FEBRUARY 2023

Data Matters:

The United States and China and Approaches to Data Governance and Cybersecurity

A Joint Report by
the **Institute for China-America Studies** and the **Grandview Institution**

ICAS
Institute for China-America Studies

国观智库
GRANDVIEW INSTITUTION

About the Report

This report, *Data Matters: The United States and China and Approaches to Data Governance and Cybersecurity*, is a joint report produced between experts at the Institute for China-America Studies and Grandview Institution; two independent think tanks housed in Washington, DC, United States and Beijing, China, respectively.

This report collects and analyzes the currently-existing tools and approaches to data governance and cybersecurity in the United States, China, as well as in global institutions, with the end goal of evaluating their efficiencies, sufficiencies, needed areas of attention, and expected upcoming areas of concern.

The expert participants from both instutites anticipate that the resulting report, published by both parties, spreads awareness of the importance of data governance in this rapidly-expanding, seemingly ever-complicated world, with the hope that governing leaders can discover ways to work together to address this challenging and borderless issue.

Cover Image: Getty Images, Royalty-Free

Institute for China-America Studies
1919 M St. NW Suite 310
Washington, DC 20036
(202) 968-0595 | www.chinaus-icas.org

Grandview Institution
3 Nanliuxiang St, Xicheng District,
Beijing, China 10005220
(+86) 010-6215-8609 | www.grandview.cn

Acknowledgements

The writers and researchers of this report would like to acknowledge the support recieved by various fellow researchers, interns, copyeditors, and designers whose support led to the successful production of this joint report.

About the Institutes

The Institute for China-America Studies is an independent think tank in Washington D.C. ICAS focuses on the evolving dynamics in the U.S.-China relationship to promote greater collaboration and mutual understanding through sincere exchanges of fresh ideas, objective policy-oriented research, and fair assessments of this critical bilateral relationship. Our research covers China-U.S. strategic relations, maritime security, economics, trade and technology relations, climate change and environment policy, global governance, and other issues central to the bilateral relationship. Ultimately, we aim to provide a window into the worldviews of both the United States and China, and thereby serve as a vehicle to promote greater understanding between these two countries and societies.

ICAS is a 501(c)3 nonprofit organization.

The Grandview Institution, founded in 2013, is an indepndent think tank housed in Beijing, China that is committed to China's security, stability and sustainable development, the dialogue between China and other countries as well as the peace and stability in the region and the world at large. While adopting the research guidelines of "objective, insightful, forward-looking and practical" based on comprehensive and accurate data, rigorous and profound analysis, authoritative and practical policy recommendations, Grandview Institution is devoted to providing research support for high-level decision-making of the government and enterprises. Grandview Institution adheres to the philosophy of "putting knowledge into practice, forging ahead steadily" and covers a wide array of areas of study, with extensive international resources and rich experience in international cooperation.

Contents

BOXES & TABLES

Executive Summary

Data is the lifeblood of the digital economy. It is also an arena of competitive maneuvering as both China and the United States seek to gain a leg-up in key data-enabled industries that will define the Fourth Industrial Revolution. President Xi Jinping has spoken of the profound changes in production processes, lifestyles and social governance methods being introduced by the revolution in data, and has emphasized the need to deepen the integration of Internet, Big Data and artificial intelligence with the real economy. For his part, U.S. National Security Advisor Jake Sullivan has alluded to data-enabled technologies as a "force multiplier" technology that will be particularly important over the coming decade. Based on the imperative to reap the benefits of digitization, both China and the United States have approached the digital frontier ambitiously. They have also approached this frontier differently. On the "3S" factors — sovereignty, supervision, and security — the are key to unlocking and securing the value of data, the approaches of China and the U.S. bear far greater dissimilarity than similarity.

China is unique in its farsighted treatment of data as a standalone "factor of production." The approach to data governance and cybersecurity has been top-down and state-driven. It is also comprehensive and aims to strike a delicate balance between the at-times competing considerations of security, privacy, inclusion, and commerce. In the area of privacy and personal information protection, the approach has been prescriptive. While most non-personal data is more-or-less allowed to freely cross borders, personal data can only flow freely across borders if the destination State is deemed to possess a comparable data protection regime with in-built safeguards. The security assessment through which such data must pass, particularly with regard to sensitive and other 'important data', is also wide-ranging and stringent (although not targeted at any particular adversary country, as such). The overall goal of the central leadership on data governance and cybersecurity is to chart out the long-term parameters of a deep, liquid and open marketplace where data elements can be traded seamlessly on the basis of efficiency and trust at home and across borders while guarding against is misuse, abuse or weaponization against the state.

