The Authoritarian Gaze

China's Global Data Reach and the Systemic Risks to Democracy

You-Hao Lai

January 2026

The Authoritarian Gaze

China's Global Data Reach and the Systemic Risks to Democracy

Research Institute for Democracy, Society and Emerging Technology (DSET)

Founded in October 2023 by Taiwan's National Science and Technology Council (NSTC), the Research Institute for Democracy, Society, and Emerging Technology (DSET) is Taiwan's first national think tank focused on the intersection of democracy, technology, and public policy. DSET places democratic values at the core of its mission and addresses emerging global challenges through evidence-based research and strategic analysis.

DSET's research focuses on four key areas: Economic Security, Democratic Governance, Climate Resilience and Sustainability, and National Security. It also operates a Non-Resident Fellow program that engages Taiwanese scholars and graduate students based in the United States, Europe, Japan, and other like-minded countries. Through policy research, international dialogue, and Track 1.5 diplomacy, DSET provides strategic recommendations to the public and government, strengthens Taiwan's global engagement, and promotes democratic, future-oriented approaches to technology governance.

Democratic Governance Program

The Democratic Governance Program studies how digital technologies shape the resilience of democratic institutions. A core strand examines China's AI development and its impact on democracies. The program analyzes how China's state-directed AI ecosystem, built on extensive data access, surveillance infrastructures, and security-driven regulation, produces technologies that may carry authoritarian features when deployed abroad. It studies how Chinese AI systems spread through commercial platforms and digital services, and how their adoption can affect transparency, accountability, and institutional resilience in democratic societies.

Disclaimer

This report was independently reviewed and published by DSET. The views expressed herein are solely those of the authors and do not represent the official position of the Government of Taiwan or the National Science and Technology Council (NSTC).

Authors

You-Hao Lai | Deputy Director of Democratic Governance Program

You-Hao Lai is a legal scholar, practicing attorney, and think tank fellow with expertise in democratic governance, technology law, and digital policy in Taiwan and the Indo-Pacific. At the Democratic Governance Program of DSET, his work focuses on how democracies can safeguard their information environments and respond to AI-enabled digital authoritarianism. His research spans cybersecurity, data protection and privacy, cross-border data governance, and foreign information manipulation and interference (FIMI). He is currently a Doctor of Juridical Science (S.J.D.) candidate at the George Washington University Law School and holds an LL.M. degree from Harvard Law School.

Contributors

Eddy Yen-Ting Lin | Non-resident Fellow

Eddy Lin is a Doctor of Juridical Science (J.S.D.) candidate at the University of California, Berkeley, School of Law. His research focuses on law and technology, comparative constitutional law, law and democracy, and the regulation of artificial intelligence. For this report, Eddy contributed by analyzing the data practices of selected China-linked AI services, identifying legal loopholes in Taiwan's existing data governance structure, reviewing and summarizing the full report, and providing legal refinement suggestions throughout.

Violet Yueh-Ning Chiang | Non-resident Fellow

Violet (Yueh-Ning) Chiang is a Master of Science in Foreign Service (MSFS) candidate at Georgetown University. She specializes in Chinese influence operations, open-source intelligence, and data visualization. She contributed to this report on Chinese AI services' data collection practices, focusing specifically on categorization and visualization.

Acknowledgements

The Democratic Governance Program of DSET extends its sincere gratitude to the following individuals for their contributions to the completion of this report. The author thanks Kai-Shen Huang for his input on the report structure and editing; Ali Demir for his research assistance in the early stages of this report; Tsai-Yuan Tsai and Ting-Kai Lu for visual design; Chia-Tien Hsu and You-Lei Su for their assistance with formatting and editing; Kuan-Wei Chen and Dah-Wei (David) Yih for their feedback on the report's arguments; Szu-Yu Chen and Min-Yen Chiang for their reviews of legal and media sources; and Yun-Ting Cai for his insights on data presentation and visualization.

The author is also grateful to many researchers and experts whose perspectives, shared during workshops and events, contributed to the refinement of this report. This report reflects the independent analysis of the Democratic Governance Program and does not necessarily represent the views of the individuals acknowledged. All errors or omissions are the sole responsibility of our team.

Table of Contents

List of Tables

List of Figures

Executive Summary

Amid China's expanding global data reach—fueled by the rapid international adoption of China-linked artificial intelligence—this report examines how the People's Republic of China is projecting an authoritarian model of data governance beyond its borders and how AI services controlled by Chinese entities may reinforce that model.

It then outlines the systemic risks these data practices pose to privacy and democratic resilience, and proposes a **DSR strategy: Defend public systems, Screen Chinese AI services, and Rally democratic allies for regulatory harmonization.** The name "DSR strategy" is deliberately chosen to counter China's own DSR: the Digital Silk Road, which represents Beijing's broader push for geopolitical influence through exporting digital infrastructure and shaping global data norms.

Part I. China's Global Data Reach and Authoritarian Governance

China's data governance model is characterized by authoritarian features rooted in arbitrary party-state power and a lack of institutional checks on data access. At the corporate level, party-state integration enables the Chinese government to exert influence over company decision-making and compel compliance with state data demands. This is reinforced by expansive data access laws that require Chinese firms to hand over data collected abroad, along with outbound transfer restrictions for information deemed relevant to national security or strategic interests.

Beyond facilitating an asymmetrical global flow of data, **China's party-state dominant model** is defined by sweeping "holistic national security" justifications, the absence of independent judicial oversight, and broad exemptions for state actors from personal data protection obligations. As Chinese digital services gain footholds in foreign markets, this model generates systemic risks for global privacy and democratic resilience.

Part II. Data Practices of Chinese AI Services: A Privacy Policy Review

The risks posed by China's authoritarian governance model are further compounded by the data practices of its digital service providers. Drawing on credible media sources and a review of privacy policies accessible to users in Taiwan, this report analyzes the data practices of ten widely used generative AI services with reported operational links to China.

- Some services explicitly state that they **store user data in China.**
- Others, despite being operated by entities incorporated abroad, maintain **corporate structures, intra-group data transfer mechanisms, and legal obligations** that create channels through which globally collected personal data can be transferred to or accessed by Chinese government authorities.
- Across 11 identified data types, most services collect between 8 and 11, averaging nearly **9 per provider**. Particularly concerning are practices involving the collection of **user inputs, sensitive data, and inferred personal information.**

Importantly, these findings suggest that **even services registered outside the PRC—possibly in an effort to "de-China"—do not necessarily eliminate the pathways through which overseas user data may flow back to China.**

Part III. The PRC's Potential Data Access and Risks to Democracy

China's expanding global data access poses risks that span from individual privacy to the foundations of democratic governance.

Through broad **consent mechanisms**, users of reportedly China-linked AI services effectively grant a "blank check" for extensive data collection, storage in China, and intra-group data sharing. The pervasive harvesting of personal information, combined with inferences about sensitive traits, enables the construction of detailed **user profiles** that

render individuals transparent, fixed, and predictable. These intrusive profiles, when paired with AI models trained or fine-tuned on globally sourced data, can significantly enhance China's **intelligence-gathering capabilities.**

At the societal level, aggregated user data enables the construction of a comprehensive "**societal mosaic**" of democratic communities, exposing their vulnerabilities and social fault lines. This "authoritarian gaze" threatens the "obscurity" that underpins privacy and enables more targeted, covert, and cognitively potent **influence operations**. Together, these forms of data exploitation undermine autonomy, both individual and collective, and present a profound challenge to democratic resilience.

Part IV. Policy Recommendations: The DSR Strategy

To address these risks, this report proposes a three-part **DSR strategy** for Taiwan and its democratic partners:

1. **Defend** public systems by banning AI services that are substantially controlled by China-based or Chinese-owned entities from use in government and critical infrastructure.

2. **Screen** these Chinese AI services through inbound review mechanisms that condition market access on compliant data practices—particularly by default prohibiting the transfer of user data to China.

3. **Rally** democratic allies to harmonize cross-border data regulations and build collective resilience against authoritarian data exploitation.

Taiwan must urgently reform its overly permissive cross-border data transfer regulations. By prioritizing data practices, the **operational-centric approach** proposed in this report offers a more practical alternative to ownership-centric models, such as TikTok bans, currently being pursued in the United States.

Introduction: Authoritarian Data Governance in China's AI Expansion

When China's AI Push Go Global

From telecom networks and data centers to social platforms, China's growing global digital footprint is raising alarm over the flow of data to China and the potential for authoritarian access.[1] Labeled by scholars as China's "data trafficking,"[2] these concerns have grown more acute with the rise of artificial intelligence (AI). AI is inherently data-hungry: training models and generating inferences, especially for generative AI and large language models (LLMs), requires constant streams and unprecedented amounts of data.[3]

Meanwhile, China is promoting the global expansion of its AI technologies. Long committed to an application-driven AI strategy, it prioritizes rapid, large-scale deployment to accelerate commercialization and ensure global market readiness.[4] Most recently, China's Ministry of Commerce issued *The Several Policy Measures on Promoting Service Exports* (关于促进服务出口的若干政策措施),[5] further signaling that China is not merely exporting manufactured goods, but is positioning itself as a global provider of data-driven and AI-enabled services.

Under this strategic push, Chinese AI is gaining significant traction worldwide. China now reportedly accounts for 36 percent of the world's 1,328 LLMs, second only to the United States.[6] Nearly one-fifth of global users now opt for Chinese-developed AI models, largely due to their cost-effectiveness.[7] This adoption extends well beyond individual users to major corporations: HSBC and Standard Chartered have reportedly tested DeepSeek internally; Saudi Aramco has deployed it in its main data center; and leading cloud providers, including AWS, Microsoft, and Google, are offering DeepSeek services to their clients.[8]

Even more significantly, Chinese AI systems are increasingly embedded in a wide array of consumer products and devices—from multimodal AI agents and audiovisual content generators to operating systems for mobiles and robotics.[9] This global diffusion has accelerated since the launch of DeepSeek, which is especially attractive to countries lacking the infrastructure to develop reliable AI systems of their own.[10] A recent

report by leading venture capital firm Andreessen Horowitz further indicates that almost half (22) of the top 50 generative AI applications by monthly active users were developed in China—though only three are primarily used domestically.[11]

China's Expanding Data Reach and the Gap in Democratic Response

Accompanying the spread of Chinese AI services are **data practices that transmit the personal information of global users back to the People's Republic of China (PRC).**[12] For example, a recent investigation by Taiwan's National Security Bureau into five popular Chinese AI applications—such as DeepSeek and Doubao—highlights widespread data security risks, including requests for location access, screenshot capture, forced acceptance of unreasonable privacy policies, and the collection of device information.[13]

In response, many democracies have barred government agencies from using those services and tools, particularly DeepSeek.[14] Legislative efforts are also underway. In the U.S., for example, bipartisan lawmakers have introduced several bills, including the *No DeepSeek on Government Devices Act*, which would prohibit federal employees from using DeepSeek on government-issued devices;[15] the *No Adversarial AI Act*, which seeks to ban agencies from acquiring or using AI developed by companies linked to adversaries such as China;[16] and the *Protection Against Foreign Adversarial Artificial Intelligence Act*, which would bar federal contractors from deploying Chinese-developed AI systems.[17]

However, even if enacted, these measures remain narrowly focused on the public sector, **leaving the adoption of Chinese AI across the private sector largely unaddressed**. A similar gap exists in Taiwan. Although the *Cyber Security Management Act* (資通安全管理法) was amended earlier this year (2025),[18] its restrictions apply only to public entities and critical infrastructure providers, with little oversight of Chinese ICT products used in other sectors.

With few jurisdictions imposing restrictions beyond the public sector,[19] there remains no comprehensive framework to address the "inbound" spread of Chinese AI systems and services into democratic markets.[20] Adoption by businesses and individual consumers is largely unregulated: individuals can freely access these tools via the open internet, and companies are able to integrate them into their operations.

As a result, Chinese AI-powered products continue to cross borders and embed themselves in democratic information systems with few safeguards—**leaving democracies vulnerable to potential authoritarian data access and exploitation.**

Countering the Authoritarian Gaze: The DSR Strategy

Especially in an era where data and information flow across borders, freedom-loving societies must strike a balance between the openness of democratic environments and the risk of authoritarian abuse. Likewise, if one is to take AI's potential disruption to democracy seriously, it is crucial not to focus narrowly on how democracies build AI. A more immediate task is to develop a systematic approach for understanding, and remaining vigilant about, how authoritarian AI is quietly permeating democratic information ecosystems.

To do so, this report shows and explains **how the PRC is projecting its authoritarian approach to data access and control globally, an effort that may be reinforced by the rise of China-linked AI services, and how like-minded countries can respond to the democratic challenges these data practices pose.**

It begins by analyzing the authoritarian characteristics of the PRC's data governance framework, then explores how Chinese AI services may be extending that model worldwide, and concludes with policy recommendations to safeguard democracy against the systemic risks of authoritarian data control.

Importantly, for the purposes of this report, "Chinese" services are defined not solely by formal registration location, but by **whether the service is substantially controlled by China-based or Chinese-owned entities.**

In doing so, the report offers the following key insights:

1. **The PRC's data governance model exhibits authoritarian characteristics rooted in arbitrary party-state power and a lack of institutional constraints.**

   While many studies have warned of the PRC's potential access to overseas data,[21] this report may be among the first to systematically map China's data governance framework and identify its authoritarian characteristics.

   Under its **party-state dominant model**, the government maintains an asymmetrical flow of data: it can compel Chinese companies to hand over data collected abroad, while restricting outbound transfers when the data involve national or strategic interests.

   This model is defined by sweeping national security justifications, the absence of independent judicial oversight, and broad exemptions from personal data protection obligations.

2. **Data practices of reportedly China-linked AI services may reinforce authoritarian approaches to data control.**

   DeepSeek is not the only China-linked AI service gaining global popularity. From the perspective of Taiwanese users, a linguistically proximate market, this report identifies ten widely used AI assistants and companion services that are reportedly connected to China. These services were selected based on global usage statistics, the biannual generative AI report by Andreessen Horowitz, and credible media reports and online sources. The report then examines their data practices through a close review of publicly available privacy policies.

   The analysis finds that, if the reported ties to China are accurate, these services may support the PRC's authoritarian approach to data access and control through practices such as storing overseas user data in China, sharing data within corporate groups, and complying with government "lawful" access requests. The scope of data collection is often extensive, with particularly concerning practices involving user inputs, sensitive data, and inferred personal information.

3. **To address associated risks, democracies must adopt a *DSR strategy*: *Defend* public systems, *Screen* Chinese AI services, and *Rally* allies for regulatory harmonization.**

   This report identifies the risks posed by the PRC's potential access to and exploitation of data, which span from individual privacy violations to collective challenges for democratic governance.

   To address this expanding "authoritarian gaze," the report proposes a three-part **DSR strategy: Defend, Screen and Rally**—a name deliberately chosen to counter China's Digital Silk Road (also commonly abbreviated as DSR), which represents Beijing's global push for digital infrastructure influence.[22]

(1) ***Defend*** public systems from authoritarian AI by banning Chinese AI services across government agencies and critical infrastructure.
(2) ***Screen*** Chinese AI services through inbound review mechanisms that condition market access on compliant data practices—particularly by default prohibiting the transfer of user data to China.
(3) ***Rally*** democratic allies to harmonize cross-border data regulations, building collective resilience against authoritarian data exploitation.

While the focus is primarily on Taiwan, these recommendations are equally relevant to other democratic allies. Taiwan, in particular, must urgently revise its overly permissive framework for regulating cross-border data flows and establish the proposed inbound review mechanisms with clear legal authority and enforcement capacity.

By centering on data practices, this operational-centric approach offers a more practical path for Taiwan than the ownership-centric model—such as TikTok bans—currently being promoted in the United States. The U.S. will also require new legislation to effectively address the data access risks posed by the global expansion of Chinese AI services.

To develop these arguments, this report is structured in four parts: **Part I** outlines China's global data reach and authoritarian governance model; **Part II** reviews the data practices of ten reportedly China-linked AI services; **Part III** assesses the PRC's potential data access and its risks to democracy; and **Part IV** presents policy recommendations to strengthen democratic resilience.

Part I.

China's Global Data Reach and Authoritarian Governance

China is advancing a global strategy to expand data access while embedding authoritarian governance into digital infrastructure. At the corporate level, party-state integration is institutionalized to ensure the Chinese Communist Party (CCP) retains influence over corporate decision-making and the fulfillment of state data demands.

The PRC also enforces sweeping data access laws that compel Chinese companies to hand over data—including information stored abroad—when requested by authorities. Meanwhile, Beijing imposes strict cross-border data controls that can block the re-outflow of foreign data once it enters China's jurisdiction.

These arrangements form a **party-state dominant model of data governance**, marked by:

- **Arbitrary state power**, enabled by a vague and expansive concept of "holistic national security";
- **Lack of independent judicial checks** on data access decisions;
- **Sweeping exemptions** for the party-state under the *Personal Information Protection Law (PIPL).*

This model poses systemic risks to global privacy and democratic resilience, especially where Chinese digital services gain footholds in foreign markets.

1. Background: China's "Big Data" Ambition

China has elevated data to a core factor of production and positioned large-scale data aggregation as a central pillar of its national development strategy—aiming to drive industrial upgrading, enhance governance, and boost economic returns through integrated digital infrastructure and cross-sector applications.

China's big data strategy was first introduced in 2014 through its inclusion in a national government work report, marking the start of broad state-led efforts to utilize data for both economic development and governance.[23] In the following years, the strategy expanded to focus on the growth of supportive industries and digital infrastructure, reflecting China's ambition to become a leading global data powerhouse.[24]

A major milestone came with the *13th Five-Year Plan (2016–2020)*, which launched a comprehensive national big data strategy.[25] This reflected Xi Jinping's 2017 directive at the 19th National Congress to integrate the internet, big data, and artificial intelligence into China's economy.[26]

The strategic weight of big data was followed by the *14th Five-Year Plan for Big Data Industry Development (2021–2025)*. This plan elevated data to the status of a core production distinct from traditional resources such as land, labor, and capital.[27] The plan identifies data as a key driver of economic transformation and an enabler of state governance, particularly through its "multiplier effect," whereby data enhances the efficiency and value of other production inputs to generate greater economic returns.[28]

At the core of this strategy is the concept of "fusion innovation" (融合创新), which stresses data sharing as a means to drive industrial upgrading and improve administrative efficiency.[29] Such sharing requires large-scale data aggregation. A key objective for 2021–2025 is therefore to accelerate the consolidation of high-volume datasets.[30]

To advance this goal, the Chinese government is upgrading enterprise digital infrastructure, modernizing information systems, and expanding Internet of Things (IoT) deployment to accelerate data collection across R&D, production, operations, and service delivery.[31] The accumulated data is intended not only to strengthen governance, social management, and risk mitigation, but also to serve as a foundational asset for broad application across key sectors, including consumer goods, telecommunications, finance, healthcare, agriculture, public security, transportation, energy, credit, employment, social insurance, and urban safety.[32]

2. Core Strategy: Cross-border Data Expansion Efforts

China uses the Digital Silk Road to export digital infrastructure and AI services, positioning its firms as global data gatekeepers. Because these firms are legally bound to share information with the state, their expansion creates foreign data reservoirs that enhance Beijing's surveillance capacity and geopolitical leverage.

