerging Data Protection Laws Bring Challenges for Conducting Investigations in China," July 2022, https://www.dlapiper.com/en-us/insights/publications/2022/07/chinas-emerging-data-protection-laws-bring-challenges-for-conducting-investigations-in-china;

70 Jones Day, "Chinese Law Restricts Cross-Border Data Transfers," August 26, 2021, https://www.jonesday.com/en/insights/2021/08/chinas-new-data-security-law-restricts-crossborder-transfers-of-data.

71 China Law Translate, "National Intelligence Law of the P.R.C. (2017)," https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/.

72 The Diplomat, "The Real Danger of China's National Intelligence Law," February 23, 2019, https://thediplomat.com/2019/02/the-real-danger-of-chinas-national-intelligence-law/.

73 U.S. Department of Homeland Security, "Data Security Business Advisory: Risks and Considerations for Businesses Using Data Services and Equipment from Firms Linked to the People's Republic of China," December 22, 2020, https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf.

74 Jeremy Daum, "What China's National Intelligence Law Says, And Why It Doesn't Matter," China Law Translate, May 6, 2025, https://www.chinalawtranslate.com/en/what-the-national-intelligence-law-says-and-why-it-doesnt-matter/.

75 Bain & Company, "Singles Day 2025 Goes Global as Chinese E-Commerce Players Outgrow Domestic Market," press release, October 30, 2025, https://www.bain.com/about/media-center/press-releases/20252/singles-day-2025-goes-global-as-chinese-e-commerce-players-outgrow-domestic-market/.

76 Momentum Works, *Ecommerce in Southeast Asia 2024* (Singapore: Momentum Works, 2024), https://thelowdown.momentum.asia/.

77 CSIS, "China's Digital Silk Road and Southeast Asia," https://reconasia.csis.org/chinas-digital-silk-road-and-southeast-asia/.

78 Vietnam, Decree 53/2022/ND-CP on Cybersecurity (August 15, 2022, effective October 1, 2022), discussed in U.S. Department of Commerce, International Trade Administration, "Vietnam: Cybersecurity Data Localization Requirements," September 20, 2022, https://www.trade.gov/market-intelligence/vietnam-

cybersecurity-data-localization-requirements; Indonesia, Government Regulation No. 71 of 2019 on the Operation of Electronic Systems and Transactions (effective October 10, 2019), discussed in Nigel Cory, "Indonesia's Data Localization Regulation," Information Technology and Innovation Foundation, June 9, 2025, https://itif.org/publications/2025/06/09/indonesia-data-localization-regulation/; see also Platform for Peace and Humanity, "The New Data Frontiers: How Tech Power Shifts Shape Privacy and Surveillance in Asia," November 2025, https://peacehumanity.org/monitor/the-new-data-frontiers-how-tech-power-shifts-shape-privacy-and-surveillance-in-asia/.

79 World Benchmarking Alliance, "Ranking Digital Rights Index: The State of Big Tech in 2025," November 2025, https://www.worldbenchmarkingalliance.org/latest/ranking-digital-rights-index-state-big-tech-2025.

80 Nigel Cory, testimony before the US-China Economic and Security Review Commission, April 15, 2021 (above), citing Alibaba Cloud statements in Indian press, 2018.

81 CGTN, “World Data Organization: WDO launched in Beijing to bridge global data divide,” March 30, 2026, https://news.cgtn.com/news/2026-03-30/VHJhbnNjcmlwdDg5OTMw/index.html

82 Yahoo Finance “China establishes data organization aimed at global industry consensus,” March 30, 2026, https://finance.yahoo.com/sectors/technology/articles/china-establishes-data-organisation-aimed-004617562.html

83 Reuters, “China establishes data organization aimed at global industry consensus,” March 31, 2026, https://www.reuters.com/business/media-telecom/china-establishes-data-organisation-aimed-global-industry-consensus-2026-03-31/.

84 DiplFoundation, “The role of the World Data Organization on the digital sovereignty chessboard,” April 01, 2026, https://www.diplomacy.edu/blog/the-role-of-the-world-data-organization-on-the-digital-sovereignty-chessboard/.

85 People’s Daily Online, “World Data Organization established to bridge global data divide,” April 07, 2026, https://en.people.cn/n3/2026/0407/c90000-20444091.html.

86 China Law Asia, "Dispute over AI Model Distillation Tech in OpenAI-DeepSeek Case," September 26, 2025, https://law.asia/openai-deepseek-ai-distillation/.

87 China Law Asia, "Dispute over AI Model Distillation Tech in OpenAI-DeepSeek Case," September 2025, https://law.asia/openai-deepseek-ai-distillation/.

88 Joe Khawam, "The Case for Imposing Costs on China's AI Distillation Campaigns," *Just Security*, March 30, 2026, https://www.justsecurity.org/134124/costs-china-ai-distillation/.

89 Joe Khawam, "The Case for Imposing Costs on China's AI Distillation Campaigns," *Just Security*, March 30, 2026, https://www.justsecurity.org/134124/costs-china-ai-distillation/.