The United States' approach to data governance, by comparison, has been far more *laissez-faire* and private sector led. On the one hand, the U.S.' regime is fiercely protective of the right to unimpeded flows — including unimpeded cross-border flows — of data. The stance on digital market access is aggressive and the nature of regulation light-touch. Aside from narrow security and law enforcement exceptions, such as the denial of transfer of sensitive data to foreign adversaries as well as unconditional access to the

data of U.S. jurisdictional subjects that maybe stored overseas, data is allowed to move unencumbered. No material distinction is made between the handling of personal and non-personal data. On the other hand, the country lacks a comprehensive data protection and privacy regime at the national level. A “patchwork” of federal and state laws exists, which — accompanied by U.S. Federal trade Commission rulings, industry-specific privacy obligations, and agency-level data protection standards — create an entanglement of data-related rules nationwide.

The differing vision, and approaches, to data governance and cybersecurity in China and the United States has stymied the development of cross-border data flow rules at the multilateral level. Until greater harmony in domestic regulatory frameworks is achieved, especially in their respective security and privacy frameworks, the effort to inscribe liberalized cross-border digital trade rules will remain a difficult proposition at the global level. In this context, regionalization is becoming the less-than-ideal alternative. Regional frameworks such as the Digital Economy Partnership Agreement (DEPA) and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) are gradually establishing themselves as the *de facto* ceilings in terms of rule-setting on cross-border data governance. Premised on this development, the United States and China could explore potential opportunities for collaboration in the field of cross-border data flows via third party frameworks — although it is important to point out that it will not be easy for either party to overcome the many barriers and find ways to align their approaches even on parallel platforms.

The same is true with the case of (lack of) cybersecurity cooperation. In recent years, cybersecurity has become an increasingly important component of data governance. Triggered by frequent ransomware attacks, data leakages and other security incidents, data is increasingly affecting social stability, economic development and national security directly. Organizing a global consensus around core cybersecurity rules has been hard to come by however, and the various proposals and initiatives that have been floated are typically couched in voluntary, non-binding terms. Global rulemaking on cybersecurity will, willy-nilly, have to evolve via a patchwork of rules and standards that are enforced nationally — or, at best, regionally. The overarching hope remains that, as with the case with cross-border data flows, a convergence of cybersecurity norms among the large digital ecosystems can be realized. And that in the absence of such a convergence, a rudimentary coexistence between these ecosystems could at minimum be fashioned.

Paving the way for purpose-fit data governance rules and norms that address the digital policy challenge, both at the U.S.-China level and at the global level, will remain a challenging endeavor for the foreseeable future. Given the profound importance of data to 21st century lifestyles and social, industrial and economic processes however, this search for convergence in global, regional and bilateral governance rules and norms must proceed with wisdom and determination.

CHAPTER I

Data Flows, Data Governance and Cybersecurity: Sizing Up the Challenge

In a world of volatile global commodity prices, high core inflation, and weakened economic growth, there are also bright spots to cheer one's confidence in the future — the digital economy being a case in kind.

As major global economies race to build a digital economy driven by a series of innovations such as 5G, artificial intelligence (AI), cloud computing and the Internet of Things (IoT), the digital frontier is an arena of both opportunity and challenge. The size of the global market constituted of new digital technologies is expected to reach trillions of dollars by 2025 and the growth potential of this market is enormous. As the world's top two economies, both the United States and China are reluctant to miss the digital economy tide, and each has rapidly promoted the digitization of its own economy as well as of the international economy. China has placed the development of the digital economy at the heart of its "Dual Circulation Economy" vision, while the United States has emphasized digital trade as a core component of its new Indo-Pacific Economic Framework (IPEF).