Data is treated as a strategic asset. As Aynne Kokas notes, China's approach amounts to "data trafficking": systematically harvesting overseas consumer information through corporate platforms, often without meaningful consent.[33] Under Chinese law, companies must grant state authorities access to the data they hold, whether stored domestically or abroad.[34]

A prime example of China's global data ambitions is the Digital Silk Road.[35] Launched in 2017 as a core pillar of the Belt and Road Initiative, the Digital Silk Road exports China's digital infrastructure—from telecom networks and submarine cables to data centers and smart city systems—across Asia, Africa, Europe, and beyond.[36]

The Digital Silk Road is propelled by the global expansion of China's e-commerce and ICT firms. Alibaba, for example, has promoted itself as a global platform for small and medium-sized enterprises (SMEs).[37] Meanwhile, Huawei and ZTE have become key providers of network infrastructure essential for broadband connectivity and IoT solutions, particularly in the development of smart cities.[38] In the realm of digital platforms, Tencent's Weixin (WeChat) and ByteDance's TikTok enable communication among billions of users worldwide.[39]

The Digital Silk Road is no longer limited to hardware or communication technologies. Chinese firms now export AI capabilities, often backed by development finance. RAND's database shows dozens of AI-enabled projects in partner countries,[40] with firms like DeepSeek lowering adoption costs through open-weight reasoning models.[41]

3. Party-State Integration into Corporate Governance

Chinese technology firms are structurally tied to the CCP through legal and governance mechanisms. The Company Law mandates internal party committees, while state ownership tools like "special management shares" give the Party direct influence over corporate decisions. Embedded party branches and dual-role executives in major firms further ensure that data collected domestically or abroad remains ultimately accessible to the state.

Control over infrastructure and AI services is not politically neutral. When Chinese firms build and maintain the backbone of digital economies abroad, they shape how data is generated, stored, and transmitted. Given their legal obligations to the PRC government, this control effectively creates reservoirs of foreign data accessible for state use, amplifying both surveillance capacity and geopolitical leverage.

China’ s global data infrastructure and AI exports may ultimately feed into the party-state: Chinese firms are structurally bound to share data with the PRC government through state ownership, legal mandates, and embedded party organs.

Chinese corporations are deeply embedded in the governance structure of the party-state. State influence operates through multiple mechanisms of ownership and control. For example, the government uses "special management shares" to obtain board seats and veto rights in private media and technology companies, enabling direct intervention in business decisions.[42]

More distinctively, *Chinese Company Law* (Article 19, amended 2018) requires all firms, including private and foreign-invested enterprises, to establish internal CCP committees. These party units are empowered to participate in and sometimes oversee key aspects of corporate governance, personnel management, and strategic planning.[43]

The CCP has prioritized establishing party structures within major technology firms.[44] Huawei reportedly has over 300 internal party branches, Alibaba around 200, and Tencent nearly 90. Many leading private firms have boardrooms and executive teams that include CCP members, with some entrepreneurs, such as Alibaba’ s founder Jack Ma, publicly identified as party members.[45] In some cases, party roles take precedence. Former Huawei executive Zhou Daiqi not only held a senior managerial position but also served as party Secretary, often acting as the company’ s representative in that capacity.[46]

4. Facilitating Inflows: Access to Global Data under National Security Laws

China has built a far-reaching system of state access to data that extends well beyond its borders. Companies can be compelled to cooperate with security and intelligence authorities through multiple legal channels—including (1) data security reviews, (2) intelligence collection mandates, and (3) counter-espionage operations.
These mechanisms apply not only within China but also extraterritorially, obligating Chinese firms to hand over data held abroad if deemed relevant to national security.

The Chinese government imposes sweeping legal obligations on companies to provide data access. The *Cybersecurity Law* (CSL) and *Data Security Law* (DSL) form the backbone of this framework. While both primarily cover entities operating or processing data within China, Article 2 of the DSL explicitly extends jurisdiction to activities abroad if deemed harmful to national security or the public interest. This effectively places the overseas operations of Chinese firms under the PRC's legal authority.

Under these laws, companies must provide "technical support and assistance" to government authorities for national security and criminal investigations.[47] When security agencies request access to data in accordance with relevant state regulations, firms are "obligated to cooperate,"[48] a duty that extends to data held abroad. Noncompliance may trigger penalties under the DSL for endangering national security.

What, then, are the legal schemes that allow the Chinese government to demand access to data? At least three mechanisms stand out.

Data Security Review

The first is the "data security review" mechanism under the DSL,[49] which empowers the state to establish a review mechanism for data processing activities that affect, or could affect, national security. As part of China's broader "national security review" framework, these reviews may apply to entities including Chinese data processors[50] as well as to operators of critical information infrastructure procuring digital products or services.[51]

To conduct security reviews of data content and processing activities, authorities may request access to relevant information. Under the CSL, DSL, and related enforcement rules issued by China's internet regulators,[52] companies subject to such reviews are obligated to provide the requested data.

Intelligence Collection Mandates

The second mechanism is national intelligence collection. Under the *National Intelligence Law* (NIL), state agencies are empowered to conduct intelligence activities abroad to protect national security and interests (arts. 10 and 11).

The law obliges all Chinese organizations to "support, assist, and cooperate with national intelligence efforts" (art. 7). This means that if intelligence authorities deem data held by a Chinese company, whether inside or outside China, relevant to their work, the company must comply or face penalties (arts. 14 and 28).

Counter-Espionage Operations

The third mechanism is counter-espionage. China's *Counter-Espionage Law* (CEL) applies extraterritorially to any activity deemed harmful to national security and requires all Chinese organizations to "support and assist" counter-espionage efforts (arts. 10 and 8). Accordingly, if security authorities demand access to data for such purposes, Chinese companies are legally bound to comply[53] or risk sanctions under the DSL.[54]

Building on these regulations, the Chinese government has reinforced data access obligations specifically for AI service providers. Under the Interim Measures for the *Management of Generative Artificial Intelligence Services* (生成式人工智能服务管理暂行办法), for instance, providers must cooperate with oversight conducted under the CSL, the DSL, and related laws. This includes disclosing training data sources and providing technical and data support upon request. Importantly, these obligations can also apply to data stored outside China.

Table 1: Legal Grounds for China's Access to Overseas Data

The CSL and DSL impose general obligations on Chinese firms to cooperate with "lawful" data access requests, including those involving data held overseas

Mechanism	Legal Basis	Scope	Obligation
Data Security Review	DSL	Reviews data processing activities that affect or could affect national security	Firms must provide requested data during the review process
Intelligence Collection Mandates	NIL	All Chinese organizations must support intelligence efforts, including those conducted abroad	Firms must cooperate with data access requests from intelligence authorities
Counter-Espionage Operations	CEL	Applies extraterritorially to any activity deemed harmful to national security	Firms must provide data if requested for counter-espionage purposes

5. Restricting Outflows: China's Cross-Border Data Controls

China imposes strict cross-border data controls on two main categories: data deemed critical to national security and the personal data of individuals located in China. In both cases, the state enforces stringent localization mandates—requiring domestic storage and tightly restricting outbound transfers—justifying these measures on national security grounds and claims of regulatory jurisdiction.

Beijing has not confined itself to large-scale data inflows. To consolidate data security, which it views as a core pillar of national security, it has tightened controls on data "outflows" beyond its borders. The Hoover Institution has also described this asymmetrical flow as an "accumulation plus hoarding" strategy."[55]

Critical Data

China tightly restricts the outflow of data deemed critical to national security. Article 25 of the DSL establishes export controls over such regulated data,[56] while the CSL introduces the concept of "critical data."

Operators of Critical Information Infrastructure (CIIOs) must store critical data collected or generated in China on domestic servers.[57] Transfers abroad are prohibited unless approved through a "security assessment" conducted by cybersecurity authorities.[58]

"Critical data" refers to any information that, if tampered with, destroyed, leaked, or illegally accessed or used, could endanger national security or disrupt social and economic stability.[59] To operationalize this concept, the Chinese government has issued official catalogs specifying data types covered by this designation.[60]

The DSL further expands localization and assessment requirements beyond CIIOs, applying them to a wider range of data processors.[61] Requests from foreign courts or law enforcement for access to such data are also tightly restricted and may only be granted with explicit authorization from Chinese regulators.[62]

Personal Data

Strict outflow controls also apply to personal data in China. Under the PIPL, introduced in 2021, three categories of entities face localization and transfer restrictions: (1) state organs, (2) CIIOs, and (3) data processors handling large volumes of personal information[63]—defined as transferring data on over one million individuals or sensitive data on over 10,000 individuals abroad since January 1 of the relevant year.[64]

These entities are required to store personal data collected or generated within China on domestic servers, and any transfer overseas must undergo a security assessment. In fact, the scope of entities subject to these obligations has already been narrowed by Chinese regulators under the 2024 *Provisions on Promoting and Regulating Cross-Border Data Flow*, which aim to balance national security concerns with commercial needs.[65] The Provisions also introduced exemptions for entities operating in free trade zones and for general data processors that fall below the above specified thresholds.[66]

However, the core principle of restricting outflows of critical data and personal data **remains unchanged**, especially when national security or strategic interests are involved.[67] Meanwhile, requests from foreign courts or law enforcement agencies are similarly restricted and may proceed only with approval from Chinese authorities.[68]

Ironically, the PIPL's "protection" framework effectively allows PRC regulators to **retain the personal data of overseas individuals within China**. This is because the entities listed above are required to store personal data collected or generated in China domestically—a scope that may include data produced by overseas users accessing services hosted in China. As a result, such data may also be subject to China's data localization and cross-border transfer restrictions.

Moreover, if personal data collected overseas is combined with domestic personal information or "critical data" during processing in China, **any re-outflow of that data becomes subject to government oversight and restrictions**.[69]

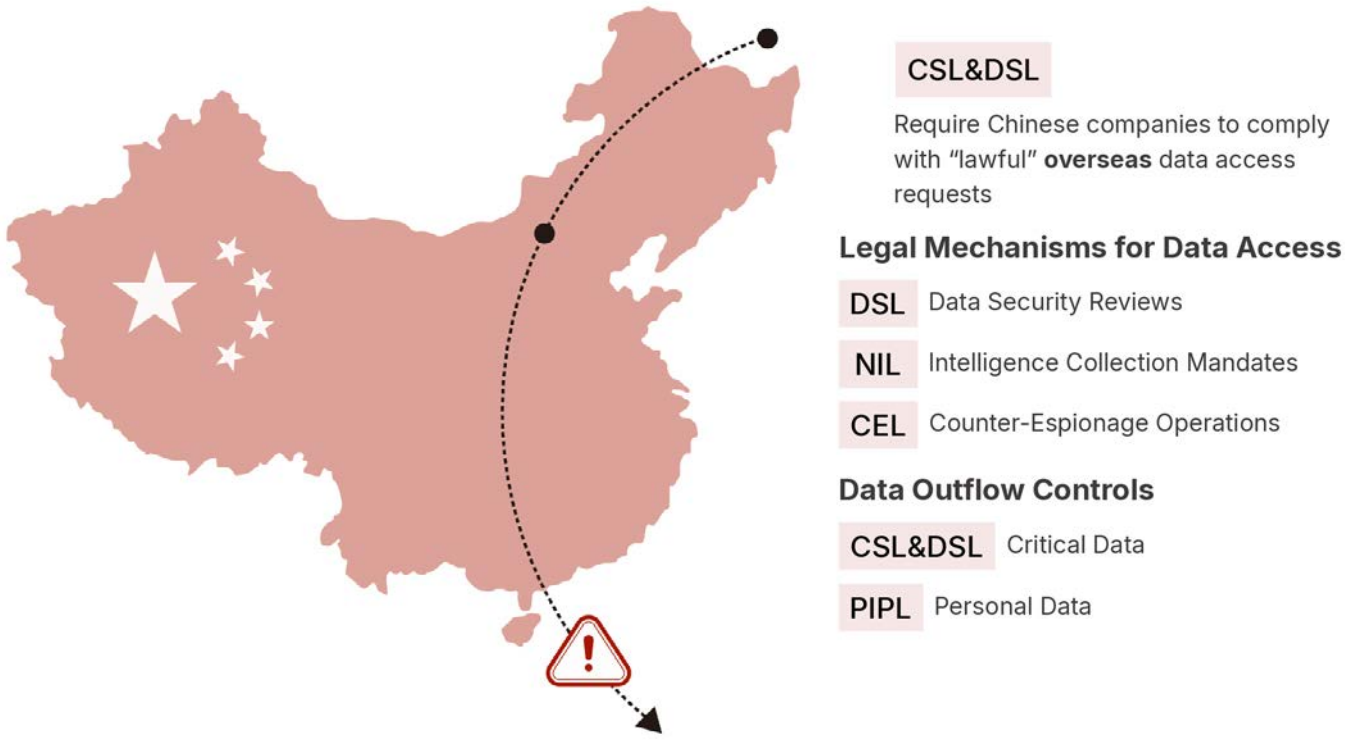
Since AI development and improvement depends on the aggregation and integration of diverse datasets, it is difficult to avoid mixing foreign-collected data with Chinese personal information or critical data. Once such data enters China, it is therefore increasingly likely to fall under government control and be treated as subject to China's claims of jurisdiction and regulatory authority over cross-border data flows.

Table 2: China's Controls on Cross-Border Data Outflows

	Critical Data	Personal Data
Legal Basis	CSL & DSL	PIPL
Scope	All data deemed "critical," collected or generated in the PRC	Personal data of individuals collected or generated in the PRC
Covered Entities	• Critical information infrastructure operators • Other data processors handling such data	• State organs • Critical information infrastructure operators • Data processors handling: (1) ≥1M individuals' data; (2) ≥ 10,000 individuals' sensitive data
Regulatory Requirements	• **Data localization**: all covered data must be stored within China • **Outbound transfer require security assessment**; restrictions also apply when personal data collected overseas is combined with domestic personal or critical data during processing in China	

As the graph below summarizes, the PRC can leverage Chinese-operated digital infrastructure and expansive legal authorities to access foreign data in service of party-state interests, while simultaneously imposing controls on outbound data flows it deems critical to national security and strategic objectives. This governance model may create an **asymmetrical dynamic: China actively pulls global data into its jurisdiction but erects walls to restrict data from flowing out.**

Figure 1: The PRC's Legal Authority to Access and Control Data



6. China's Party-State Dominant Data Governance Model

The PRC's access to and control over data held by Chinese companies embodies clear authoritarian characteristics.

- First, decisions on data access are entirely administrative, with no meaningful judicial checks.
- Second, the sweeping and ever-expanding concept of "holistic national security" grants Beijing arbitrary authority to obtain data at will.
- Third, China's personal data protection framework is riddled with exemptions, leaving the state's control over global data flows effectively unconstrained.

Lack of Independent Judicial Checks

These global data access mechanisms are especially concerning because they lack even minimal institutional checks:

- Regarding **security reviews**, Article 24 of the DSL designates decisions from the national security review process as final, barring administrative reconsideration or judicial appeal.
- Regarding **intelligence collection mandates**, Article 14 of the NIL likewise imposes no substantive limits on intelligence agencies' requests.
- Regarding **counter-espionage operations**, under Article 26 of the CEL, such access requires only approval from the head of a national security agency at the districted city level or above, a process entirely devoid of independent judicial oversight.

Even countries often criticised for expansive intelligence practices, such as the U.S., maintain far stronger legal safeguards than China. Under the *Foreign Intelligence Surveillance Act* (FISA), surveillance requests must be approved by the Foreign Intelligence Surveillance Court (FISC), which requires the government to show "probable cause" that the target is a "foreign power" or its "agent."[70] FISC decisions may be appealed to the

Foreign Intelligence Surveillance Court of Review (FISCR), and ultimately, by the U.S. Supreme Court.[71]

In addition, the *Electronic Communications Privacy Act* (ECPA) and the *Stored Communications Act* (SCA) require law enforcement to obtain a judicial warrant before compelling disclosure of electronic communications.[72] *The Clarifying Lawful Overseas Use of Data (CLOUD) Act* extends this requirement to data stored abroad, but only through the same judicial process.[73]

Together, these laws, at least in regulatory terms, ensure that U.S. government access to data is subject to independent judicial oversight and procedural safeguards. While not without flaws, the U.S. legal framework still provides meaningful institutional checks—protections conspicuously absent from China's administrative, party-led model of data access.

National Security as a Hollow Requirement

Even more troubling is China's expansive definition of national security, which places virtually any type of data within the PRC's reach. China's *National Security Law* explicitly states that national security work is led by the CCP.[74] Since Xi Jinping introduced the concept of "holistic national security" (总体国家安全观) in 2014,[75] it has been institutionalized as the cornerstone of China's security architecture.[76]

This framework treats national security as an integrated whole, spanning politics, the military, territorial integrity, the economy, finance, culture, society, science and technology, cyberspace, food, ecology, resources, nuclear issues, overseas interests, outer space, the deep sea, polar regions, biosafety—and, crucially for this report, cybersecurity, artificial intelligence, and data security.[77]

In essence, almost every sphere of human activity is treated as a potential national security concern. China's approach is not merely defensive but emphasizes proactive prevention and the cultivation of capabilities to sustain a "secure" environment.[78] At its core, the objective is to protect the

regime, sovereignty, national unity, and territorial integrity—explicitly encompassing the prevention of permanent loss of Taiwan.[79]

Against this backdrop—marked by the absence of judicial checks and an ever-expanding notion of national security—the CCP can invoke security to justify virtually any action. In this sense, almost any data held by a Chinese company can be deemed relevant. Once a Chinese firm collects user data through digital services such as AI services abroad, that information falls under the legal authority of the Chinese government. The PRC may access it "in accordance with the law" at any time.

The Limits of PIPL

China's PIPL was designed to enhance consumer data protection. Yet it does little to limit the PRC's ability to access data globally—for two main reasons:

- First, the law's protections apply only to (1) personal data processing activities taking place within China, and (2) activities conducted outside of China that involve the personal data of individuals located in China and meet certain legal conditions.[80] In other words, individuals located overseas whose data is collected and processed outside of China are not covered by the law.

- Second, even when the PIPL does apply, it exempts national security authorities when handling personal information "to fulfill their legal duties."[81] These authorities are also not required to notify individuals if doing so would "impede the performance of their duties."[82]

As a result, the Chinese government retains sweeping authority to access data under the banner of national security, despite the PIPL. The law offers little meaningful constraint on China's global data absorption practices.

7. Summary: Data Governance with Authoritarian Characteristics

Since Freedom House's influential 2018 report, China has been regarded as the leading example of "digital authoritarianism."[83] As defined by Alina Polyakova and Chris Meserole, this concept refers to: (1) the use of information technology, (2) by authoritarian regimes, (3) to surveil, repress, and manipulate both domestic and foreign populations, (4) in order to reshape the power balance between democracies and autocracies.[84]

The previous sections have shown that Chinese digital infrastructure has significantly enhanced the PRC's ability to access and control data on a global scale. In turn, **China's data governance regime reflects core authoritarian features—arbitrary state power and the absence of institutional constraints.**

Authoritarianism is a form of government in which power is **unconstrained by law, institutional checks are absent, and fundamental rights lack protection**:[85]

- As discussed above, China's expansive and ambiguous "holistic national security" framework enables the CCP to access data arbitrarily, on virtually any grounds.

- There is also no independent judicial oversight: security reviews, intelligence collection, and counter-espionage operations all bypass the courts and rely solely on internal administrative approvals.