90 Institute for AI Policy and Strategy, "AI Distillation Attacks: The Case for Targeted Government Intervention," March 18, 2026, https://www.iaps.ai/research/ai-distillation-attacks-the-case-for-targeted-government-intervention.

91 CGTN, "World Data Organization Launches in Beijing to Boost Data Governance," March 30, 2026, https://news.cgtn.com/news/2026-03-30/World-Data-Organization-launches-in-Beijing-to-boost-data-governance-1LW8SriyLq8/p.html.

92 Liu Liehong, "Using Advanced Data Infrastructure to Support the Construction of Digital China," *Qiushi*, March 1, 2026, via https://digitalchinawinsthefuture.com/digital-china-national-data-infrastructure/; Liu Liehong (刘烈宏), "Using Advanced Data Infrastructure to Support the Construction of Digital China" (以高水平数据基础设施助力数字中国建设), *Qiushi* (求是), Issue 2026/05, March 1, 2026, https://www.qstheory.cn/20260228/b97f48ebe2f74b80b1c0249632f27b73/c.html. All translations by the author.

93 ICLG, "China's Key Developments in Artificial Intelligence Governance in 2025," December 2025, https://iclg.com/practice-areas/telecoms-media-and-internet-laws-and-regulations/03-china-s-key-developments-in-artificial-intelligence-governance-in-2025; Chambers and Partners, "Artificial Intelligence 2025 — China," May 2025, https://practiceguides.chambers.com/practice-guides/artificial-intelligence-2025/china; IAPP, "Global AI Governance Law and Policy: China," https://iapp.org/resources/article/global-ai-governance-china.

94 Reed Smith, "China's Key Data and Privacy Developments in the First Eight Months of 2025," February 2026, https://www.reedsmith.com/articles/chinas-key-data-and-privacy-developments-in-the-first-eight-months-of-2025/.

95 Platform for Peace and Humanity, "The New Data Frontiers: How Tech Power Shifts Shape Privacy and Surveillance in Asia," November 2025, https://peacehumanity.org/monitor/the-new-data-frontiers-how-tech-power-shifts-shape-privacy-and-surveillance-in-asia/.

[96] Cyberspace Administration of China, "Regulation on Promoting and Regulating Cross-Border Data Flows," Article 5, March 22, 2024, https://www.cac.gov.cn/2024-03/22/c_1712776611775634.htm.

[97] President Joseph R. Biden, Executive Order 14117, February 28, 2024, https://www.whitehouse.gov/presidential-actions/2024/02/executive-order-on-preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related-data-by-countries-of-concern/.

[98] NIST, "Post-Quantum Cryptography," https://csrc.nist.gov/projects/post-quantum-cryptography; NIST IR 8547, November 2024, https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf.

[99] Nigel Cory, testimony before the US-China Economic and Security Review Commission, Panel on China's Cloud Market, April 15, 2021, Information Technology and Innovation Foundation (ITIF).

[100] Nigel Cory and Samm Sacks, "China Gains as U.S. Abandons Digital Policy Negotiations," *Lawfare*, November 15, 2023, https://www.lawfaremedia.org/article/china-gains-as-u.s.-abandons-digital-policy-negotiations.

[101] Senators Todd Young, Chris Coons, Jerry Moran, and Michael Bennet, Digital Trade Promotion Act. Senate press release: https://www.young.senate.gov/newsroom/press-releases/young-colleagues-introduce-bill-to-strengthen-american-leadership-in-digital-trade/.

[102] US-China Economic and Security Review Commission, "2024 Annual Report to Congress."

[103] Crowell Global Advisors, "ASEAN Digital Ministers' Meeting 2026: Spotlight on AI Cooperation in Asia's Rising Markets," January 29, 2026, https://www.crowell.com/en/insights/client-alerts/asean-digital-ministers-meeting-2026-spotlight-on-ai-cooperation-in-asias-rising-markets.

[104] ASEAN Framework on Cross-Border Cloud Computing and accompanying landscape study, endorsed at the 6th ASEAN Digital Ministers' Meeting, https://bit.ly/4bVbxML. See also the author's analysis at LinkedIn, https://www.linkedin.com/posts/nigelcory_asean-framework-on-cross-border-cloud-computing-activity-7429562973053943813-L6uP/.

[105] "Declaration on Government Access to Personal Data Held by Private Sector Entities," OECD, OECD Legal Instruments, December 14, 2022, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487.

[106] Executive Order 14117, "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern," February 28, 2024, The American Presidency Project, https://www.presidency.ucsb.edu/documents/executive-order-14117-preventing-access-americans-bulk-sensitive-personal-data-and-united.

[107] Nigel Cory, "Technical and Legal Criteria for Assessing Cloud Trustworthiness," ITIF, April 22, 2024, https://itif.org/publications/2024/04/22/technical-legal-criteria-for-assessing-cloud-trustworthiness.

[108] Mackenzie Hawkins, "US Plans AI Chip Curbs on Malaysia, Thailand Over China Concerns," Bloomberg, July 4, 2025, https://www.bloomberg.com/news/articles/2025-07-04/us-plans-ai-chip-curbs-on-malaysia-thailand-over-china-concerns.