Based on the digitization of their economies, China and the United States have each formulated a bold vision. To turn their respective visions into reality however, data governance and cybersecurity are unavoidable issues that need to be grappled with. The digital economy drives global development, while data is responsible for driving the digital economy. Data governance and cybersecurity are based on the basic element of data and are essential to carrying out planning management as well as coordination and cooperation to ensure the safe and orderly operation of data.

Object and Scope of Data Governance and Cybersecurity Research

The concept of data governance first cropped up during the age of the "information explosion" in the 1990s. According to the definition of the International Organization for Standardization (ISO), data governance refers to the collection of activities that exercise power and control over the management of data assets, including planning, regulation and execution. It aims to lay the foundation and empower the digital transformation of an entity or organization, help maximize the value of data

assets, and expand the imagination for digital applications. Some studies also argue that data is an asset that generates value through services, and data governance is the evaluation, guidance and control implemented by the governance team in the process of generating value from data.

The value of data lies in its flow and convergence, which is realized through data origination, exchange and transaction. However, if flow and aggregation only follow market rules, it will lead to data monopoly within national markets and potentially data hegemony on a global scale. Both scenarios will lead to network security problems. Data monopoly often leads to data abuse as well as problems such as “profiteering on big data” (big data-enabled price discrimination) and “inducing push” and even illegal collection of personal data. Therefore, with a view to sorting through the problems existing in data flow, it is important to standardize cybersecurity and promote the regulation and security of data use.

Global data governance and cybersecurity are new frontiers of regulation with few existing templates. As such, paradigm-building is open-ended. As the driving force of the digital economy, data is generated on a large scale; indeed, with the advancement of the IoT and AI, new data is also generated every moment and the quantity of data is increasing exponentially. To cope with the requirements, existing solutions for data storage, analysis, and usage need to be iterated over time. Therefore, data governance and cybersecurity should not only be based on existing ground realities but must also look to the future and establish an open framework that allows for the shaping of data market rules and improved data governance.

A concept image of a data protection concept.
Source: Getty Images, Royalty-Free

Research Purpose of Data Governance and Cybersecurity

Data governance and cybersecurity, which is the purposeful practice of planning, monitoring, executing and managing data assets, aims to unlock as well as protect the value of data. In order to achieve this goal, it is necessary to pay attention to data's "3S" factors, namely Sovereignty, Supervision and Security.

When data is regarded as a strategic resource by a country, it gets endowed not only with a broad space for development and growth but is also introduced to a new field: which is, how to effectively divide the ownership of data that travels across borders between countries - namely the issue of data sovereignty. Data sovereignty is the natural extension of national sovereignty in network applications. Every state enjoys the right to protect, develop and utilize its own data resources, including its own data production, processing, storage, circulation, exchange and transmission free from interference by other countries. In this vein, the state also enjoys the power to regulate the output of domestic data and the data input overseas.

The regulation of data is an important part of a nation's sovereign interests, reflecting the ability to manage, control and analyze data. The basis of prudent regulation is assignment and confirmation of (data) ownership. Domestically, it is necessary to clarify whether the ownership, use, and benefit rights of data belong to individuals, platforms, or are public goods. Data governance requires the extensive participation of the government, enterprises, and individuals. Though the interests of the three parties are all concentrated in the data field, their respective interests with regard to the governance issue however are varied. The entry point for government regarding data is its regulatory and oversight power while the focus of platform entities is on promoting the free flow of information elements. As for individuals, they aim to enjoy the consumptive benefits of data while also staying focused on protecting the security and privacy of their own data.

In this triangular model, the role of data governance is to release and protect the value of data by covering all processes and states across the entire data cycle, and with the aim to ensure the balanced needs of all parties as much as possible. Currently, the consensus in this regard is to promote a balance between the free flow of data and the protection of personal data rights under the premise of ensuring effective regulation. In other words, it is an adjustment between efficiency and fairness.

The current system of cloud-based data poses a further challenge to data governance because both cloud computing and cloud storage separate data ownership and data control from each other. Users can access the data stored in the cloud at any time while the control over the data is in the hands of service providers who provide cloud storage services. In the context of cross-border data flow, all parties involved will claim data rights, resulting in overlap and even conflict of data sovereignty claims. Dividing these claims according to a model of GDD (Gross Domestic Data) — on lines similar to GDP

A Hong Kong skyline with a smart city network overlay at night.
Source: Getty Images, Royalty-Free

— would seem to perhaps be the most feasible method of data supervision at the time of drawing up rules in its regard.