- While the PIPL provides consumer data protections against intrusive actors like big tech firms, it explicitly exempts the party-state from constraints that could weaken its surveillance and political control.[86]

Together, these features reinforce a party-state dominant model of data governance. Enabled by expansive global data access and unchecked exploitation, **the PRC can project its authoritarian influence beyond its borders**—placing foreign populations under surveillance and enabling both repression and manipulation.[87] This poses profound risks to privacy and democratic integrity worldwide.

Even more troubling, the more Chinese digital services deployed overseas comply with PRC regulations and collect diverse, intrusive forms of user data, the more severe the governance challenges become for democratic societies. The next part turns to these concerns.

Figure 2: Authoritarian Logic Behind China's Data Access Regime

Lack of Judicial Oversight	Sweeping "National Security" Scope	Illusory Privacy Protections
• No court approval required under DSL,NIL, or CEL. • National security decisions are final and unappealable.	• Covers nearly all domains—politics, economy, tech, AI, and data. • Justifies access to virtually any data.	• Overseas individuals whose data is processed outside China are not covered. • Exempts national security agencies from data protection obligations.

Part II.

Data Practices of Chinese AI Services: A Privacy Policy Review

The risks of China's authoritarian governance model are further compounded by the compliant data practices of Chinese digital service providers. To justify these practices through **user consent**, providers outline in their privacy policies how they collect, use, transfer, store, and share data.

Building upon a compilation of relevant media reports and materials, this analysis—if the information contained therein proves accurate—finds that the privacy policies of the ten most widely used China-linked generative AI services indicate the following:

- Some services explicitly state that they **store user data in China**.
- In other cases, even when services are operated by entities incorporated abroad, their corporate structures**, intra-group data transfers, and obligations under Chinese law** may create pathways for globally collected personal data to be transferred into, or accessed from, the PRC.
- Among the 11 data types identified in this report, most of the examined services collect between **8 and 11 types**, with an average of nearly **9 per service**. Particularly concerning are practices involving the collection of **user inputs, sensitive data, and inferred personal information**.

Importantly, these findings suggest that **even services registered outside the PRC—possibly in an effort to "de-China"—do not necessarily eliminate the pathways through which overseas user data may flow back to China.**

This analysis is based on the versions of privacy policies accessible to **users in Taiwan using Mandarin-language settings** and reflects the most up-to-date versions available as of **November 15, 2025**. Links to the archived full texts of these policies are provided in the Appendix, along with summary tables outlining data storage locations, data sharing and government disclosure practices, and the categories of data collected from each policy.

Chinese AI Services in Global Usage Rankings

The "Chinese" AI services examined in the report are selected from the Top 100 GenAI Consumer Apps report,[88] published biannually by Andreessen Horowitz. Since 2023, the report has ranked the 50 most-visited AI-first web products (based on unique monthly visits via Similarweb) and the 50 most-used AI-first mobile applications (based on monthly active users via Sensor Tower). Across the past two editions, ten globally popular China-linked LLM assistant and companion services have stood out.

1. **DeepSeek.** Despite experiencing a drop-off in the past six months, it remains the most prominent example of global adoption of Chinese AI, ranking #3 among web products—behind only ChatGPT and Gemini—and #8 among mobile applications.

2. **Doubao**, ByteDance's AI chatbot, surpassed 80 million monthly active users (MAUs) as of February 2025.[89] It now ranks #12 among AI-first web products and has overtaken DeepSeek to become #4 among mobile applications.

3. **Cici**, the overseas version of Doubao, has been gaining traction in countries like the UK, Mexico, and Indonesia[90]—rising from #41 in March 2025 to #14 in August among AI-first mobile applications.

4. **Kimi**, developed by the Chinese startup Moonshot AI, ranked #17 among mobile applications. Its supporting LLM was praised by Nature as another top-performing Chinese model, following the release of DeepSeek R-1.[91]

5. **Qwen Chat**, an AI assistant developed by Alibaba's LLM,[92] jumped to #20 on the web products list in the latest edition.

6. **Quark**, developed by Alibaba, is another leading AI assistant. As of April 2025, it reportedly reached around 150 million MAUs,[93] ranking just behind DeepSeek at #9 among AI-first web products and #47 on the mobile applications list. News reports also indicate that Quark once topped the download charts in Taiwan, with its MAUs in the country rising 53% year-over-year.[94]

7. **Baidu AI Search** ranked as the 7th most widely used mobile application—surpassing DeepSeek and trailing only Doubao.

8. **Manus** is a newly emerged general-purpose AI agent with global reach, appearing for the first time on the web products list at #31. Beyond the reasoning and planning capabilities of a LLM, it can also carry out complex tasks from start to finish—marking a shift toward more integrated and action-oriented human-AI collaboration.

9. **Talkie** has been one of the most popular AI companion apps in the U.S.[95] Previously ranked #39 among web products and #11 among mobile applications, it now remains on Andreessen Horowitz's "Brink List," holding the #51 spot on the mobile applications list.

10. **Monica** is an all-in-one assistant powered by multiple models, consistently featured in the web products rankings over the past two editions.

While Andreessen Horowitz notes that Quark, Doubao, and Kimi primarily serve users in China, they remain accessible in Taiwan, and some have gained notable popularity among Taiwanese users. As such, analyzing their data practices remains essential to the purpose of this report. Most of the other Chinese AI services have been "exported" globally, with the vast majority of their usage occurring outside of China.

An important update: On December 30, 2025, Meta announced that it would acquire Manus and was reported as stating that Manus would sever ties with Chinese investors and cease operations in China following the acquisition.[96] Since the aim of this report is to examine how AI services with operational links to China structure their data practices and how those practices may align with or be influenced by China's authoritarian data-governance model, our analysis of Manus (and Monica), as they operated on or before November 15, 2025, remains relevant.

Indeed, Meta's reported commitment to eliminate all ongoing ties with China post-acquisition reinforces the core concerns raised by this report. For that reason, the following analysis is retained in full as a pre-acquisition baseline of Manus's data practices.

Corporate Disclosures and Media-Reported China Ties

Some of these AI services explicitly state in their privacy policies that they are operated by Chinese companies. For example:

- **DeepSeek's** privacy policy states that its services are "provided and controlled" by a China-registered entity, Hangzhou DeepSeek Artificial Intelligence Co., Ltd.[97]
- **Kimi's** privacy policy notes that its service provider is Beijing Moonshot Technology Co., Ltd (北京月之暗面科技有限公司).[98]
- **Baidu AI Search** states in its privacy policy that its services are provided by Beijing Baidu Netcom Science & Technology Co., Ltd (北京百度网讯科技有限公司).[99]
- **Doubao's** privacy policy states that the service is provided by Beijing Chuntian Zhiyun Technology Co., Ltd. (北京春田知韵科技有限公司),[100] which, according to Chinese media sources, is a wholly owned subsidiary of Beijing Douyin Information Service Co., Ltd. (北京抖音信息服务有限公司).[101]

- **Quark's** privacy policy explicitly states that its service provider is Guangzhou Dongyue Information Technology Co., Ltd. (广州市动悦信息技术有限公司), a company registered in Guangzhou, China.[102]

For the remaining five services—**Cici, Monica, Manus, Qwen, and Talkie**—their privacy policies list Singapore-registered companies as service providers. However, as shown below, multiple media and online sources have reported that these services appear to maintain operational or developmental ties with affiliated corporate group entities that are China-based or Chinese-owned.

For example, Andreessen Horowitz notes that Cici is a product produced by ByteDance, while both Manus and Monica are developed in China.[103] In its analysis of the Andreessen Horowitz rankings, Chinese tech media outlet 36Kr similarly reports that Cici is a ByteDance product,[104] Monica and Manus were created by the same China-based team, and Qwen is a product of Alibaba.[105]

- Regarding **Cici**, Forbes reported in 2024 that the AI chatbot was launched by ByteDance for users outside of China, and that its overseas provider, Spring (SG) Pte. Ltd., is a ByteDance subsidiary.[106] The report also cited a ByteDance spokesperson confirming that user data from Cici may be accessed by ByteDance employees in China, "subject to the company's access controls and approval processes."[107]

- For **Talkie**, The Wall Street Journal reported in 2024 that its ultimate parent is MiniMax, a Shanghai-based AI unicorn often referred to as one of China's "Four Little AI Dragons."[108] Backed by major Chinese tech firms such as Alibaba and Tencent, MiniMax was valued at over $2.5 billion in its most recent funding round in March 2024.[109]

- **Qwen Chat** is reportedly operated by Alibaba Cloud,[110] and its underlying model, Qwen, is an open-weight LLM developed by the Hangzhou-based Alibaba Group.[111] CNBC has reported that Alibaba's cloud business expanded into Singapore in 2015, establishing it as one of the company's key overseas centers.[112] In 2023, Alibaba Group attempted to spin off its cloud unit with an independent CEO and board, but ultimately scrapped the plan due to rising geopolitical uncertainties.[113]

- **Monica**, according to the Taipei Times, has gained visible traction in Taiwan through extensive local advertising, but the app was developed by a Chinese parent company.[114] Public records further show that Monica was registered and launched in Beijing in accordance with China's *Interim Measures for the Management of Generative Artificial Intelligence Services*,[115] underscoring its origin from a China-based developer.

- Since its launch, **Manus** has often been described as a "Chinese AI agent" developed by a China-based team.[116] Tech in Asia reported that Manus's parent company was linked to Beijing Red Butterfly Technology Co., Ltd., a firm founded in 2023.[117] In April 2025, Manus received a $75 million investment from the U.S.-based venture capital firm Benchmark, a deal that soon drew scrutiny under the U.S. Treasury Department's Outbound Investment Security Program (OISP)—which restricts certain investments by U.S. persons in sensitive Chinese technologies, including AI.[118]

  By mid-July, Manus had relocated its global headquarters to Singapore, transferring around 40 core technical personnel and laying off most of its China-based staff.[119] Its three co-founders also moved abroad.[120] However, Lianhe Zaobao (联合早报), a Singaporean news outlet, reported that Manus AI's parent company still maintains its headquarters in China.[121]

While these actions appear aimed at complying with U.S. investment restrictions, observers note that it remains unclear whether such restructuring is sufficient to classify Manus as a "non-Chinese company."[122] In similar cases, such as TikTok, U.S. regulators have continued to treat firms as Chinese, even after they formally moved their headquarters overseas.[123]

8. Data Storage Practices

According to their privacy policies, DeepSeek, Kimi, Doubao, Quark, and Baidu store user data within the PRC. Qwen's policy indicates that China is among the locations where user data may be processed. As such, overseas user data may be stored in China, subject to government access and cross-border transfer restrictions.

Cici, Talkie, and Monica state that user data may be stored and processed in jurisdictions such as the U.S. and Singapore. Manus notes that user data may be transferred to the U.S. or "other locations," but does not specify whether China is among them.

Data Stored in China

Several of the examined services indicate that user data is stored on servers located within the PRC. **DeepSeek, Kimi, Doubao, Quark, and Baidu AI Search** all appear to fall into this category. **Qwen's** policy likewise suggests that China is among the locations where user data may be processed and possibly stored.

For instance, DeepSeek's privacy policy explicitly states: "To provide you with our services, we directly collect, process, and store your Personal Data in the People's Republic of China."[124]

Meanwhile, services such as Doubao, Quark, and Baidu specify that personal data collected or generated within China is stored domestically.[125] No additional storage locations are specified. Given that these services remain accessible to users in Taiwan and are operated by entities registered in China, data entered by these overseas users may still be transmitted to servers in China for processing. As such, this data could similarly be classified as "collected or generated within China" and stored accordingly.

These data storage practices are possibly shaped by China's data laws. The PIPL requires that personal data collected or generated within China be stored domestically. Since all but Qwen Chat are operated by China-based entities, data they handle—including overseas user input—could be legally classified as "collected or generated within China" and thus subject to localization requirements. These legal obligations are ultimately reflected in the language of their privacy policies.

On the other hand, Qwen's privacy policy indicates that its designated service providers may be located in Singapore, Indonesia, and/or China, and that user data may be processed in one or more of these countries.[126] This suggests that its user data could also be stored or processed in China.

Once stored in China, personal data falls directly under the authority of Chinese laws and regulators, subject to arbitrary access by the party-state on sweeping national security grounds and without independent judicial oversight. Moreover, overseas user data becomes subject to China's strict cross-border transfer restrictions, effectively placing it under Beijing's asserted data sovereignty[127] and turning it into a strategic asset for further authoritarian use.

Data Stored Outside China

By contrast, services such as **Cici, Talkie, Monica, and Manus** indicate that user data may be stored and processed in jurisdictions including the U.S. and Singapore. Cici specifies that its servers are located in both the U.S. and Singapore,[128] while Talkie and Monica note that their services are operated from or store data in the U.S.[129]

Manus presents a more complex case. Although its privacy policy emphasizes that the company is headquartered in Singapore, it also states that it may use service providers operating "in other countries," and that user data may be transferred to the U.S. or "other locations where privacy laws may not be as protective as those in your state, province, or country."[130] However, it does not specify which "other locations" are included or whether China is among them.

9. Data Sharing Practices

Except for Talkie, nine of the examined services state in their privacy policies that user data may be shared within their corporate groups. If reported ties to China are accurate, this means data stored overseas could still be shared with China-based entities.

All of the examined services also state that user data may be disclosed to government authorities to comply with legal obligations. For China-based services, this subjects data directly to Chinese laws that grant broad government access.

For non-China-based services with reported ties to Chinese corporate groups, cross-border sharing may trigger compliance conflicts. Chinese law can compel access to overseas data while host jurisdictions may lack strong safeguards against such transfers.

Intra-Group Data Sharing

Even when data is stored abroad, intra-group sharing may still create pathways for user information to flow back to China. With the exception of Talkie, **nine of the examined services** state in their privacy policies that user data may be shared with entities within their corporate groups—such as parent companies, subsidiaries, or affiliates.

As noted earlier, media investigations have suggested potential ties between these services and China-based or Chinese-owned corporate groups. If accurate, this suggests that data originally stored overseas could nonetheless be shared with entities located in China.

The following are examples of services that store data outside China but permit intra-group sharing:

- **Monica's** privacy policy states that the company "may be required to provide information about [users] to [its] parent or subsidiary company or corporate affiliates."[131]
- **Cici's** policy notes intra-group data sharing, stating that the service is "supported by certain entities within our corporate group."[132]
- **Qwen's** indicates that personal data may be disclosed to "affiliated companies in the Alibaba Group and/or their designated service providers."[133]
- **Manus'** states that personal information may be shared with its "corporate parent, subsidiaries, and affiliates."[134]

Again, once data is shared with affiliated entities based in China, it becomes directly subject to the PRC's authoritarian access and control under its national security regime.

Government Access to Overseas Data

All of the examined services state in their privacy policies that user data may be disclosed to law enforcement agencies or other public authorities when deemed necessary to fulfill legal obligations under applicable laws, legal processes, or government requests. In many cases, this includes responding to matters related to national security, criminal investigations, judicial proceedings, or administrative enforcement.

While including "government access" clauses is common practice in privacy policies, such provisions carry additional weight for services with operational ties to China. As noted earlier, some examined services are operated by China-based entities and store user data within the PRC. In these cases, the "applicable laws" referenced in their privacy policies are likely to be Chinese laws. Given that refusing a government request on security grounds can itself constitute a legal violation, China's sweeping and unchecked national security regime effectively grants authorities broad access to corporate-held data.

For services operated by non-China-based entities that claim to store data overseas, reported ties to Chinese corporate groups may raise cross-jurisdictional **compliance dilemmas.** Under Chinese law, particularly the DSL, Chinese firms are obligated to provide access to data held abroad if deemed relevant to national security. However, their overseas affiliates are simultaneously subject to local data protection laws.

For example, Cici's privacy policy states that data transfers will be conducted "in accordance with the requirements of applicable data protection laws," which may include U.S. and Singaporean laws due to data storage in those regions.[135]

In such cases, the strength of cross-border transfer restrictions in host jurisdictions becomes critical. But some jurisdictions, notably the U.S., have been criticized for having weak and fragmented frameworks that fail to prevent China's cross-border "data trafficking."[136]

Table 3: Data Storage and Sharing of Reportedly China-Linked AI Services
Source: Privacy policies of the listed providers (data collected November 15, 2025)

Services	Data Storage Locations	Intra-Group Sharing	Government Access
deepseek	China	YES	YES
Kimi	China	YES	YES
豆包	China	YES	YES
Quark	China	YES	YES
du	China	YES	YES
Monica	US	YES	YES
Cici	US,SG	YES	YES
talkie	US	Not specified	YES
Qwen	China,SG,Indonesia	YES	YES
manus	US or others	YES	YES

10. Data Collection and Usage

Of the eleven data types identified in this report, most services collect between 8 and 11, with an average of nearly 9 per service.

All ten services collect user-provided data, including personal identifiers and user inputs—raising concerns about oversharing and sensitive self-disclosure.

All ten services collect device and network information, as well as service usage data, while seven also gather location data—reflecting widespread practices of tracking user devices, behaviors, and geographic information.

Several services collect sensitive biometric-adjacent data, such as voiceprints, facial images, and health-related information. Six services collect inferred information, enabling the construction of detailed personal profiles.

As a recent study shows, Chinese apps are not only popular globally but, more importantly, rank among the most "data-hungry" in terms of data types they collect and share.[137] This appetite for data is especially strong in the context of AI services, as AI development depends heavily on data—driving providers to continually collect user information to enhance performance and refine their models and algorithms.[138]

This section provides a high-level overview of the key data types collected by Chinese AI services, based on a detailed review of their privacy policies. The data is grouped into three overarching categories: (1) data provided by users, (2) data automatically collected, and (3) data obtained from third parties. Within these categories, eleven distinct data types were identified.

Table 4: Data Types Collected by Reportedly China-Linked AI Services

Data Types	Definitions and Scope
User-Provided Data	
1. Personal Identifiers& Profile Information	Data that can be used to identify a specific individual, usually provided by users when setting up or managing an account. This includes basic account details (e.g., email address, phone number, and username) and profile information (e.g., nickname, bio, and date of birth).
2. User Input	Content actively provided by users, including text prompts, chat histories, uploaded files (e.g., images, audio, video, documents), and user feedback. This category may also include users' marketing preferences and communication records with the company.
Automatically Collected Data	
3. Device & Network Information	This category includes details such as device model, operating system, IP address, unique device identifiers, browser type, and system language.

4. Service Usage Data	Information on how users interact with the service, including duration, frequency, settings, features used, actions taken, access times, and types of content viewed or engaged with.
5. Location Data	Information about a user's location, which may be determined approximately via IP address or SIM card, or more precisely through GPS.
6. Cookies	Widely used tracking technologies that help operate and provide services, including for purposes such as security, personalization, and usage analysis.
7. Payment & Subscription Details	Information such as transaction date and time, currency, and transaction amount.
8. Inferred Information	Data derived from analyzing user content and other signals to predict attributes such as age, gender, occupation, and interests (e.g., hobbies or preferred topics).