In recent years, cybersecurity has become an increasingly important component of data governance too. The cross-border flow of data has brought many challenges to governance and security, with the latter being a completely new field compared to traditional concepts of security. In this era of the digital economy, data has become a basic and strategic resource as well as a new production factor nationally. Accompanied by escalation of data security risks, frequent ransomware attacks, data leakages and other security incidents, data is increasingly affecting social stability, economic development and national security directly. Therefore, all sectors of society must pay close attention to these new technologies as well as its applications, such as user portrait and algorithm recommendation, and all of these also strongly reflect the problems of information abuse and security loopholes in related products and services. How to promote the reasonable and effective use of data under the premise of ensuring security and privacy; how to implement data security in a systematic and specific way; and how to use key technologies to meet the security requirements of full data application scenarios require new ways of thinking and constitute new challenges to governance practices in the area of data security.

Research Methods on Data Governance and Cybersecurity

Since the digital economy is regarded as a key strategic field by both China and the United States, the two countries have in recent years successively issued a series of policy as well as legal documents aimed at the “3S” factors. As a reflection of the public will, these documents constitute a basic text for analyzing Beijing and Washington approaches towards data governance and cybersecurity. Through research on approaches towards policy formulation as well as an assessment of the key players

and departments involved in the decision-making process, researchers can glean a clearer understanding of the context, focus areas, and differing approached towards data governance and cybersecurity in both China and the United States.

Policy documents and legal documents constitute authoritative domestic texts on data governance and cybersecurity. This is also the case with relevant bilateral and multilateral trade agreements signed by the two countries with third parties. The digital economy has become an important part of international trade. At this time, there are on-going efforts at the regional and multilateral level to ensure cross-border data trade and strengthen coordinated regulations. The latest attempt was in mid-June 2022, when both China and the United States participated in the 12th WTO Ministerial Conference. At the meeting, participating states discussed the 'Work Programme on Electronic Commerce', and all parties agreed to maintain the current practice of not imposing tariffs on electronic data transmission until the 13th ministerial conference which is slated to be held in February 2024.[1]

Relevant Policies and Suggestions

Both China and the United States have adopted various methods of varying strictness with regard to data governance and the protection of data. In an era of geopolitical competition, like two engineering vehicles digging tunnels at different points, there appears to be very little or no coordination between Beijing and Washington in the data governance field. Coupled with the fact that the European Union, which has considerable sway in the field of data governance is carving out a third passageway, this kind of fragmentation makes the prospect for global data governance and cybersecurity coordination very challenging.

As a result, the primary purpose, and outcome, of this study is to understand and perceive the differences in policies and regulations on data governance and cybersecurity between China and the United States, and squarely face up to these differences. An in-depth understanding of data governance and cybersecurity policies in the two countries is the starting point of this research project. To realize the true value of cross-border data flows, it is imperative to form a unified data standard.

An intermediate purpose, and outcome, of this study is to provide a framework for managing related disagreements. Internationally, multi-track and parallel data governance and cybersecurity policies may easily lead to policy misinterpretation and result in decoupling and even confrontation at the digital frontier. By understanding the root causes of such disagreement, it is possible to control its intensity more effectively and reduce the cost of data resources-related contention.

An aspirational focus of this study, finally, is to explore potential opportunities for Sino-U.S. collaboration in the fields of data governance and cybersecurity — especially via third

party frameworks. In the digital age, both China and the United States face challenges in data governance and cybersecurity and with the creeping retreat of globalization, regionalization has become the less-than-ideal alternative. In terms of data governance, regional frameworks such as the Digital Economy Partnership Agreement (DEPA), the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), and the on-going Indo-Pacific Economic Framework (IPEF) negotiations are gradually establishing themselves as the *de facto* ceilings in terms of rule-setting on cross-border data governance. As such, these agreements could serve as realistic channels for fostering greater alignment among the competing Chinese and American frameworks on data governance and cybersecurity. It bears noting though that even premised on this point of view, it will not be easy for China and the United States to overcome their many barriers and find ways to cooperate on the same or parallel platforms.