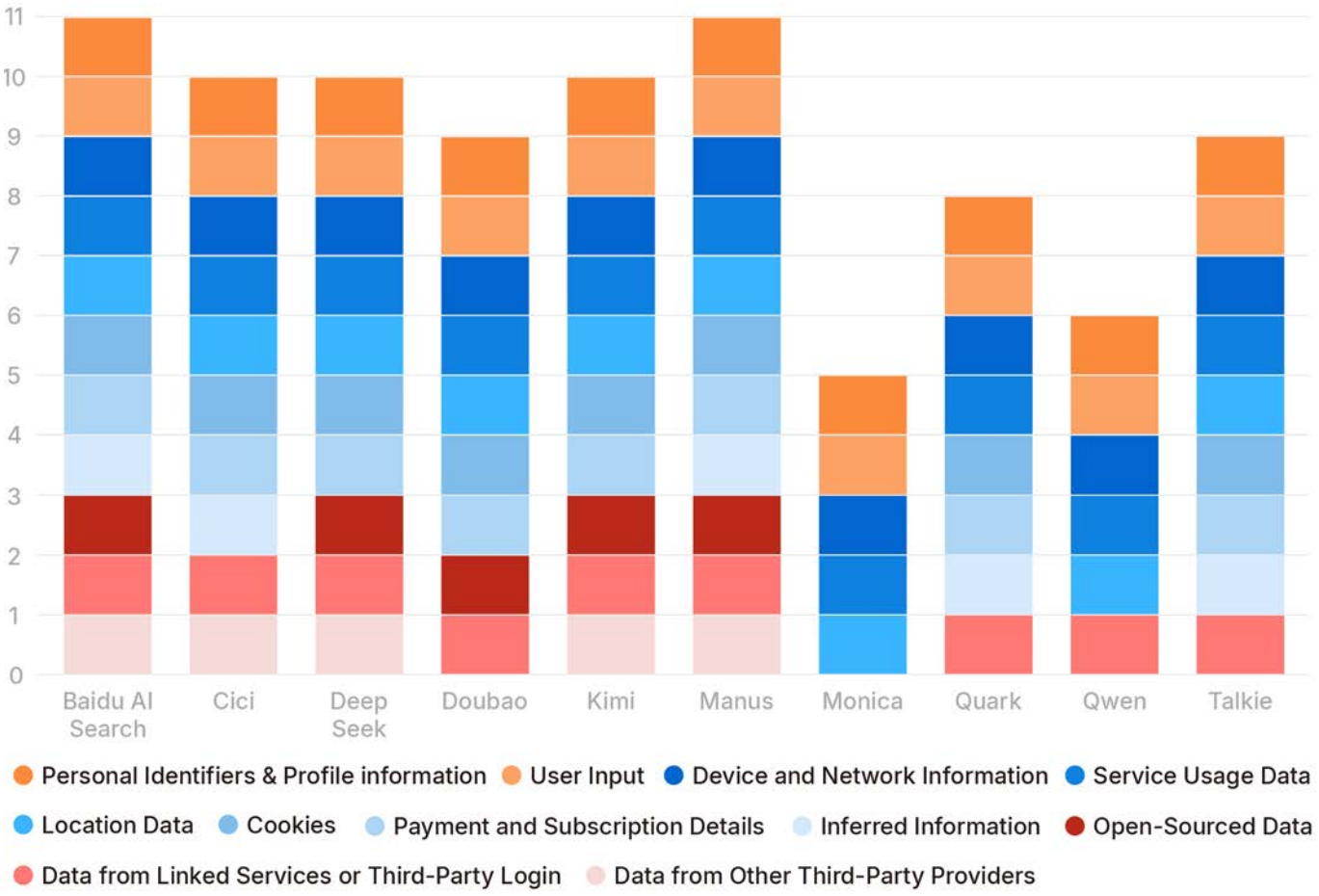
Third-Party Sources	
9. Open-Sourced Data	Information drawn from publicly available sources.
10. Data from Linked Services or Third-Party Login	Information collected when users log in or sign up through external accounts (e.g., Google or Apple), or link their account to a third-party service, including data associated with those services.
11. Data from Other Third-Party Providers	Information about users' activities on other websites and apps, user personal data,or processed user data shared by advertisers, analytics providers, security partners, and other third-party partners.

For this analysis, the report focuses on the general provisions of each privacy policy—excluding clauses that apply only to specific jurisdictions, such as the EU or California. It records only those data types that are **explicitly identified** as being collected in the policies. For example, Cici is noted as collecting inferred information because its privacy policy explicitly references the collection of "inferred data."[139]

By contrast, Monica's policy includes language such as: "We may use your information to develop and display content and advertising tailored to your interests and/or location and to measure its effectiveness," and "We may use your information for other purposes, such as data analysis, identifying usage trends…"[140] Although such statements could suggest the use of inferred data, the absence of an explicit mention means this data type is not recorded for Monica in this report.

If the examined services follow their stated policies, **most collect between 8 and 11 of these data types, with an average of nearly 9 per service.** Baidu AI Search and Manus collect all 11 types, while Monica collects only 5. This reflects a generally consistent but still varied approach to data collection, with some services adopting more expansive practices than others.

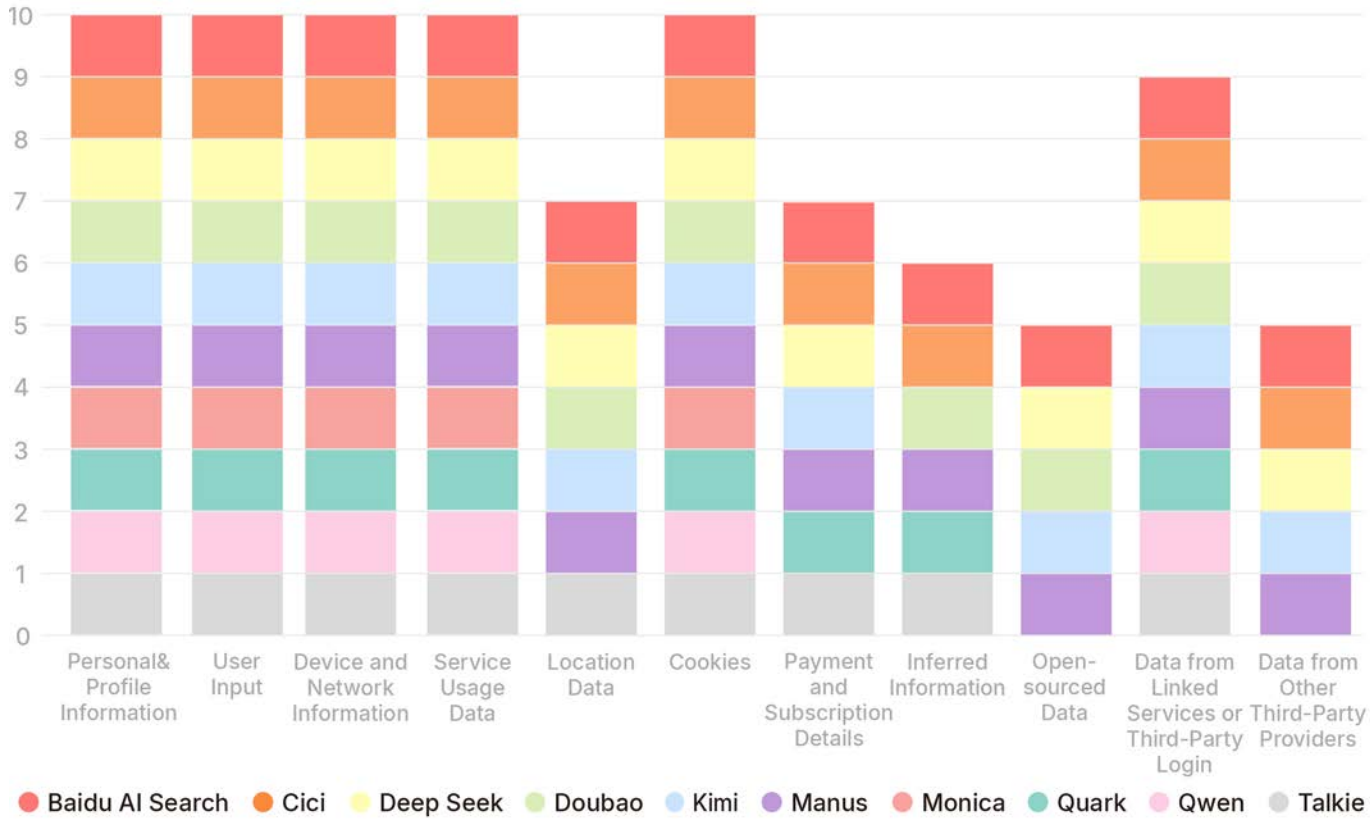
Figure 3: Data Types Collected by Chinese AI Services Providers
Source: Official websites of the listed providers (Data collected November 15, 2025)
Visualization: Violet (Yueh-Ning) Chiang



These services collect a wide range of user data, including inputs such as prompts, uploaded files, and chat histories. Some also gather sensitive information, such as biometric identifiers and health records, and generate inferred data from user interactions to build detailed personal profiles. While many of these practices resemble those of other digital platforms, their integration with intimate chatbot interactions significantly heightens the associated privacy risks.

Figure 4: Chinese AI Services' Data Collection by Type

Source: Official websites of the listed providers(Data collected November 15, 2025)
Visualization: Violet (Yueh-Ning) Chiang



User-Provided Data

Broadly speaking, **all of the** examined **AI services** collect user-provided data, including personal identifiers and various types of user inputs.

For example, services such as **Manus** even capture "associated metadata" linked to user-generated content, including details on how, when, and where content was created or edited, as well as keywords and location information.[141]

Interaction with multi-functional AI assistants raises particular concerns about **sensitive self-disclosure**. Chatbots encourage **oversharing** by offering perceived anonymity and their non-judgmental responses.[142] Since the release of ChatGPT-3 in late 2022, the most cited privacy risk has been users' tendency to reveal excessive personal information.[143] Confidential or intimate data entered into these systems may be retained for model retraining or improvement and, in some cases, could even surface inadvertently in outputs to other users.[144]

Automatically Collected Data

All ten services collect device and network information, as well as service usage data, while **seven** also collect location data. This indicates a widespread practice of tracking user devices, behaviors, and geographic information across the examined AI services.

Kimi, for example, collects both approximate and precise location data. It automatically gathers general location information to provide location-based services.[145] Its privacy policy also states that precise location data (精确位置信息) may be collected "to better use some functions," such as "nearby" searches and route planning.[146] Given the breadth of this language, actual compliance will depend on how strictly the service applies the legality and necessity principles outlined in its policy.[147]

Other data categories extend into **everyday browsing and profiling.** For instance, **Cici's** browser plugin may collect users' browsing history.[148] **Quark** logs webpage browsing and search histories, and automatically collects service log information that includes click/view events and access

dates and times.[149] **Manus** may automatically log online activity data, including pages or screens viewed, time spent on each page, navigation paths, on-page interactions, and engagement with emails from Manus such as opens and link clicks.[150]

The accumulation of device information, service usage data, and location data and other types of automatically collected data raises several concerns.

- First, it might enable detailed tracking and behavioral profiling of users and their movements.
- Second, re-identification remains a persistent risk. Service logs and technical details can be cross-referenced with prompts or usage patterns to link sensitive content back to individuals.
- Third, secondary uses and data sharing amplify these risks,as cookies and similar tools facilitate cross-platform tracking and expose user data to third-party advertisers or analytics firms. These practices, while common in digital services, become significantly more problematic in the context of generative AI assistants, which handle intimate user inputs.

Sensitive and Inferred Data

A particular concern is the handling of highly **sensitive data**. Several services process biometric or biometric-adjacent information. For example:

- **Kimi** explicitly collects voiceprint data to deliver personalized voice replies, though it allows users to delete this data afterward.[151]

- **Doubao** processes facial images for its avatar and image generation functions, such as its AI Portrait (AI 写真) feature.[152] Notably, it also offers a health consultation service that asks users to provide medical history, allergy information, and test results to generate summarized responses.[153]

- **Manus** states that it may derive biometric-like data from user-provided images, videos, and audio or voice clips to enable features such as avatar creation and video conversions.[154]

Six services incorporate **inference-based data collection and processing**. These practices directly support the creation of detailed user profiles, demonstrating how seemingly routine inputs can be transformed into intimate portraits of individuals. For example:

- **Cici** states that it may infer users' attributes (e.g., age, gender, job) and their interests, based on user inputs and other collected data.[155]

- **Manus** notes that its integrated third-party AI providers may infer information about users and share it back with Manus.[156]

- **Doubao** analyzes user conversations to extract "memories" and deliver personalized responses based on past interactions. When the personalized recommendation and memory features are enabled, which users can opt out of, the service processes input data (e.g., chat content, search queries, and behavioral signals) to tailor replies and recommendations.[157]

- **Baidu AI's** policy states that users' personal information may be aggregated and analyzed to generate "tagged information" (标签信息) reflecting traits such as behavioral habits, interests, and even credit status.[158] These tags are then used to make automated decisions for delivering personalized content and commercial marketing.

Part III.

The PRC’s Potential Data Access and Risks to Democracy

China's global data reach poses risks that span from individual privacy to collective democratic governance.

- Through broad consent mechanisms, users effectively grant reportedly China-linked AI services a "blank check" for extensive data collection, storage in China, and intra-corporate data sharing—rendering self-control largely illusory.

- Pervasive data harvesting and the inference of sensitive traits enable the construction of detailed personal profiles, making individuals increasingly transparent, fixed, and predictable.

- Such intrusive profiling, especially when combined with other globally sourced data to improve AI models, could significantly enhance China's intelligence-gathering capabilities.

- At a population level, aggregated user data allows the PRC to construct a comprehensive "societal mosaic" of democratic communities, exposing key vulnerabilities and fault lines.

- When fed into AI models, these insights can enable more precisely targeted, harder to detect, and cognitively disruptive influence operations aimed at democratic societies.

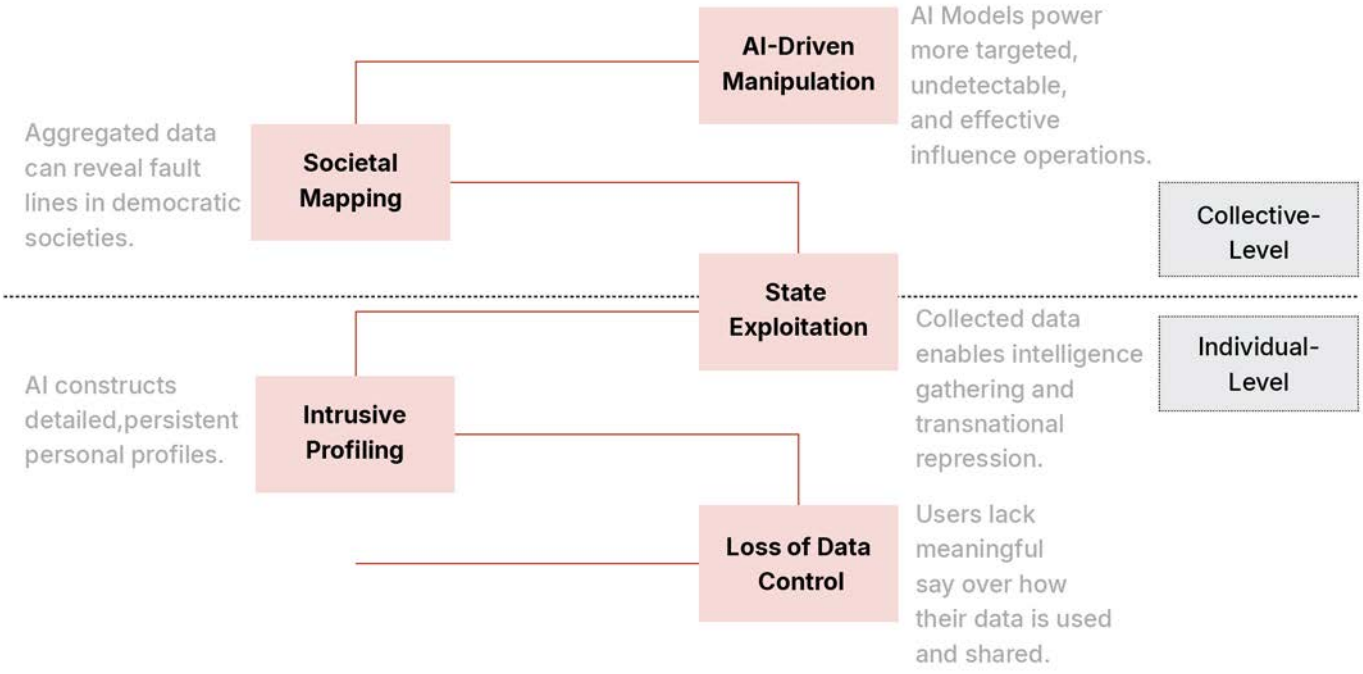
As the previous Part shows, Chinese AI services collect various types of data from global users, leading to the concentration of vast amounts of information in the hands of a few dominant companies. If these firms are compelled to serve state interests, as is often the case with major Chinese tech companies, data collection is no longer a purely commercial activity but becomes a strategic national asset.

The authoritarian access and use of overseas data could pose fundamental risks to democratic societies. As the following sections will analyze, individual consent is wholly inadequate to prevent data collected by Chinese AI services from flowing back to China. Given the party-state's ability to access such data, Beijing can aggregate and analyze vast information sets—constructing highly detailed profiles of targeted individuals and supporting broader intelligence operations.

This "**authoritarian gaze**" not only pierces the "obscurity" that underpins personal privacy[159] but also enables the construction of a "societal mosaic"—mapping the vulnerabilities and fault lines within democratic communities that can be exploited for more effective manipulation and influence campaigns.

As a result, the PRC's potential data exploitation threatens autonomy at both the individual and collective level, posing a profound challenge to democratic governance.

Figure 5: Risks of China's Global Data Reach: Individual to Societal



11. The Fiction of Consent and Self-Control

The data practices of these AI services could erode users' control over personal information, which is long considered a core principle of privacy. The loss of control itself is a privacy harm, as it limits individuals' ability to manage future risks.[160] Consent-based collection has long been the primary safeguard of personal control.[161] Yet, as Daniel Solove notes, consent has increasingly become a "blank check."[162] Companies routinely update privacy notices to grant themselves broad rights to collect and use personal data for developing AI.

Through their privacy policies, the examined service providers obtain broad user consent for a range of data practices—including data collection, storage locations, and intra-corporate group sharing. If reported ties to China are accurate, this effectively means overseas users are consenting to their data being transferred back to China and subjected to the PRC's expansive data access.

It is also common for users to consent, often through broadly worded terms, to the use of their data for service improvement or AI model optimization. Yet since the specific uses are rarely clear at the time consent is given, such consent can function as a "free pass" for virtually any purpose.[163] In practice, it becomes a legal fiction that undermines the very notion of self-control over personal data.

12. Pervasive Data Collection and Profiling

Many of the services examined engage in extensive data collection. Beyond standard content such as chat histories and uploaded files, some also collect biometric identifiers and detailed records of users' daily interactions. Kimi records voiceprints. Doubao gathers facial images and health-related information. Cici tracks browsing histories, while Manus logs pages or screens viewed, time spent on each page, navigation paths, and on-page interactions.