CHAPTER II

China's and the United States' Approaches to Data Governance and Cybersecurity

- THE CASE OF CHINA -

Introduction

China's digital development has been nothing short of astonishing. From digital infrastructure buildout to the size of the digital economy to the scale of data generation, the state of China's national digitization has grown in leaps and bounds over the past decade.[2]

In terms of digital infrastructure buildout, China ended 2021 with 1,425,000 5G base stations, 60% of the global total, and 455 million 5G users. More than 300 cities have installed gigabit-level optical fiber, and 34.6 million users have access to gigabit-speed fixed broadband. As for total number of internet users, it has grown from 564 million in 2012 to 772 million in 2017 to 1.032 billion in 2021 — an internet penetration rate of 73%. The digital economy has been just as rip-roaring. Total annual value, both in terms of ICT hardware and equipment manufacturing as well as software development and revenues, grew from RMB 27.2 trillion accounting for 32.9% of GDP in 2017 to RMB 45.5 trillion accounting for 39.8% of GDP in 2021. And at the foundation of this remarkable digital development has been the explosively growing nature of data generation. Raw data output in the Chinese cybersphere jumped from 2.3 zetabytes (ZB) in 2017 to 6.6ZB at the end of 2021, constituting 9.9% of total data worldwide. Revenue in the big data industry has nearly tripled too, to RMB 1.3 trillion. Data generation, and more broadly the data infrastructure system, is woven into the fabric of the Chinese economy as a new "factor of production" today.

The sweep of China's basic approach to data governance and cybersecurity that underpins its data infrastructure system has been equally breathtaking too. Much like the deep, liquid and open capital markets has been a hallmark of America's financial preeminence, China's approach to the cybersphere is geared towards gradually fostering a similarly deep, liquid and open data elements marketplace. Data is more than just the lifeblood of the digital economy; it is a full-fledged new "factor of production," joining land, labor, capital and technology.[3] And with 1.4 billion potential digital consumers, China's ambition to become a "cyber superpower" is well within reach.

The political framework of China's data elements market is composed of four pillars.[4]

1. **Establishment of a modern data property rights system,** with the goal of promoting the orderly separation of data holding rights and data use rights and thereby facilitate the efficient market-based circulation of data. Within this rights-based context, the differentiated, graded, and authorized use of public, private and enterprise data is to be promoted.

2. **Systems to enable the fair access and equal use of data elements within Chinese society,** with the goal of, both, expanding the scope of market-based allocation of data elements as well as protecting the income and livelihood of data factors that contribute their capital or labor. Large data enterprises, further, are expected to shoulder a greater share of social responsibility.

3. **Establishment of a modern data security governance system**, based on bottom-line security and a clarified red line on supervision, with the goal of creating a secure and trustworthy environment for all digital social actors.

4. **Systems to enable the circulation and trading of data elements internationally,** with the goal of promoting a trustworthy cross-border data circulation system in which the sources of data can be confirmed, the scope of use can be defined, the circulation process can be traced, and security risks can be prevented. International exchanges and participation in digital rulemaking and standards-setting bodies as well as data security, digital currencies and digital economy taxation is to be promoted too.

In a nutshell, privacy, commerce, inclusivity, and security reside at the heart of China's intertwined approach to data governance and cybersecurity. Within this matrix, considerations of security have been accorded greatest prominence, followed thereafter by detailed rules on privacy and personal information protection. With data security, data ownership and data use rules more-or-less in place (and being updated on a frequent basis), the focus of regulatory attention has now turned to the framing of data flow rules, particularly cross-border data flows rules that would promote international commerce.

Alongside, the drafting is also underway of regulations to safeguard against fintech-driven financial stability risks based on the principle of "same industry, same rules," as well as crack down on the anti-competitive business practices of Big Tech. Amendments to update the Anti-Monopoly Law's (AML) scrutiny of Big Tech's acquisition and market concentration practices have been passed by the National People's Congress Standing Committee recently (June 2022) too.[5] Separate work-streams are under way to develop rules for artificial intelligence (AI) applications, algorithmic recommendation engines, and against the propagation of deepfakes.