Some services also explicitly state that they generate inferred information. AI systems can aggregate seemingly trivial data points to derive highly sensitive personal traits—often in ways that exceed users' ability to anticipate or control.[164] Scholars have warned that such practices may even revive discredited methods like phrenology by inferring attributes from physical features.[165]

These inferential capabilities also blur the line between data collection and data processing. As Daniel Solove aptly warns: "[I]f organizations can simply generate new data through inferences, then limitations on data collection lose much of their intended effect."[166] AI's ability to infer sensitive personal traits from seemingly non-sensitive data may also serve as an "end-run" around heightened protections designed for sensitive personal information.[167]

Detailed user profiles may therefore be systematically constructed. Once established, such intimate knowledge can be leveraged for purposes beyond immediate service delivery and may erode autonomy by rendering individuals increasingly transparent, fixed, and predictable.[168]

Together, these practices may enable reportedly Chinese-linked AI service providers—and, if compelled, the Chinese government—to build a comprehensive picture of you: who you are, where you are, your digital footprint, what you look and sound like, and even your vulnerabilities and most intimate characteristics.

13. Intelligence Gathering and Transnational Repression

Profiling could further enhance China's intelligence capabilities. The PRC has long invested in gathering intelligence on strategic foreign targets. As early as 2021, The Washington Post reported that China had been expanding its global surveillance infrastructure to provide its security agencies and military with information on foreign individuals.[169] Professional and even psychological profiles of journalists, academics, and political figures are often constructed by aggregating data from a wide range of sources.[170]

The Hoover Institution has also highlighted how the Chinese party-state leverages data obtained from commercial entities to support intelligence activities. These include compiling databases of human genomic information, mapping foreign economic sectors and borders, extracting commercial and strategic intelligence from telecommunications infrastructure, manipulating digital information environments, and profiling individuals and targeting journalists who report critically on China or its companies.[171]

Data collected through Chinese AI services may serve as a new vector for this objective. These platforms routinely aggregate a broad range of user data—including personal identifiers, chat histories, location information, and detailed records of digital behavior—which can support the construction of highly granular personal profiles. When the PRC invokes its sweeping national security authorities, such data may be accessed with little friction, particularly in cases involving high-value foreign targets.

Datasets of overseas users can also be leveraged to enhance AI models used in intelligence operations. Recent research indicates that the People's Liberation Army (PLA) has likely procured and deployed LLMs fine-tuned specifically for such tasks.[172] This includes models developed by providers such as **Alibaba Cloud, which supports Qwen, and DeepSeek**.[173] These developments underscore how ostensibly consumer-facing Chinese AI systems can be readily repurposed for state-led intelligence efforts—bolstered by the vast troves of global data they collect.

Beyond military applications, such intelligence-gathering efforts may further facilitate transnational repression. These risks are especially acute for dissidents, journalists, and public officials in other societies. According to ARTICLE 19, the PRC is the most prolific perpetrator of such repression worldwide, targeting millions across at least 36 countries.[174] Tactics include digital harassment, intimidation, forced repatriation, abduction, and pressure on family members. These practices inflict multiple forms of harm—from physical danger and emotional distress to autonomy harms such as coercion and the chilling of dissent.

14. Building the "Societal Mosaic" of Democratic Countries

Beyond individual harms, aggregated data produces systemic risks for democratic societies. A Stanford-affiliated think tank warns that unrestrained data collection results in societal-level harms.[175] Scholarship on the relational nature of privacy also underscores that powerful actors use data less to study individuals than to generate population-level insights: mapping relationships, classifying groups, modeling behaviors, and predicting or influencing collective outcomes.[176] These insights can then be applied across all individuals who share those traits.

When Chinese firms extract such analytics from their global user base, they potentially enable their government to construct a comprehensive "societal mosaic" of democratic communities. As Aynne Kokas observes, the strategic danger of China's global data collection lies in combining disparate datasets to map social behavior.[177] This mapping provides the PRC with deep insights into political beliefs, economic vulnerabilities, and social dynamics—intelligence that can be leveraged for geopolitical strategy and coercion.[178]

Democracies are no strangers to such population-level profiling. The 2016 Cambridge Analytica scandal revealed how data-driven demographic insights can be weaponized to undermine democratic processes.[179] In fact, researchers have uncovered a Chinese-compiled database containing information on 2.4 million individuals worldwide, many linked to sectors Beijing considers strategically important for monitoring.[180] China's research institute has also systematically collected and analyzed data on Taiwan's economic, political, military, and cultural domains to generate strategic understanding.[181] ASPI also warns that the CCP is gaining unprecedented insight into social trends by exerting control over data collected from companies operating abroad.[182]

15. AI-Enhanced Information Manipulation

Driven by massive datasets, generative AI has long raised concerns about its potential to intensify information manipulation. It enables the large-scale production of deceptive content at significantly lower cost.[183] The RAND Corporation warns that generative AI may also enhance the credibility of the "messengers" who spread disinformation, as LLMs can be used to develop more human-like bot networks.[184] Moreover, users are increasingly exposed to highly personalized content to maximize cognitive impact.[185] From content creation and dissemination to audience targeting, AI tools can be exploited to conduct manipulation that is **broader in scale, harder to detect, and more cognitively effective**.

China is actively working to turn this potential into reality. Chinese military and political scholars openly promote the concept of "**algorithmic cognitive warfare**" (ACW), which leverages AI to influence and divide foreign populations by analyzing individuals and exploiting social fault lines within rival states.[186] The success of ACW begins with creating detailed user portraits—mapping not only individual profiles but also the broader ideological landscape of a society.[187] This enables the generation of tailored content designed to manipulate public opinion and deepen internal divisions. To support this effort, China requires the collection and processing of granular, comprehensive data on target populations.[188]

A recently disclosed document confirms the deployment of AI-driven influence operations from China.[189] A Chinese company called **GoLaxy** (**中科天玑**) has been found supporting state-aligned campaigns targeting Hong Kong and Taiwan by deploying human-like bot networks and using psychological profiling to target individuals. Through user data extraction and behavioral analysis, GoLaxy's GoPro system can activate AI-generated personas to disseminate tailored content designed to resonate with specific social groups. These personas mimic real user behavior to evade platform detection and are intended to exploit existing societal divisions to manipulate public opinion.

GoLaxy has already amassed extensive datasets on Taiwan to support such operations, including detailed profiles of political figures, influential individuals and organizations across multiple sectors, more than 5,000 high-priority social media accounts, and a wide range of demographic and societal data. It has also compiled data profiles on U.S. targets, including members of Congress and more than 2,000 American political figures and thought leaders. Notably, GoLaxy's public-facing AI platform integrates with several of China's leading AI models, including DeepSeek-R1.[190]

In this context, **Chinese AI services are not only potential sources of data, their underlying models may also serve as engines of more effective manipulation.** Leaked GoLaxy documents reveal that, to enhance its ability for social division and cognitive shaping, the company requires repositories of material on different social groups, political issues, and cognitive scenarios specific to Taiwan. When Taiwanese users engage with Chinese AI services—providing chat content, browsing histories, and inferred information derived from scattered data points—they may unknowingly contribute to the **construction of macro-level insights into Taiwan's societal dynamics.**

Chinese AI systems trained on such data will, in turn, **become increasingly capable of delivering content tailored to manipulate Taiwanese users**. Furthermore, interaction logs and biometric data collected during these engagements could support **the development of AI personas finely tuned to Taiwan's sociocultural context**.

In short, these platforms are not merely data conduits, they are evolving into potent weapons of information manipulation, capable of undermining democratic processes, eroding public trust, and amplifying social divisions.

Figure 6: GoLaxy supports multiple forms of manipulative content generation (Source: Vanderbilt Institute of National Security, 2025)

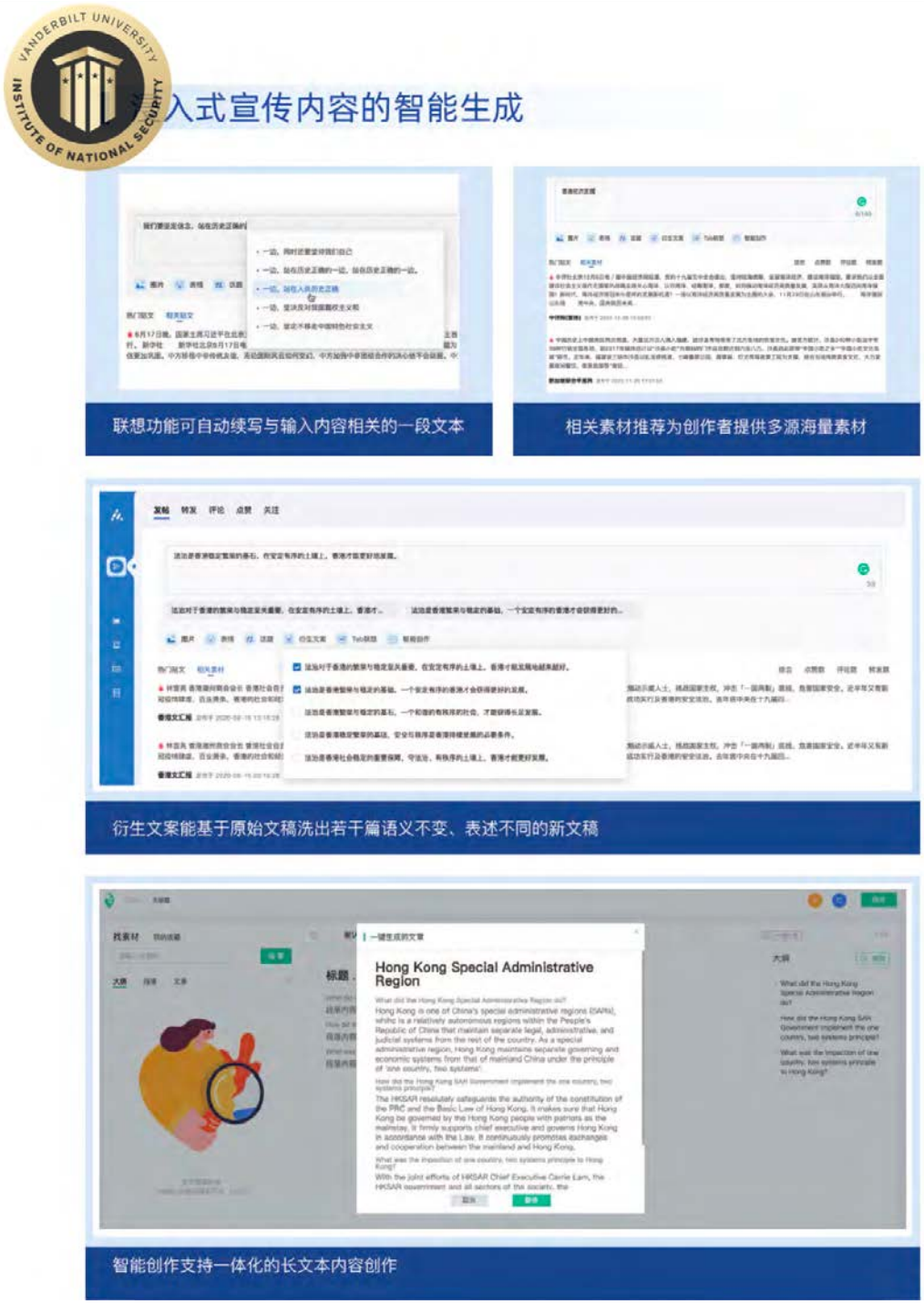


Figure 7: GoLaxy can deploy highly human-like bot accounts to evade detection
(Source: Vanderbilt Institute of National Security, 2025)

Figure 8: GoLaxy has built profiles of key Taiwanese figures and collected extensive demographic and social data

(Source: Vanderbilt Institute of National Security, 2025)

类型	子类	数据量
新闻资讯及社媒数据	内容数据，关系数据	6221577+
全球涉T信源	——	10000+
重点目标社交账号	——	5000，可实现虚实映射
T知识图谱数据	——	10w以上，包括：人物共14881，三元组共182238；其他实体：56413，三元组共403242，总的三元组数：585480。
人物库	T政要画像	170
	T民众户籍数据（闭源数据）	2300w
	宗教界、学术界、商界人物等	13847
组织库	T政党资料	75个政党
	T智库名单	——
	T企业资料	1478家企业，通联方式、地址（台在大陆的企业、500强、上市企业等）
	T宗教资料	13546个宗教团体
	T民调机构资料	——
	T族群结构资料	——
	T人民团体相关资料	23785个人民团体

Figure 9: GoLaxy has built personal profiles of U.S. political figures and opinion leaders

(Source: Vanderbilt Institute of National Security, 2025)

涉M数据积累：政要数据

117届国会议员、2022年国会候选人、建制派、特朗普支持者、右翼势力4000+、NGO账号数据数百个、其他A政治人物和意见领袖2000+

类别	党籍	两院	职位	英文名-去空格	英文名	author_name
右翼势力	共和党			Abraham Hamade	Abraham Hamadeh	Abe Hamadeh for Arizona AG
右翼势力	共和党			Adam Laxalt	Adam Laxalt	Adam Paul Laxalt
右翼势力	共和党			Alison Hayden	Alison Hayden	Alison Hayden 賀亞珊us CA-14 vs.Eric Swalwell
右翼势力	共和党			Andy Biggs	Andy Biggs	Andy Biggs
右翼势力	共和党			Barry Loudermilk R	Barry Loudermilk R	Barry Loudermilk
右翼势力	共和党			Ben Cline	Ben Cline	Ben Cline
右翼势力	共和党			Bill Posey	Bill Posey	Bill Posey
右翼势力	共和党			Brian Babin	Brian Babin	Brian Babin
右翼势力	共和党			Brian Perras	Brian Perras	Brian Perras
右翼势力	共和党			Byron Donalds	Byron Donalds	Byron Donalds
右翼势力	共和党			Chip Roy	Chip Roy	Chip Roy
右翼势力	共和党			Bob Good	Bob Good	Congressman Bob Good
右翼势力	共和党			Dan Bishop	Dan Bishop	Dan Bishop
右翼势力	共和党			Dan Cox	Dan Cox	Dan Cox us - Delegate & Candidate for Governor
右翼势力	共和党			Darren Bailey	Darren Bailey	Darren Bailey for Governor
右翼势力	共和党			Darren Aquino	Darren Aquino	Darren.Dione.Aquino usCONGRESSusUS.House Elec
右翼势力	共和党			Debbie Lesko	Debbie Lesko	Debbie Lesko
右翼势力	共和党			Gary Palmer	Gary Palmer	Gary Palmer
右翼势力	共和党			Greg Steube	Greg Steube	Greg Steube
右翼势力	共和党			Jim Marchant	Jim Marchant	Jim Marchant

Part IV.

Policy Recommendations: The DSR Strategy

As the previous parts have shown, the risks posed by Chinese AI services to democracy are systemic. These risks stem from service providers' transfer of user data to China, either by storing it within Chinese territory or by sharing it with Chinese parent companies or government authorities upon request.

Under China's sweeping national security regimes and in the absence of independent judicial oversight, the Chinese government effectively enjoys unrestricted access to a wide range of intrusive data collected by these services, creating serious potential for exploitation.

For these reasons, Chinese AI services fall squarely within the category of "products deemed to endanger national cybersecurity"—the central focus of Taiwan's evolving data governance framework.[191] To address these threats, this report introduces **the DSR strategy**, comprising three core policy recommendations:

1. To **DEFEND** public systems, Chinese AI services should be comprehensively banned across government agencies and critical infrastructure;

2. To **SCREEN** Chinese AI services entering the domestic market, Taiwan should establish inbound review mechanisms to evaluate their data transfer practices;

3. To **RALLY** democratic allies, cooperation should focus on harmonizing cross-border data regulations among trusted countries to prevent China’s access through regulatory loopholes.

While this report focuses primarily on AI services, the proposed measures may also apply to other Chinese digital services that engage in similar data practices. Also, although these recommendations are tailored to Taiwan's policy landscape, they are also intended to inform the efforts of democratic allies, especially in areas where multilateral cooperation is essential.

Recommendation 1

DEFEND: Banning Chinese AI Services Across Government and Critical Infrastructure

Taiwan must enforce a comprehensive ban on Chinese AI services across government and critical infrastructure. Effective implementation at least requires:

- An interagency task force to identify and update the list of Chinese-controlled AI services;
- Stronger compliance and audits, including expanding public-sector cybersecurity talent and disclosing restricted service lists;
- Regulatory requirements prohibiting public entities and critical infrastructure operators from procuring China-linked products.

Given the risks of intrusive data collection and potential access by the PRC, Taiwan must enforce a comprehensive ban on the use of Chinese AI services, along with other digital products, in government and critical infrastructure (CI) sectors.

Taiwan has already prohibited public entities from using or procuring IT products made by Chinese vendors.[192] Before 2025, these restrictions were enforced through administrative guidance. In August 2025, the legislature amended the Cyber Security Management Act. With narrowly defined exemptions, the new provisions explicitly prohibit the public sector from downloading, installing, or using products deemed to endanger Taiwan's cybersecurity.[193] While identification still requires careful risk assessment, the legislative explanation makes clear that products from Chinese vendors fall within this scope.[194]

Importantly, prior to the 2025 amendment, the Act only imposed general cybersecurity obligations on private CI providers and relied on sectoral regulators to discourage them from using Chinese products. The revised law now explicitly extends the statutory prohibition to include these CI providers.

The real challenge, however, lies in **enforcement capacity**. This involves at least three critical tasks:

1. accurately identifying Chinese vendors and their AI services, and continuously updating the list;

2. ensuring compliance and conducting effective inspections and audits; and

3. verifying that third-party contractors do not embed such products in the services they deliver.

Identifying and Continuously Updating Chinese AI Service Lists

While Taiwan's new law already mandates the establishment of review and information-sharing mechanisms for such products, it is also necessary to create a dedicated interagency task force—including representatives from security, trade, industry, procurement, and data protection—with sufficient authority, personnel, resources, and information to ensure the timely identification of Chinese AI services gaining popularity.

A comparable effort exists in the United States. The Federal Acquisition Security Council (FASC), established in 2018, is an interagency body tasked with protecting federal supply chains from national security threats.[195]

Based on its recommendations, the Secretaries of Defense and Homeland Security, along with the Director of National Intelligence, may issue exclusion or removal orders. Exclusion orders bar companies, products, or services from federal procurement, while removal orders require the elimination of designated items from federal information systems. A recent bipartisan bill would further authorize the FASC to publish a list of AI systems developed by foreign adversaries.[196]

To fulfill its role effectively, Taiwan's task force should establish standards for determining whether a service is substantively controlled by an entity that is China-based or Chinese-owned, including through direct or indirect ownership or control via successor entities or overseas subsidiaries. This approach can help reveal the full extent of Chinese companies' global operational control and prevent policy decisions from being misled by the formal registration locations of overseas service providers.

Ensuring Compliance and Effective Audits

Taiwan's recent legal amendments have taken the right step in strengthening the auditing authority of cybersecurity agencies and expanding the scope of entities subject to oversight. However, given the severe shortage of qualified personnel,[197] the government must act swiftly to expand the talent pool.

Key measures should include investing in robust in-service training to strengthen internal expertise and enhancing career incentives for public-sector cybersecurity professionals—such as better compensation and clearly defined missions that are both meaningful and instill a sense of honor. Mechanisms allowing cybersecurity personnel to rotate between the public and private sectors would also help attract talent to serve temporarily in government and contribute their expertise.

To support effective compliance, Taiwanese policymakers should also **improve the transparency and accessibility of the list of restricted Chinese AI services**. Although other agencies can submit search requests for items on the list, cybersecurity authorities have long withheld it from public disclosure, citing concerns that Chinese companies could circumvent restrictions by altering product names or service locations.[198] There is also fear that disclosure might cause government personnel to focus solely on listed items, overlooking similarly risky products not yet formally identified.