Legal Framework of China's Data Governance and Cybersecurity Regime

The origins and build-out of the legal framework that underpins China's data elements market and its data infrastructure system dates back to the new National Security Law (NSL) of July 1, 2015. The law introduced a sweeping concept of national security, created an enabling legal infrastructure, and repealed the original National Security Law of 1993 which had been overly focused on counterespionage. A direct link between national security and economic, cultural, and social security is articulated in Article 3 of the new NSL. A subsidiary article (Article 25) calls for the need to establish a "national network and system security safeguard system" with the objective of "achieving the security and controllability of core network and information techniques, key infrastructure, information systems in important fields and data," "punishing unlawful and criminal activity on networks," and "maintaining cyberspace sovereignty, security, and the development interests of the State." A reference to the national security review process regarding infringing foreign investment, key materials and technologies, and internet or information technology products and services is contained in Article 59.

A companion National Intelligence Law was adopted too by the Standing Committee of the 12th National People's Congress in June 2017. An Encryption Law followed in October 2019.

BOX 1: Laws and Regulations that Supposedly "Compel" Chinese Companies and Citizens to Assist in National Security and Intelligence work, as per U.S. Government

Senior U.S. national security and justice department officials have from time-to-time issued alerts and advisories claiming that China is the greatest counterintelligence threat to the United States.[11] In this overwrought view, "every Chinese citizen and company," ranging from "ostensibly private companies, graduate students and researchers" — let alone China's intelligence services and state-owned enterprises — is "compel[led]" by law to "assist in national security or intelligence work".[12] To buttress its point, a list of offending provisions in China's security and intelligence laws have been trotted out:

- **Article 35 of Data Security Law of June 2021:** "Public security organs and state security organs collecting data as necessary to lawfully preserve national security or investigate crimes shall follow relevant state provisions and complete strict approval formalities to do so, and relevant organizations and individuals shall cooperate."
- **Article 7 of National Intelligence Law of June 2017:** "Any organization or citizen shall support, assist, and cooperate with state intelligence work in accordance with the law, and maintain the secrecy of all knowledge of state intelligence work."

  On the other hand, it bears noting though that **Article 8** of the National Intelligence Law stipulates that the national intelligence service should carry out its work according to law, respect and protect rights, and safeguard the legal rights and interests of individuals and organizations.
- **Article 28 of Cybersecurity Law of November 2016:** "Network operators shall provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law."
- **Article 11 of National Security Law of July 2015:** "All citizens of the People's Republic of China…shall have the responsibility and obligation to maintain national security."

The list is neither unique nor eye-opening. All major countries have a variety of similar statutes on the books to assist law enforcement agencies in their investigations and/or safeguard digital and national security. The U.S.' CLOUD (Clarifying Overseas Use of Data) Act, for example, can compel a service provider — say Google — to hand over a user's content and metadata stored in a foreign jurisdiction without having to follow that country's privacy laws.[13] And at home, the U.S. government has coerced tech firms to hand over source code not only in civil cases filed under seal but also via clandestine rulings authorized by the secretive Foreign Intelligence Surveillance Court (FISC).[14] As for the breadth and depth of cyberespionage activities, there is no comparable tapping or surveillance operation of the likes of PRISM, the Equation Group, ECHELON, or Israel's NSO Group's Pegasus

The November 2016 Cybersecurity Law (CL) is the centerpiece of China's cyber regulation and enforcement regime.[6] The CL derives from the National Security Law. The Law is composed of 79 articles spread over seven chapters. The key highlights of this basic and overarching "fundamental law" can be subsumed under a number of heads:

- **Advocating the Principle of Cyberspace Sovereignty:** The Law champions the concept of "cyberspace sovereignty" by creating a framework to regulate the Internet within China's borders, as well as ensure the secure and controllable development of technologies to enhance cybersecurity.
- **Security Protection Obligations of Network Operators and Providers of Network Products and Services:** The Law obligates network operators to safeguard their networks against disruption, damage or unauthorized access and to prevent data leakage, theft or tampering. As for providers of network products and services, they must abide by "national standards" and ensure the security of their products. "Critical Network Equipment and Network Security Specialized Products" must undergo a higher level of accreditation.
- **Protection of Critical Information Infrastructure (CII):** The Law defines CII broadly as "infrastructure that, in the event of damage, loss of function, or data leak, might seriously endanger national security, national welfare or the livelihoods of the people, or the public interest," and mandates tough rules for CII operators and their suppliers. CII operators are also required to sign security and confidentiality agreements with suppliers when procuring network products and services.
- **Protection of Personal Information:** The Law imposes a number of data protection obligations on network operators, including the obligation to (a) not disclose, tamper with, or damage citizens' personal information that they have collected, (b) not provide citizens' personal information to others without consent, and (c) delete unlawfully collected information and amend incorrect information. Breach notification requirements are also specified.
- **Cross-Border Data Transfers of Data:** The Law obliges CII operators to store within Chinese territory "citizens' personal information and important business data" collected or generated in the course of operations. Transfers of data offshore that are necessary for operational reasons are to be subject to a security assessment.
- **Network Standardization and Interoperability:** The Law promotes the interoperability of network infrastructures and encourages enterprises, institutions, and universities to participate in the formulation of network security standards.