However, this approach creates material compliance frictions. Without access to the full list of prohibited vendors and products, agencies cannot proactively embed exclusion clauses in procurement documents. Verification must be done case by case, significantly increasing time and audit costs. It also deprives bidders of clear market signals, making timely supply-chain adjustments harder.

These frictions are likely to intensify as the statutory restrictions are formally extended to designated non-governmental CI providers, whose procurement networks are typically more diverse and decentralized.

Taiwan's cybersecurity authorities should enhance intelligence sharing in this area. At a minimum, **they should make the list of restricted services and any updates accessible to all public entities and critical infrastructure providers**.

For services on the list, government personnel and CI providers are obligated to avoid their use. For services not listed, they must still conduct due diligence to ensure the product is not of Chinese origin before procurement or deployment. Finally, cybersecurity authorities should continue expanding the existing "safe list" of previously vetted products to further support compliance.

Closing Loopholes in Third-Party Contractor Use

As for the third task, Taiwan's Ministry of Digital Affairs has issued regulations prohibiting public entities from procuring "products deemed to endanger national cybersecurity"[199]—a category that, as previously noted, naturally includes China-linked products. Taiwan's government procurement templates have also long prohibited Chinese vendors from bidding on contracts and bar other vendors from fulfilling contracts using Chinese ICT products.

However, even after the 2025 legal amendments, these procurement restrictions still apply only to public entities and have not yet been explicitly extended to non-government CI providers. While CI providers often avoid such products in practice due to general cybersecurity obligations, this remains a regulatory loophole. It should be addressed promptly to prevent third-party contractors in critical sectors from becoming weak links in the supply chain.

Recommendation 2

SCREEN: Implementing Inbound Reviews to Restrict Data Transfers to China

Taiwan should establish inbound review mechanisms that condition the market access of Chinese AI services on compliant data practices—particularly by default prohibiting the transfer of user data to China. To comply, Chinese AI service providers must:

- Store all data collected in Taiwan locally or in trusted jurisdictions,
- Process and secure data through a locally incorporated third party in Taiwan or a trusted partner country; and
- Report their data practices to regulators and undergo periodic independent audits.

The Taiwanese government should have clear legal authority to enforce these rules, including access restrictions—such as delisting apps or blocking services—as a last resort.

Compared to the U.S. divestiture-centric model, this operational-centric approach offers a more feasible path for Taiwan.

Taiwan should establish inbound review mechanisms to scrutinize the data practices of Chinese AI services. As a general rule, these providers should be prohibited from transferring data to China through any channel. The government should also be equipped with clear legal authority to block persistently non-compliant services within its jurisdiction as a proportional last resort.

As a precondition for operating in Taiwan, **Chinese AI service providers must be prohibited from transferring or storing user data in China, including transfers routed through third countries**. Only narrowly tailored, statutory exceptions are allowed. Providers must also be barred from sharing data across borders with Chinese parent companies or government authorities upon request.

In cases involving law enforcement, access to user data should occur only through applicable mutual legal assistance arrangements. Under no circumstances should service providers unilaterally disclose data in response to foreign government demands.

Compliance Standards and Enforcement Mechanisms

To be effective, Taiwan's inbound review mechanism should require Chinese AI service providers to demonstrate compliance with the following governance practices:

- To restrict data transfers to China, Chinese AI service providers **must store and process all data collected in Taiwan on servers located either in Taiwan or in trusted partner countries** that are officially recognized by the Taiwanese government as having comparable data protection mechanisms. As a general rule, user data must not be transferred beyond these jurisdictions.

- Data access, processing, and security must be performed either in Taiwan or in a trusted partner country, and must be handled by **a locally incorporated third party with vetted personnel and key functions located in that jurisdiction.**

- Compliance with these requirements should be verified through **periodic reporting of data practices** to the relevant authority and **regular reviews conducted by independent auditors**, whose findings must also be made public.

Closing Statutory Gaps in Taiwan's Cross-Border Data Regulation

Taiwan's legal framework must be urgently updated to establish such an inbound review mechanism.

Currently, Taiwan's Personal Data Protection Act (PDPA) is the sole legal framework governing cross-border data transfers. However, the existing regime operates on a "**permissive by default, restrictive by exception**" basis and has long delegated responsibility to sectoral regulators to determine whether a foreign jurisdiction provides adequate data protection—only imposing restrictions when a jurisdiction is deemed inadequate.

To date, such restrictions have only been applied in three sectors: labor, telecommunications, and social work.[200] In all other critical domains, such as health, finance, or transportation, no systemic safeguards exist to prevent data from flowing into China.

Although Taiwan amended the PDPA in November 2025 with the aim of centralizing cross-border data transfer regulation under the newly established Personal Data Protection Commission,[201] transfers to China remain permitted by default. **This overly permissive approach must be reformed.**

At a minimum, the law should prohibit Chinese digital service providers operating in Taiwan from transferring user data to China. In addition, the government must be granted clear legal authority to require such providers to appoint legal representatives in Taiwan and to impose penalties on those who violate data security or cross-border transfer regulations.

Where a service provider persistently refuses to comply with corrective orders, authorities may, subject to due process and judicial oversight, restrict access to the service through measures such as directing ISPs to block DNS resolution or requesting app store delisting, as actions of strict necessity and last resort.

An Operational-Centric Approach with Teeth

Blocking access in cases of continued violations can be consistent with the principle of proportionality. For example, DeepSeek was temporarily removed from app stores in **South Korea** after the country's Personal Information Protection Commission found its data protection practices inadequate.[202] It was only reinstated after the service provider complied with specific requirements, such as obtaining separate user consent for cross-border data transfers and halting the transmission of user inputs to a Chinese partner company.[203]

The European Union offers another instructive example of such regulations. With judicial safeguards in place, the General Data Protection Regulation (GDPR) empowers supervisory authorities to impose fines and corrective orders, including restrictions on data processing and cross-border transfers.[204] The Digital Services Act (DSA) further authorizes access restrictions on intermediary services, provided strict necessity and last-resort conditions are met to prevent ongoing serious harm.[205]

For instance, in June 2025, the Berlin Commissioner for Data Protection found that DeepSeek's transfer of user data to China violated the GDPR.[206] Citing Article 16 of the DSA, the Commissioner flagged the app as illegal content and requested that Apple and Google consider removing it from their app stores in Germany. While some questioned whether Article 16 was the appropriate legal basis,[207] the case highlights how EU law equips regulators with necessary tools to respond to data processing violations by Chinese digital services.

The United States has also strengthened its legal tools to bar adversary-controlled digital services. In April 2024, Congress enacted the "TikTok law," which bars U.S. app stores and internet-hosting providers from distributing, maintaining, or providing services to any foreign-adversary-controlled application unless the owner completes a President-approved qualified divestiture.[208]

However, a divestiture-centric approach is less suited to Taiwan. Most Chinese services reach Taiwan via entities in China or third countries (e.g., Singapore), and Taiwan's smaller market offers limited leverage to compel ownership restructuring. A more workable path is to condition market access on the operational side—such as through strict cross-border data controls, as proposed in this report.

Recommendation 3

RALLY: Harmonizing Cross-Border Data Regulations Through Multilateral Cooperation

Taiwan and its trusted allies must harmonize cross-border data transfer rules to close regulatory loopholes.

Current U.S. tools offer only partial safeguards. The informational-materials exception under IEEPA limits regulatory reach, while CFIUS (transaction-triggered) and the TikTok Law (definition-bound and ownership-centric) do not provide a sufficient legal basis for imposing ongoing operational restrictions on foreign-based services.

New legislation is needed to establish robust data transfer controls and align U.S. policy with Taiwan and other partners.

Harmonizing Data Transfer Rules across Democracies

Taiwan and its democratic allies must harmonize their regulatory frameworks to prevent the continued data outflow to China, especially through the AI services highlighted in this report.

As shown in the previous parts, some Chinese AI services do not transmit user data directly to China but instead store it in third countries, including the U.S. However, this data may still be subject to access requests from Chinese parent companies or government authorities. If the third countries lack adequate restrictions on secondary data transfers, these regulatory gaps may result in the data reaching China, defeating the very purpose of containment efforts.

For the U.S., it is also necessary to establish restrictions on cross-border data flows to China in order to mitigate both the individual and collective-level risks outlined above. **In fact, several regulatory efforts are already underway, backed by bipartisan support.**[209]

For example, Executive Order (E.O.) 14117 bars U.S. persons from data transactions that would give countries of concern access to bulk sensitive personal data or U.S. government-related data.[210] Congress also enacted the *Protecting Americans' Data from Foreign Adversaries Act* (PADFA), which makes it unlawful for data brokers to sell or otherwise make available sensitive data of U.S. individuals to a foreign adversary country or any entity it controls.[211]

Limitations of the U.S. Regime for Data Transfer Control

These measures, however, **do not fully address the challenge**. First, the data-transfer practices of Chinese service providers remain largely unregulated. Second, focusing only on "sensitive" data may ease enforcement but overlooks modern AI's ability to infer highly personal traits from large volumes of seemingly trivial data.

Moreover, actions grounded in the *International Emergency Economic Powers Act* (IEEPA) framework are more vulnerable to legal challenge. While granting the President sweeping authority to address peacetime emergencies, IEEPA explicitly excludes the power to regulate "informational materials."[212] U.S. courts enjoined the 2020 TikTok restrictions as exceeding IEEPA in light of those statutory exceptions.[213]

A similar concern applies to E.O. 13873, which authorizes the Secretary of Commerce to block ICT products or services provided by entities under the jurisdiction of a foreign adversary if they are deemed to pose an unacceptable data security risk.[214] Such actions may also invite ultra vires challenges if interpreted as regulating informational materials.

E.O. 14117 could face analogous objections if a court deemed restrictions on bulk data access indistinguishable from restrictions on informational flows—though the DOJ's final rule implementing E.O. 14117 is in force and is framed around national-security-relevant data transactions, not expressive content.[215]

In sum, given IEEPA's internal limitations, regulations based on it may not serve as a durable mechanism for addressing data outflows to China.

Limits of CFIUS in Governing Foreign AI Services

Another relevant mechanism is the Committee on Foreign Investment in the United States (CFIUS), which reviews covered transactions involving foreign investment in the U.S. to assess and mitigate national security risks.[216] Under the *Foreign Investment Risk Review Modernization Act of 2018* (FIRRMA), CFIUS's jurisdiction was expanded to include investments that may grant foreign entities access to sensitive personal data of U.S. citizens.[217]

However, CFIUS review is **transaction-triggered.** For example, the process became applicable to TikTok only after ByteDance acquired U.S.-based Musical.ly in 2017.[218] Today, many Chinese AI services reach U.S. users without a covered investment or on-shore corporate presence; accordingly, CFIUS is ill-suited to police ongoing data-collection practices by foreign services operating from abroad.

Divest-or-Ban Is Not Enough for Chinese AI Services

The third relevant mechanism is the TikTok Law—*the Protecting Americans from Foreign Adversary Controlled Applications Act*—which establishes a framework for restricting foreign-adversary-controlled applications.[219] Beyond TikTok, it authorizes the President to designate any content-sharing app with over one million monthly active users as a national-security threat if it is operated by an entity controlled by a foreign adversary.

Once designated, the company must complete a President-approved qualified divestiture or face a nationwide prohibition on distribution, maintenance, and updating by U.S. app stores and internet-hosting providers.

However, the **TikTok Law may also fall short in addressing Chinese AI services**. Under its statutory definitions, the Act primarily targets applications that enable social networking. General-purpose AI assistants like DeepSeek—lacking such features—are therefore less likely to qualify as "foreign adversary-controlled applications" under the Act.

The law's divest-or-ban model presents additional limitations: unlike TikTok, many Chinese AI services are operated by entities incorporated overseas and are less likely to restructure ownership merely to retain U.S. market access. In such cases, regulating cross-border data transfers may offer a more effective policy lever.

The Need for New Legislation

Accordingly, the U.S. should consider harmonizing its regulations with Taiwan and other allies to prohibit Chinese AI service providers from transferring user data to China by any means. Yet existing tools present scope and durability gaps.

The informational-materials carve-outs under IEEPA may constrain such efforts, while neither CFIUS (transaction-triggered) nor the TikTok Law (definition-bound, ownership-centric) provides a sufficient legal basis to impose ongoing operational restrictions on foreign-based services.

To close these gaps, new legislation from the U.S. Congress is essential.

Appendix

Privacy Policies of AI Services Examined

The privacy policies of the services examined in this report are based on the versions linked in the biannual generative AI reports by Andreessen Horowitz and confirmed to be accessible to users in Taiwan. They reflect the most up-to-date versions available as of November 15, 2025. To ensure consistency and verifiability, each policy has been preserved either via Archive.today or exported directly from the original webpage, recognizing that service providers may revise their policies over time.

Please note that the version of a privacy policy displayed, even when accessed through the same link, may vary depending on the user's IP address, browser settings, or operating system language. Accordingly, all analyses in this report are based on the versions accessible to users in Taiwan operating in Mandarin-language environments, as reflected in the archived content below.

1. DeepSeek
Archived copy: http://archive.today/Ojpkk
Original link: https://cdn.deepseek.com/policies/en-US/deepseek-privacy-policy.html

2. Kimi
Archived copy: https://chai.dset.tw/docs/Kimi%20Privacy%20Policy.pdf
Original link: https://www.kimi.com/user/agreement/userprivacy?version=v2

3. Doubao
Archived copy: http://archive.today/wwhEu
Original link: https://www.doubao.com/legal/privacy

4. Quark (Mobile)
Archived copy: http://archive.today/9EGgF
Original link: https://terms.alicdn.com/legal-agreement/terms/c_end_product_protocol/20230831162328667/20230831162328667.html

5. Baidu AI Search
Archived copy: http://archive.today/vPw6u
Original link: https://s.bdstatic.com/common/agreement/privacy.html

6. Monica
Archived copy: http://archive.today/lm9ws
Original link: https://monica.im/privacy

7. Cici
Archived copy: http://archive.today/2Qrr8
Original link: https://www.ciciai.com/legal/privacy/en

8. Talkie
Archived copy: https://chai.dset.tw/docs/Talkie%20Privacy%20Policy.pdf
Original link: https://www.talkie-ai.com/static/privacy

9. Qwen Chat
Archived copy: http://archive.today/nABNC
Original link: https://chat.qwen.ai/legal-agreement/privacy-policy?spm=a2ty_o01.29997169.0.0.3d4d5171NzzXkH

10. Manus
Archived copy: http://archive.today/Z45Ih
Original link: https://manus.im/privacy

Summary Table: Data Collection, Storage, and Sharing Practices of Examined China-Linked AI Services

This report categorizes the data collected by the examined Chinese AI services based on an analysis of their privacy policies, which were archived above and reflect the most up-to-date versions available on their official websites as of November 15, 2025. The categorization framework originated from DeepSeek's privacy policy structure but was modified to accurately encompass the data types collected by all services in this study.

The accompanying spreadsheet, accessible via the link and QR code below, details these findings. Its first sheet provides a summary pivot table (1 = collection, 0 = non-collection) with a "SUM" row totaling the number of distinct data types each service collects. Sheets 2 through 11 provide a detailed breakdown for each service (Y = collection, N = non-collection), citing the corresponding passages from their respective privacy policies.

(Excel sheets) Chinese AI Services: Data Collection

The accompanying spreadsheet, accessible via the link and QR code below, lists the data storage locations, data-sharing scopes, and government access provisions for the ten identified China-linked AI services. For each service, the corresponding provisions, articles, or clauses are cited directly from its privacy policy. To preserve the precise meaning of these policies, where only a Chinese-language version was available, the original Chinese text was extracted and listed.

(Excel sheets) Chinese AI Services: Data Storage, Sharing, and Government Access

References

1. Bradford, A. (2024). Exporting China's digital authoritarianism through infrastructure. In *Digital Empires: The Global Battle to Regulate Technology* (pp. 234–267). Oxford University Press; de La Bruyère, E., Strub, D., & Marek, J. (Eds.). (2022, March 1). *China's digital ambitions: A global strategy to supplant the liberal order* (NBR Special Report No. 97). The National Bureau of Asian Research. https://www.nbr.org/publication/chinas-digital-ambitions-a-global-strategy-to-supplant-the-liberal-order/

2. Kokas, A. (2022). *Trafficking data: How China is winning the battle for digital sovereignty.* Oxford University Press.

3. Harris, L., & Zhu, L. (2023, May 23). *Generative artificial intelligence and data privacy: A primer* (CRS Report No. R47569). Congressional Research Service. https://www.congress.gov/crs-product/R47569

4. State Council of the People's Republic of China. (2017, July 20). *Notice of the State Council on the issuance of the New Generation Artificial Intelligence Development Plan* (Guofa [2017] No. 35) *[国务院关于印发新一代人工智能发展规划的通知]*. http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm; State Council of the People's Republic of China. (2025, August 26). *Opinions of the State Council on comprehensively implementing the "AI +" initiative* (Guofa [2025] No. 11) *[国务院关于深入实施 "人工智能＋ " 行动的意见（国发〔2025〕11 号）]*. https://www.gov.cn/zhengce/content/202508/content_7037861.htm

5. Ministry of Commerce et al. (2025, September 22). *Notice of the Ministry of Commerce and other nine departments on Printing and Distributing the "Several Policy Measures to Promote Service Export"* (Shang-Fu Mao Fa [2025] No. 186) *[商务部等 9 部门印发《关于促进服务出口的若干政策措施》的通知]*. https://www.gov.cn/zhengce/zhengceku/202509/content_7042162.htm

6. Global Times. (2025, April 27). *GT Voice: What does China's $96b AI industry mean for the world?* https://www.globaltimes.cn/page/202504/1332992.shtml

7. AInvest. (2025, July 3). *Chinese AI models gain ground globally as cost-effective alternatives to U.S. giants.* https://www.ainvest.com/news/chinese-ai-models-gain-ground-globally-cost-effective-alternatives-giants-2507/

8. Ibid.

9. Depoux, D. (2025). *Five key trends in China's generative AI market in 2025.* Roland Berger. https://www.rolandberger.com/en/Insights/Publications/Five-key-trends-in-China-s-generative-AI-market-in-2025.html

10. Au, A., & Chen, F. (2025, April 11). *China expands AI globally through the Digital Silk Road.* East Asia Forum. https://eastasiaforum.org/2025/04/11/china-expands-ai-globally-through-the-digital-silk-road/

11. Andreessen Horowitz. (2025, August 27). *The top 100 Gen AI consumer apps (5th ed.).* https://a16z.com/100-gen-ai-apps-5/

12. Burgess, M., & Newman, L. H. (2025, January 27). *DeepSeek's popular AI app is explicitly sending US data to China. WIRED.* https://www.wired.com/story/deepseek-ai-china-privacy-data/; Select Committee on the Strategic Competition between the United States and the Chinese Communist Party. (2025). *DeepSeek unmasked: Exposing the CCP's latest tool for spying, stealing, and subverting U.S. export control restrictions.* https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/DeepSeek%20Final.pdf

13. Wu, C.-y., & Khan, F. (2025, November 17). China's AI models pose risks, NSB says. Taipei Times. https://www.taipeitimes.com/News/front/archives/2025/11/17/2003847325

14. Hively, A. (2025, November 9). *These US states have outlawed DeepSeek, and more bans may be on the way.* BGR. https://www.bgr.com/2014815/deepseek-illegal-us-states/; Bloomberg News. (2025, February 7). *Canada bans DeepSeek chatbot on government devices.* Bloomberg. https://www.bloomberg.com/news/articles/2025-02-07/canada-bans-deepseek-chatbot-on-government-devices;
Reuters. (2025, February 4). *Australia bans DeepSeek on government devices, citing security concerns.* https://www.reuters.com/technology/australia-bans-deepseek-government-devices-citing-security-concerns-2025-02-04/;
Blanchard, B. (2025, January 31). *Taiwan bans government agencies from using DeepSeek, citing security concerns. Reuters. Reprinted in Taipei Times.* https://www.taipeitimes.com/News/taiwan/archives/2025/01/31/2003831128

15. Gottheimer, J., & LaHood, D. (2025, February 6). *RELEASE: Gottheimer, LaHood introduce new bipartisan legislation to protect Americans from DeepSeek* [Press release]. U.S. House of Representatives. https://gottheimer.house.gov/posts/release-gottheimer-lahood-introduce-new-bipartisan-legislation-to-protect-americans-from-deepseek

16. Krishnamoorthi, R., & Moolenaar, J. (2025, June 25). *Krishnamoorthi and Moolenaar lead bipartisan, bicameral bill to protect federal agencies from the risks of AI technologies developed by foreign adversaries* [Press release]. Select Committee on the Chinese Communist Party, U.S. House of Representatives. https://democrats-selectcommitteeontheccp.house.gov/media/press-releases/krishnamoorthi-and-moolenaar-lead-bipartisan-bicameral-bill-protect-federal

17. Rosen, J., & Cassidy, B. (2025, May 9). Rosen, *Cassidy introduce legislation to protect sensitive federal data from CCP-owned DeepSeek, adversarial AI technologies* [Press release]. U.S. Senate. https://www.rosen.senate.gov/2025/05/09/rosen-cassidy-introduce-legislation-to-protect-sensitive-federal-data-from-ccp-owned-deepseek-adversarial-ai-technologies/

18. Baker McKenzie. (2025, October 7). *Taiwan: Amendment to Cybersecurity Management Act.* https://insightplus.bakermckenzie.com/bm/data-technology/taiwan-amendment-to-cybersecurity-management-act_1

19. Reuters. (2025, February 4). *Italy's regulator blocks Chinese AI app DeepSeek on data protection.* https://www.reuters.com/technology/artificial-intelligence/italys-privacy-watchdog-blocks-chinese-ai-app-deepseek-2025-01-30/;
Ersen, H., & Murray, M. (2025, June 27). *DeepSeek faces ban from Apple, Google app stores in Germany.* Reuters. https://www.reuters.com/sustainability/boards-policy-regulation/deepseek-faces-expulsion-app-stores-germany-2025-06-27/

20. Huang, K.-S. (2025, June). *What democracies get wrong about Chinese AI.* The Diplomat. https://thediplomat.com/2025/06/what-democracies-get-wrong-about-chinese-ai/

21. ARTICLE 19. (2025). *Cybersecurity with Chinese characteristics: Digital governance in the Indo-Pacific and the Taiwanese alternative.*https://www.article19.org/wp-content/uploads/2025/02/cybersecurity-with-chinese-characteristics.pdf;
Center for Internet Security, Inc. (CIS). (2024, August 14). *The Chinese Communist Party (CCP): A quest for data control.* https://www.cisecurity.org/insights/blog/the-chinese-communist-party-ccp-a-quest-for-data-control;
Johnson, M. (2023). *China's grand strategy for global data governance. The Hoover Institution.* https://www.hoover.org/sites/default/files/research/docs/Johnson_ChinasGrandStrategy_Web.pdf

22. Council on Foreign Relations. (n.d.). *Assessing China's Digital Silk Road initiative: A transformative approach to technology financing or a danger to freedoms?* Retrieved November 13, 2025, from https://www.cfr.org/china-digital-silk-road/

23. China Academy of Information and Communications Technology. (2019). *White paper on big data.* http://www.caict.ac.cn/english/research/whitepapers/202003/P020200327550643303469.pdf

24. State Council of the People's Republic of China. (2015, August 15). *State Council notice on issuing the action outline for promoting the development of big data [国务院关于印发促进大数据发展行动纲要的通知].* https://www.gov.cn/zhengce/content/2015-09/05/content_10137.htm

25. China Academy of Information and Communications Technology. (2019). *White paper on big data.* http://www.caict.ac.cn/english/research/whitepapers/202003/P020200327550643303469.pdf

26. Xinhua. (2017, November 3). *Full text of Xi Jinping's report at 19th CPC National Congress.* http://www.xinhuanet.com/english/special/2017-11/03/c_136725942.htm

27. Ministry of Industry and Information Technology of the People's Republic of China. (2021). *14th Five-Year plan for big data industry development ["十四五"大数据产业发展规划].*https://www.gov.cn/zhengce/zhengceku/2021-11/30/5655089/files/d1db3abb2dff4c859ee49850b63b07e2.pdf

28. Ibid.

29. Ibid.

30. Ibid.

31. Ibid.

32. Ibid.

33. Kokas, A. (2022). *Trafficking data: How China is winning the battle for digital sovereignty.* Oxford University Press.

34. Johnson, M. (2023). *China's grand strategy for global data governance.* The Hoover Institution. https://www.hoover.org/sites/default/files/research/docs/Johnson_ChinasGrandStrategy_Web.pdf

35. Chatzky, A., & McBride, J. (2020, January 28). *China's massive Belt and Road initiative.* Council on Foreign Relations. https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative.

36. Greene, R., & Triolo, P. (2020, May 8). *Will China control the global internet via its Digital Silk Road?* Carnegie Endowment for International Peace. https://carnegieendowment.org/posts/2020/05/will-china-control-the-global-internet-via-its-digital-silk-road?lang=en

37. Erie, M. S., & Streinz, T. (2021). The Beijing effect: China's Digital Silk Road as transnational data governance. *New York University Journal of International Law and Politics*, 54(1), 1–92.

38. Ibid.

39. Ibid.

40. Bouey, J., Hu, L., Scholl, K., Marcellino, W., Yi, S., Dossani, R., Gazis, J., Malik, A. A., Solomon, K., Zhang, S., & Shufer, A. (2023). *China's AI exports database (CAIED)* (Tool No. TL-A2696-1). RAND Corporation. https://www.rand.org/pubs/tools/TLA2696-1.html

41. Au, A., & Chen, F. (2025, April 11). *China expands AI globally through the Digital Silk Road.* East Asia Forum. https://eastasiaforum.org/2025/04/11/china-expands-ai-globally-through-the-digital-silk-road/

42. Kokas, A. (2022). *Trafficking data: How China is winning the battle for digital sovereignty.* Oxford University Press.

43. See Company Law of the People's Republic of China (promulgated Dec. 29, 1993, amended Oct. 26, 2018) (China).

44. Johnson, M. (2023). *China's grand strategy for global data governance.* The Hoover Institution. https://www.hoover.org/sites/default/files/research/docs/Johnson_ChinasGrandStrategy_Web.pdf

45. Brant, R. (2018, November 27). *Why is Jack Ma a member of the Communist Party of China?* BBC News. https://www.bbc.com/news/business-46353767

46. ARTICLE 19. (2024). *The Digital Silk Road: China and the rise of digital repression in the Indo-Pacific*. https://www.article19.org/wp-content/uploads/2024/04/DSR_final.pdf

47. Cybersecurity Law of the People's Republic of China, art. 30 (2026).

48. Data Security Law of the People's Republic of China, art. 35 (2021).

49. Data Security Law of the People's Republic of China, art. 24 (2021).

50. Regulation on Network Data Security Management, art. 13 (State Council, 2024) (China).

51. Cybersecurity Law of the People's Republic of China, art. 37 (2026).

52. Provisions on Procedures for Administrative Law Enforcement by Cyberspace Departments, art. 19-21 (the Cyberspace Admin. of China, 2023) .

53. Counter-Espionage Law of the People's Republic of China, art. 26 (2014).

54. Counter-Espionage Law of the People's Republic of China, art. 59 (2014).

55. Johnson, M. (2023). *China's grand strategy for global data governance.* The Hoover Institution. https://www.hoover.org/sites/default/files/research/docs/Johnson_ChinasGrandStrategy_Web.pdf

56. Data Security Law of the People's Republic of China, art. 25 (2021).

57. Cybersecurity Law of the People's Republic of China, art. 39 (2026).

58. Ibid.

59. Regulation on Network Data Security Management, art. 62 (State Council, 2024).

60. Data Security Law of the People's Republic of China, art. 21 (2021).

61. Data Security Law of the People's Republic of China, art. 31 (2021).

62. Data Security Law of the People's Republic of China, art. 36 (2021).

63. Personal Information Protection Law of the People's Republic of China, arts. 36, 40 (2021).

64. Provisions on Promoting and Regulating Cross-Border Data Flow, art. 7 (the Cyberspace Admin. of China, 2023).

65. Horsley, J. P. (2025). *China's data dilemma: Maximizing data utilization while ensuring data security. SSRN.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5674524

66. Provisions on Promoting and Regulating Cross-Border Data Flow, art. 3-6, 8 (the Cyberspace Admin. of China, 2023).

67. Cyberspace Administration of China. (2025, April 9). *Q&A on cross-border data security management policy [数据出境安全管理政策问答].* https://www.cac.gov.cn/2025-04/09/c_1745906286623776.htm

68. Personal Information Protection Law of the People's Republic of China, arts. 36, 41 (2021).

69. Provisions on Promoting and Regulating Cross-Border Data Flow, art. 4 (the Cyberspace Admin. of China, 2023).

70. Electronic Privacy Information Center. (n.d.). *Foreign Intelligence Surveillance Court (FISC).* https://epic.org/foreign-intelligence-surveillance-court-fisc/

71. Ibid.

72. Library of Congress, Congressional Research Service. (2018). *Cross-border data sharing under the CLOUD Act* (CRS Report No. R45173). https://www.congress.gov/crs-product/R45173

73. Ibid.

74. National Security Law of the People's Republic of China (2015).

75. National People's Congress, *A Holistic View of National Security* (Dec. 9, 2021), http://en.npc.gov.cn.cdurl.cn/2021-12/09/c_688389.htm

76. National Security Law of the People's Republic of China (2015).

77. 中共中央宣传部、中央国家安全委员会办公室 . (2022). *总体国家安全观学习纲要 [Outline for studying the holistic national security concept].* 人民出版社／学习出版社 . https://news.ucas.ac.cn/docs/2024-04/0e2a5f54cc994a738a22930ee022892d.pdf

78. National Security Law of the People's Republic of China, arts. 2, 9 (2015).

79. National Security Law of the People's Republic of China, arts. 2, 11 (2015).

80. Personal Information Protection Law of the People's Republic of China, art. 3 (2021).

81. Personal Information Protection Law of the People's Republic of China), art. 34 (2021).

82. Personal Information Protection Law of the People's Republic of China, art. 35 (2021); See also Jia, M. (2024). Authoritarian privacy. *The University of Chicago Law Review,* 91(3), 733-809.

83. Shahbaz, A. (2018). *Freedom on the Net 2018: The rise of digital authoritarianism.* Freedom House. https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism

84. Polyakova, A., & Meserole, C. (2019). *Exporting digital authoritarianism.* Brookings Institution. https://www.brookings.edu/wp-content/uploads/2019/08/fp_20190826_digital_authoritarianism_polyakova_meserole.pdf

85. Tóth, G. A. (2017). *Authoritarianism.* Oxford Constitutional Law. https://oxcon.ouplaw.com/display/10.1093/law-mpeccol/law-mpeccol-e205?prd=OXCON

86. Jia, M. (2024). Authoritarian privacy. *The University of Chicago Law Review*, 91(3), 733-809.

87. Johnson, M. (2023). *China's grand strategy for global data governance.* The Hoover Institution. https://www.hoover.org/sites/default/files/research/docs/Johnson_ChinasGrandStrategy_Web.pdf

88. Andreessen Horowitz. (2025, March 6). *The top 100 Gen AI consumer apps (4th ed.).* https://a16z.com/100-gen-ai-apps-4/;
Andreessen Horowitz. (2025, August 27). *The top 100 Gen AI consumer apps (5th ed.).* https://a16z.com/100-gen-ai-apps-5/

89. Roland Berger. (2025, March 28). *Five key trends in China's generative AI market in 2025.* https://www.rolandberger.com/en/Insights/Publications/Five-key-trends-in-China-s-generative-AI-market-in-2025.html

90. Yang, Z. (2025, October 17). *ByteDance's other AI chatbot is quietly gaining traction around the world.* WIRED. https://www.wired.com/story/bytedances-ai-chatbot-is-quietly-gaining-traction-around-the-world/

91. Gibney, E. (2025, July 16). *'Another DeepSeek moment': Chinese AI model Kimi K2 stirs excitement. Nature*, 643(8073), 889-890. https://doi.org/10.1038/d41586-025-02275-6

92. Investing.com. (2025, May 13). *Alibaba's Qwen Chat AI chatbot now features Deep Research.* https://www.investing.com/news/stock-market-news/alibabas-qwen-chat-ai-chatbot-now-features-deep-research-93CH-4042545

93. Tech in Asia. (2025, April 13). *Alibaba's Quark becomes top AI app in China.* https://www.techinasia.com/news/alibabas-quark-becomes-top-ai-app-in-china

94. Ruan, Y. (2025, April 21). *Quark tops download list in Taiwan.* DAO Insights. https://daoinsights.com/news/quark-tops-download-list-in-taiwan/

95. Huang, R. (2024, July 27). One of *America's hottest entertainment apps is Chinese-owned. The Wall Street Journal.* https://www.wsj.com/tech/ai/one-of-americas- hottest-entertainment-apps-is-chinese-owned-04257355

96. Au-Yeung, A., Huang, R., & Clark, K. (2025, December 29). *Meta buys AI startup Manus for more than $2 billion. The Wall Street Journal.* https://www.wsj.com/tech/ai/meta-buys-ai-startup-manus-adding-millions-of-paying-users-f1dc7ef8; Yu, Y., & Zhou, C. (2025, December 30). *Meta says AI startup Manus to cut China ties after acquisition. Nikkei Asia.* https://asia.nikkei.com/business/technology/artificial-intelligence/meta-says-ai-startup-manus-to-cut-china-ties-after-acquisition.

97. DeepSeek. (2025, July 4). *DeepSeek privacy policy.* https://cdn.deepseek.com/policies/en-US/deepseek-privacy-policy.html

98. Kimi. (2025, October 29). *Kimi privacy policy.* https://kimi.moonshot.cn/user/agreement/userprivacy?version=v2

99. Baidu. (2025, February 18). *Baidu AI Search privacy policy.* https://s.bdstatic.com/common/agreement/privacy.html

100. Doubao. (2025, October 17). *Doubao privacy policy.* https://www.doubao.com/legal/privacy

101. 界面新闻 . (2023, July 31). 抖音在北京成立春田知韵科技公司，注册资本 100 万 . https://www.jiemian.com/article/9838390.html

102. Quark. (2025, March 25). *Quark privacy policy.* https://terms.alicdn.com/legal-agreement/terms/c_end_product_protocol/20230831162328667/20230831162328667.html

103. Andreessen Horowitz. (2025, August 27). *The top 100 Gen AI consumer apps (5th ed.).* https://a16z.com/100-gen-ai-apps-5/

104. 张凯然 . (2025, March 10). 全球 AI 产品再次洗牌，" 中国制造 " 后来居上 . 36Kr. https://www.36kr.com/p/3200517350948230

105. 张凯然 . (2025, August 28). 全球 Top50 AI 产品榜单更新，华人团队成最大赢家？. 36Kr. https://www.36kr.com/p/3442571656123781

106. Baker-White, E. (2024, January 17). *TikTok owner ByteDance quietly launched 4 generative AI apps powered by OpenAI's GPT. Forbes Australia.* https://www.forbes.com.au/news/innovation/tiktok-owner-bytedance-launched-4-generative-ai-apps-powered-by-openais-gpt/

107. Ibid.

108. Huang, R. (2024, July 27). O*ne of America's hottest entertainment apps is Chinese-owned. The Wall Street Journal.* https://www.wsj.com/tech/ai/one-of-americas-hottest-entertainment-apps-is-chinese-owned-04257355/

109. Ibid.

110. Alibaba's Qwen Chat AI chatbot now features Deep Research, Investing.com, https://www.investing.com/news/stock-market-news/alibabas-qwen-chat-ai-chatbot-now-features-deep-research-93CH-4042545.