As a basic law, the Cybersecurity Law has a broad and overarching character by design. Two waves of implementing regulations (Measures for Cybersecurity Review) have been issued thereafter by the cybersecurity regulator, the Cyberspace Administration of China (CAC), to fine-tune the law's broad provisions. The most recent of these Measures was issued by CAC in conjunction with 12 other agencies in January 2022 and specifies, among other items, the network security risk-review factors to be considered by network platform operators that plan to list their shares abroad and which are in possession of more than one million users' personal information.[7] The risk of "core data" or "important data" being maliciously used by a foreign government is one such risk-review factor. The Measure was itself occasioned at the time (July 2021) by Didi Chuxing listing on the New York Stock Exchange, despite informal requests from Chinese officials to Didi to delay the listing and conduct an examination of network security.[8]

The Data Security Law (DSL) of June 2021 complements China's November 2016 Cybersecurity Law as the second of the three basic pillars of China's data governance regime.[9] The purpose of this 55-article law is to regulate data processing activities that could have a national security implication. The key articles of the DSL are:

- **Article 21,** which establishes a data categorization and classification protection system to govern data, depending on the importance of different types of data to the national economy, national security and public interest. The article introduced a new category of data called "national core data" (that sits hierarchically above "important data") and refers to data that are related to "national security, lifeline of the national economy, and important people's livelihood and vital public interests." A National Data Security Coordination Mechanism is tasked with coordinating the relevant agencies in this regard.

- **Article 26,** which permits the adoption of reciprocal measures against countries and regions that impose discriminatory measures against China with respect to matters such as investment and trade related to data, data development and technology use.

- **Article 27,** which requires data processing entities to comply with the data security requirements of the Multi-level Protection Scheme (MLPS) that classifies networks physically located in China according to their relative impact on national security. The Multi-level Protection Scheme was first introduced in the 2016 Cybersecurity Law.

- **Article 36,** which forbids organizations and individuals on Chinese soil from providing data stored in China to foreign judicial or law enforcement agencies without the approval of the competent Chinese authorities.

- **Articles 45 and 46,** which enumerate stiff fines for violating requirements related to the protection of "national core data" as well as violating rules related to the cross-border transfer of "important data" by CII and non-CII data processing entities.

The final pillar of China's basic data governance regime is the Personal Information Protection Law (PIPL) of August 2021.[10] It is similar to the EU's General Data Protection Regulation (GDPR), particularly in its extraterritorial reach, and focuses on protecting the personal information of individuals and organizations based on Chinese soil. The PIPL provides a legal basis for processing personal information related to cross-border transfer (i.e., where data processing activities are carried out outside the territory of China), based on a "standard contract" published by the CAC. Jurisdiction is enforced extraterritorially based on the source of the data rather than its location of storage or processing.

The PIPL enumerates a number of data protection principles that personal information handlers and data processors must abide by — ranging from lawfulness, fairness, necessity, and good faith (Article 5); purpose limitation and data minimization (Article 6); openness and transparency (Article 7); accuracy and completeness (Article 8); security and accountability (Article 9); and limited data retention (Article 19). And, relatedly, it accords various rights to "data subjects" with regard to the handling of their private information. Large-scale internet platform operators bear responsibilities which are outlined in Article 58. Finally, remedies available to individuals and organizations for a violation of the PIPL and the ensuing allocation of the burden of proof during litigation is outlined in the concluding articles.