111. Investing.com. (2025, May 13). *Alibaba's Qwen Chat AI chatbot now features Deep Research.* https://www.investing.com/news/stock-market-news/alibabas-qwen-chat-ai-chatbot-now-features-deep-research-93CH-4042545/;
Alibaba Cloud. (2025, April 29). *Alibaba introduces Qwen3, setting new benchmark in open-source AI with hybrid reasoning.* https://www.alibabacloud.com/blog/alibaba-introduces-qwen3-setting-new-benchmark-in-open-source-ai-with-hybrid-reasoning_602192

112. Tang, S. K. (2015, August 18). *New Singapore HQ to underpin Alibaba's cloud push. CNBC.* https://www.cnbc.com/2015/08/18/new-singapore-hq-for-aliyun-underpins-alibabas-cloud-push.html

113. Reuters. (2023, November 16). *Alibaba split: What are the six units of the Chinese e-commerce company?* https://www.reuters.com/markets/deals/how-alibabas-six-new-business-units-stack-up-2023-06-20/

114. Hsu, T.-l., & Yeh, E. (2024, August 25). *China-made AI apps a concern: Expert. The Taipei Times.* https://www.taipeitimes.com/News/taiwan/archives/2024/08/25/2003822741

115. 网信北京 . (2025, March 14). 北京市生成式人工智能服务已登记信息公告 (3 月 14 日) . 新浪财经 . https://finance.sina.com.cn/tech/roll/2025-03-14/doc-inepqxcs3007807.shtml

116. Chen, W. (2025, March 7). "*Was Manus another DeepSeek moment? Chinese AI agent faces doubts after rapid rise to fame". South China Morning Post.* https://www.scmp.com/tech/big-tech/article/3301547/was-manus-another-deepseek-moment-chinese-ai-agent-faces-doubts-after-rapid-rise-fame

117. Tech in Asia. (2025, March 13). *Chinese tech firm Monica raises new funding led by Tencent.* https://www.techinasia.com/news/chinese-tech-firm-monica-raises-funding-led-tencent

118. Internet Law Review. (2025, July 16). *Manus Capital's dilemma: Chinese roots hard to shake, headquarters relocated to Singapore and layoffs after Silicon Valley financing.* 36Kr European Central Station. https://eu.36kr.com/en/p/3381045007423621; McMorrow, R., Liu, N., Hammond, G., & Miller, J. (2025, August 11). *Manus and Benchmark: The AI deal that upset China and the U.S. Financial Times.* https://www.ft.com/content/8e8521a7-b232-4fe0-b262-9dafb8ff5bdd

119. Tech in Asia. (2025, July 8). *Manus shifts HQ to Singapore, cuts China jobs.* https://www.techinasia.com/news/manus-shifts-hq-singapore-cuts-china-jobs

120. Thorbecke, C. (2025, July 16). *Manus AI's 'De-China' playbook is a trap. Bloomberg Opinion.* https://www.bloomberg.com/opinion/articles/2025-07-16/manus-ai-s-de-china-playbook-is-a-trap

121. 林娉莹 . (2025, June 18). 开发智能体 Manus AI 总部迁至新加坡 . 联合早报 . https://www.zaobao.com.sg/finance/singapore/story20250618-6864600

122. Internet Law Review. (2025, July 16). *Manus Capital's dilemma: Chinese roots hard to shake, headquarters relocated to Singapore and layoffs after Silicon Valley financing.* 36Kr European Central Station. https://eu.36kr.com/en/p/3381045007423621; Thorbecke, C. (2025, July 16). *Manus AI's 'De-China' playbook is a trap. Bloomberg Opinion.* https://www.bloomberg.com/opinion/articles/2025-07-16/manus-ai-s-de-china-playbook-is-a-trap

123. Ibid.

124. DeepSeek. (2025, July 4). *DeepSeek privacy policy.* https://cdn.deepseek.com/policies/en-US/deepseek-privacy-policy.html

125. Doubao. (2025, October 17). *Doubao privacy policy.* https://www.doubao.com/legal/privacy; Baidu. (2025, February 18). *Baidu AI Search privacy policy.* https://s.bdstatic.com/common/agreement/privacy.html; Quark. (2025, March 25). *Quark privacy policy.* https://terms.alicdn.com/legal-agreement/terms/c_end_product_protocol/20230831162328667/20230831162328667.html

126. Qwen Chat. (2025, April 25). *Qwen Chat privacy policy.* https://chat.qwen.ai/legal-agreement/privacy-policy?spm=a2ty_o01.29997169.0.0.3d4d5171kJY995

127. World Internet Conference. (2023, November 9). *Sovereignty in Cyberspace: Theory and Practice* (Version 4.0). https://cn.wicinternet.org/2023-11/09/content_36955448.htm

128. Cici. (2024, October 30). *Cici privacy policy.* https://www.ciciai.com/legal/privacy/en

129. Talkie. (2025, July 31). *Talkie privacy policy.* https://www.talkie-ai.com/static/privacy; Monica. (2024, June 14). *Monica privacy policy.* https://www.monica.im/privacy

130. Manus. (2025, September 1). *Manus privacy policy.* https://manus.im/privacy

131. Monica. (2024, June 14). *Monica privacy policy.* https://www.monica.im/privacy

132. Cici. (2024, October 30). *Cici privacy policy.* https://www.ciciai.com/legal/privacy/en

133. Qwen Chat. (2025, April 25). *Qwen Chat privacy policy.* https://chat.qwen.ai/legal-agreement/privacy-policy?spm=a2ty_o01.29997169.0.0.3d4d5171kJY995

134. Manus. (2025, September 1). *Manus privacy policy.* https://manus.im/privacy

135. Cici. (2024, October 30). *Cici privacy policy.* https://www.ciciai.com/legal/privacy/en

136. Kokas, A. (2022). *Trafficking data: How China is winning the battle for digital sovereignty.* Oxford University Press.

137. Incogni. (n.d.). *10 popular apps that collect extensive personal data on Americans are foreign-owned.* https://blog.incogni.com/popular-foreign-apps/

138. King, J., & Meinhardt, C. (2024, February). *Rethinking Privacy in the AI Era: Policy Provocations for a Data-Centric World.* Stanford University Human-Centered Artificial Intelligence. https://hai.stanford.edu/policy/white-paper-rethinking-privacy-ai-era-policy-provocations-data-centric-world

139. Cici. (2024, October 30). *Cici privacy policy.* https://www.ciciai.com/legal/privacy/en

140. Monica. (2024, June 14). *Monica privacy policy.* https://www.monica.im/privacy

141. Manus. (2025, September 1). *Manus privacy policy.* https://manus.im/privacy

142. Croes, E. A. J., Antheunis, M. L., van der Lee, C., & de Wit, J. M. S. (2024). *Digital Confessions: The Willingness to Disclose Intimate Information to a Chatbot and Its Impact on Emotional Well-Being.* Interacting with Computers, 36(5), 279–292. https://academic.oup.com/iwc/article/36/5/279/7692197

143. Gumusel, E. (2024). *A Literature Review of User Privacy Concerns in Conversational Chatbots: A Social Informatics Approach (ARIST paper). Journal of the Association for Information Science and Technology*, 76(1), 121–154. https://doi.org/10.1002/asi.24898

144. King, J., & Meinhardt, C. (2024, February). *Rethinking Privacy in the AI Era: Policy Provocations for a Data-Centric World.* Stanford University Human-Centered Artificial Intelligence. https://hai.stanford.edu/policy/white-paper-rethinking-privacy-ai-era-policy-provocations-data-centric-world

145. Kimi. (2025, October 29). *Kimi privacy policy.* https://kimi.moonshot.cn/user/agreement/userprivacy?version=v2

146. Ibid.

147. Ibid.

148. Cici. (2024, October 30). *Cici privacy policy.* https://www.ciciai.com/legal/privacy/en

149. Quark. (2025, March 25). Quark privacy policy. https://terms.alicdn.com/legal-agreement/terms/c_end_product_protocol/20230831162328667/20230831162328667.html

150. Manus. (2025, September 1). *Manus privacy policy.* https://manus.im/privacy

151. Kimi. (2025, October 29). *Kimi privacy policy.* https://kimi.moonshot.cn/user/agreement/userprivacy?version=v2

152. Doubao. (2025, October 17). *Doubao privacy policy.* https://www.doubao.com/legal/privacy

153. Ibid.

154. Manus. (2025, September 1). *Manus privacy policy.* https://manus.im/privacy

155. Cici. (2024, October 30). *Cici privacy policy.* https://www.ciciai.com/legal/privacy/en

156. Manus. (2025, September 1). *Manus privacy policy.* https://manus.im/privacy

157. Doubao. (2025, October 17). *Doubao privacy policy.* https://www.doubao.com/legal/privacy

158. Baidu. (2025, February 18). *Baidu AI Search privacy policy.* https://s.bdstatic.com/common/agreement/privacy.html

159. Selinger, E., & Hartzog, W. (2016). Obscurity and privacy. In J. C. Pitt & A. Shew (Eds.), *Spaces for the future: A companion to philosophy of technology* (pp. 119–130). Routledge.

160. Solove, D. J., & Citron, D. K. (2022). *Privacy harms. Boston University Law Review*, 102(3), 793–854.

161. Solove, D. J. (2025). *Artificial intelligence and privacy. Florida Law Review,* 77(1), 1–73. https://www.floridalawreview.com/article/129976-artificial-intelligence-and-privacy; Cofone, I. (2023). *The privacy fallacy: Harm and power in the information economy. Cambridge University Press.*

162. Solove, D. J. (2025). *Artificial intelligence and privacy. Florida Law Review*, 77(1), 1–73. https://www.floridalawreview.com/article/129976-artificial-intelligence-and-privacy

163. Bietti, E. (2020). *Consent as a free pass: Platform power and the limits of the informational turn. Pace Law Review*, 40(1), 310–398.

164. Solove, D. J. (2025). *Artificial intelligence and privacy. Florida Law Review,* 77(1), 1–73. https://www.floridalawreview.com/article/129976-artificial-intelligence-and-privacy

165. Lee, H.-P., Yang, Y.-J., von Davier, T. S., Forlizzi, J., & Das, S. (2024). *Deepfakes, phrenology, surveillance, and more! A taxonomy of AI privacy risks*. Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems. https://doi.org/10.1145/3613904.3642116

166. Solove, D. J. (2025). *On privacy and technology*. Oxford University Press.

167. Solove, D. J. (2025). *Artificial intelligence and privacy. Florida Law Review*, 77(1), 1–73. https://www.floridalawreview.com/article/129976-artificial-intelligence-and-privacy

168. Cohen, J. E. (2013). *What privacy is for. Harvard Law Review,* 126(7), 1904-1933.

169. Cadell, C. (2021, December 31). *China harvests masses of data on Western targets, documents show. The Washington Post.* https://www.washingtonpost.com/national-security/china-harvests-masses-of-data-on-western-targets-documents-show/2021/12/31/3981ce9c-538e-11ec-8927-c396fa861a71_story.html

170. Balding, C. (2020). *Chinese open source data collection, big data, and private enterprise work for state intelligence and security: The case of Shenzhen Zhenhua.* SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3691999

171. Johnson, M. (2023). *China's grand strategy for global data governance.* The Hoover Institution. https://www.hoover.org/sites/default/files/research/docs/Johnson_ChinasGrandStrategy_Web.pdf

172. Haver, Z. (2025, June 17). *Artificial eyes: Generative AI in China's military intelligence* (Insikt Group Report). Insikt Group. https://assets.recordedfuture.com/insikt-report-pdfs/2025/ta-cn-2025-0617.pdf

173. Ibid.

174. ARTICLE 19. (2025, June). *Going global: China's transnational repression of protesters worldwide*. https://www.article19.org/wp-content/uploads/2025/06/Right-to-Protest-China-TNR_EN.pdf

175. King, J., & Meinhardt, C. (2024, February). *Rethinking Privacy in the AI Era: Policy Provocations for a Data-Centric World.* Stanford University Human-Centered Artificial Intelligence. https://hai.stanford.edu/policy/white-paper-rethinking-privacy-ai-era-policy-provocations-data-centric-world

176. Sloan, R. H., & Warner, R. (2017). *Relational privacy: Surveillance, common knowledge, and coordination. University of St. Thomas Journal of Law & Public Policy*, 11(1), 1–35. Available at: https://doi.org/10.2139/ssrn.2864663; Viljoen, S. (2020). *A relational theory of data governance. Yale Law Journal.* Advance online publication. https://doi.org/10.2139/ssrn.3727562

177. Kokas, A. (2022). *Trafficking data: How China is winning the battle for digital sovereignty.* Oxford University Press.

178. Ibid.

179. Cadwalladr, C., & Graham-Harrison, E. (2018, March 17). *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian.* https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

180. Balding, C. (2020). *Chinese open source data collection, big data, and private enterprise work for state intelligence and security: The case of Shenzhen Zhenhua.* SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3691999

181. 王宏恩 . (2025, April 24). 當開放資料被拿來模擬整個國家 . 思想坦克 . https://voicettank.org/20250424-1/

182. Hoffman, S., Hoja, T., Lau, Y., & Lee, L. M.-C. (2024, May 2). *Truth and reality with Chinese characteristics: The building blocks of the propaganda system enabling CCP information campaigns*. Australian Strategic Policy Institute. https://www.aspi.org.au/report/truth-and-reality-chinese-characteristics/

183. Marcellino, W., Beauchamp-Mustafaga, N., Kerrigan, A., Chao, L. N., & Smith, J. (2023, September). *The rise of generative AI and the coming era of social media manipulation 3.0: Next-generation Chinese astroturfing and coping with ubiquitous AI* (Perspectives Paper No. PEA2679-1). The RAND Corporation. https://www.rand.org/pubs/perspectives/PEA2679-1.html

184. Ibid.

185. West, D. M. (2023, May 3). *How AI will transform the 2024 elections*. Brookings Institution. https://www.brookings.edu/articles/how-ai-will-transform-the-2024-elections/

186. Lange, L. (2024, November 21). *Decoding China's AI-powered "algorithmic cognitive warfare"* [White paper]. Special Competitive Studies Project. https://www.scsp.ai/resource/decoding-chinas-ai-powered-algorithmic-cognitive-warfare/

187. 陈昌孝 , 李浩 , 晁帅 , 冯明月 , & 杨延飞 . (2023). 算法认知战的致效机理与关键技术探析 [Mechanisms and key technologies of algorithmic cognitive warfare]. 信息安全与通信保密 , (8), 71–82. [In Chinese].

188. Lange, L. (2024, November 21). *Decoding China's AI-powered "algorithmic cognitive warfare"* [White paper]. Special Competitive Studies Project. https://www.scsp.ai/resource/decoding-chinas-ai-powered-algorithmic-cognitive-warfare/

189. Vanderbilt Institute of National Security. (2025). *The GoLaxy Documents: Inside one Chinese company's AI-driven influence machine*. Vanderbilt University. https://www.vanderbilt.edu/national-security/wicked-problems-lab/golaxy/

190. Goldstein, B. J., & Benson, B. V. (2025, August 5). *The era of A.I. propaganda has arrived, and America must act.* The New York Times. https://www.nytimes.com/2025/08/05/opinion/china-ai-propaganda.html

191. Ministry of Digital Affairs, Taiwan. (2025, September 24). *Cybersecurity Management Act [資通安全管理法]*. https://law.moda.gov.tw/LawContent.aspx?id=FL088622

192. Administration for Cyber Security, Ministry of Digital Affairs, Taiwan. (n.d.). *FAQs on the Cybersecurity Management Act [資安法常見問題].* https://moda.gov.tw/ACS/laws/faq/28/646

193. Ministry of Digital Affairs, Taiwan. (2025, September 24). *Cybersecurity Management Act [資通安全管理法]*. https://law.moda.gov.tw/LawContent.aspx?id=FL088622

194. Lawtrace. (2025, August 29). *Cybersecurity Management Act [資通安全管理法]* (2025 version). https://lawtrace.tw/law/show/02823?version=02823:2025-08-29

195. Cassidy, S. B., Fein, A., Wagner, M., & Burnette, R. (2025, September 29). *First order issued under the Federal Acquisition Supply Chain Security Act, triggering immediate requirements on contractors.* Inside Government Contracts. https://www.insidegovernmentcontracts.com/2025/09/first-order-issued-under-the-federal-acquisition-supply-chain-security-act-triggering-immediate-requirements-on-contractors/; Robinson, A. B., Hastings, A. B., & Ahdieh, E. (2025, October 1). *FASC issues first Federal Acquisition Supply Chain Security Act exclusion order: Implications for federal contractors and ICTS supply chains*. Morgan Lewis & Bockius LLP. https://www.morganlewis.com/pubs/2025/10/fasc-issues-first-fascsa-exclusion-order-implications-for-federal-contractors-and-icts-supply-chains

196. Select Committee on the Chinese Communist Party. (2025, June 25). *China Select Committee launches AI campaign with legislation to block CCP-linked AI from U.S. government use.* https://selectcommitteeontheccp.house.gov/media/press-releases/china-select-committee-launches-ai-campaign-with-legislation-to-block-ccp-linked-ai-from-us-government-use

197. 中央社 . (2025, May 10). 數發部推動資安職能轉換計畫 充實公部門人才庫 . https://www.cna.com.tw/news/ait/202505100032.aspx

198. 中央社 . (2023, October 20). 唐鳳：不公布危害國家資安產品名單 避免廠商洗產地 . https://www.cna.com.tw/news/aipl/202310200103.aspx

199. Ministry of Digital Affairs, Taiwan. (2022, November 28). *Principles on restricting use of products that endanger national cybersecurity by government agencies [各機關對危害國家資通安全產品限制使用原則]*. https://law.moda.gov.tw/LawContent.aspx?id=FL091047

200. National Communications Commission. (2012). *Tongchuan-Tongxun No. 10141050780 Notice [通傳通訊字第 10141050780 號公告]*; Ministry of Health and Welfare. (2022). *Wei-Bu-Jiu No. 1111360009 Notice [衛部救字第 1111360009 號公告]*; Ministry of Labor. (2023). *Laodong-Faguan No. 1120500319A Notice [勞動發管字第 1120500319A 號公告].*

201. Ministry of Justice. (2025, Nov 11). *Personal Data Protection Act* [個人資料保護法], art. 21. https://law.moj.gov.tw/LawClass/LawSearchContent.aspx?pcode=I0050021&norge=21

202. Personal Information Protection Commission. (2025, February 18). *DeepSeek temporarily suspends its application service in Korea* [Korea notice]. https://www.pipc.go.kr/eng/user/ltn/new/noticeDetail.do

203. Personal Information Protection Commission. (2025, April 30). *The PIPC announces status examination results of DeepSeek service.* https://www.pipc.go.kr/eng/user/ltn/new/noticeDetail.do; Reuters. (2025, April 30). *DeepSeek available to download again in South Korea after suspension.* https://www.reuters.com/sustainability/boards-policy-regulation/deepseek-available-download-again-south-korea-after-suspension-2025-04-28/

204. European Union. (2016). *General Data Protection Regulation (GDPR), Article 58: Powers.* Regulation (EU) 2016/679 of the European Parliament and of the Council. Official Journal of the European Union, L119, 1–88. Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj

205. European Union. (2022). *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), Articles 51 & 82*. Official Journal of the European Union, L277, 1–102. https://eur-lex.europa.eu/eli/reg/2022/2065/oj

206. Berlin Commissioner for Data Protection and Freedom of Information. (2025, June 27). *Press release: Berlin data protection commissioner reports AI app DeepSeek in Germany to Apple and Google as illegal content* [Press release]. https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2025/20250627-BlnBDI-Press-Release_DeepSeek.pdf

207. Christakis, T. (2025, September 25). *From transfers to takedowns: Can Article 16 DSA police GDPR violations? European Law Blog.* https://www.europeanlawblog.eu/pub/hn5byrag/release/2

208. United States. (2024, April 17). *21st Century Peace through Strength Act, H.R. 8038, 118th Cong.* (2023-2024 session). https://www.congress.gov/bill/118th-congress/house-bill/8038/all-info

209. Swire, P., & Sacks, S. (2025). *Personal data as a dual-use technology: Critically assessing the new alliance of privacy and national security. Virginia Journal of International Law*, 1–71. SSRN. https://doi.org/10.2139/ssrn.5683285

210. Executive Order No. 14,117, 89 Fed. Reg. 15421 (Mar. 1, 2024).

211. United States. (2024). *Making Emergency Supplemental Appropriations for the Fiscal Year ending September 30, 2024, and for other purposes*, H.R. 815, 118th Cong., Div. I. https://www.congress.gov/bill/118th-congress/house-bill/815

212. Chander, A., & Schwartz, P. M. (2024). *The President's authority over cross-border data flows. University of Pennsylvania Law Review*, 172(7), 1989–2052. https://doi.org/10.58112/uplr.172-7.7

213. *Marland v. Trump*, 498 F. Supp. 3d 624 (E.D. Pa. 2020).

214. Executive Order No. 13,873, 84 Fed. Reg. 22689 (May 17, 2019).

215. U.S. Department of Justice. (2024). *Fact sheet: Justice Department issues final rule to address urgent national security risks posed by access to U.S. sensitive personal and government-related data from countries of concern and covered persons.* https://www.justice.gov/archives/opa/media/1382526/dl

216. U.S. Department of the Treasury. (n.d.). *The Committee on Foreign Investment in the United States (CFIUS).* https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius

217. Foreign Investment Risk Review Modernization Act of 2018, Pub. L. No. 115–232, § 1702(c)(5), 132 Stat. 2174 (2018).

218. Regarding the Acquisition of Musical.ly by ByteDance Ltd., 85 Fed. Reg. 51297 (Aug. 14, 2020).

219. Making Emergency Supplemental Appropriations for the Fiscal Year Ending September 30, 2024, and for Other Purposes, H.R. 815, 118th Cong. div. I (2024).

Research Institute for **Democracy**, **Society**, and **Emerging Technology**