'Much Thunder, Much Rain': China's Active Buildout of Data Governance and Cybersecurity Regulations

2021 and 2022 were busy years with regard to China's regulatory buildout of its data governance regime. A number of draft and final rules that are based on the articles of the Cybersecurity Law, the Data Security Law and the Personal Information Protection Law were released, to implement their provisions.

In early-July 2021, the General Office of the CPC Central Committee issued its Opinions on Strictly Combating the Illegal Securities Activities, which was in part triggered by the (unsanctioned) start of trading of Didi Chuxing's American Depositary Shares (ADS) on the New York Stock Exchange (NYSE) six days earlier.[15] Four days later, on July 10, 2021, the Cyberspace Administration of China (CAC) issued its Draft New Measures for Cybersecurity Review. A final version of the regulation was issued on January 4, 2022. Later, in October 2021, CAC released its Draft Data Export Security Assessment rules which, following minor revisions, was issued as a final rule on July 7, 2022.[16] The rule standardizes data export activities by data processors, particularly concerning the security assessment of "important data" and personal information of domestic users. Moreover, the aforementioned DSL and the PIPL were enacted too on June 10, 2021, and August 20, 2021, respectively.

Most notably, on November 14, 2021, CAC released a gargantuan 75-article omnibus Draft Network Data Security Management Regulation that covers the gamut from personal information protection (Chapter 3) to the security of "core data" and "important data' (Chapter 4), to the security management of cross-border data flow (Chapter 5), to the obligations of internet platform operators, including checks on anti-competitive behavior (Chapter 6), to the supervision, management and legal responsibility of data processors, network managers and state regulators (Chapters 7 and 8).[17] The Regulation is a veritable combination of the EU's General Data Protection Regulation, the Digital Markets Act and the Digital Services Act and much more, all bundled into a single regulation. A final rule has yet to be issued.[18]

China's recent breakneck pace of digital regulation might leave the impression that the leadership and senior bureaucracy focused on demonstrating its resolve to maintain the network security of important data systems and the integrity of personal information protection at home. This is not an incorrect reading; these are certainly very important considerations.

But it is also an insufficient reading. An underlying premise of the comprehensive, hierarchical and systematic classification of domestic data and network security is to also develop a more granular basis to ensure not just which (essential) data elements must be stored securely and controllably within China's jurisdiction but also to ensure that all other (non-essential) elements can be freely transferred abroad. In that sense, this classification system also doubles as a negative list system to ensure the robust and trustworthy cross-border flow of data elements, and thereby facilitate international commerce in digital goods and services.

Typically, the trigger threshold for a stricter assessment of network or data security in the various rules and regulations is linked to:

- a data processor being an "important data" handler;
- a data processor seeking to list overseas;
- the party/processor/platform operator being a provider of cloud computing services to state organs or an operator of critical infrastructure;
- the processor/platform operator being a "large-scale internet platform operator", i.e., platform operator with 100 million daily users;[1] and
- the platform operator being a user of new technologies, such as AI, Virtual Reality, and Deep Learning to carry out data processing activities.

1 *According to the Guidelines for Classification and Grading of Internet Platforms (Draft for Comment) issued by the State Administration for Market Regulation in 2021, Internet platforms were divided into super platforms, large platforms, small and medium-sized platforms based on their scale of users, business types and restrictive capacity. A super platform has no fewer than 500 million active users in China the previous year, with more than one type of platform business as its core businesses, its market value (valuation) not less than RMB 1,000 billion at the end of last year, and a super strong ability to restrict merchants from contacting consumers (users); A large platforms has no fewer than 50 million active users in China the previous year; A small and medium-sized platform has a certain number of annual active users in China. Super platform operators should conduct risk assessment at least once a year to identify various risks that may be caused by the Internet platform services they provide.*

At this time, an instructive definition of "important data" is also available. It includes, but is not limited to:

- undisclosed government affairs data, work secrets, intelligence data, and law enforcement judicial data;
- export control data, data on core technologies, design schemes, production processes and other related technologies involved in export control items, and data on scientific and technological achievements in the fields of cryptography, biology, electronic information, and artificial intelligence;
- data linked to operation of key industries and fields such as industry, energy, telecommunications, transportation, water conservancy, finance, national defense science and technology industry, customs, taxation, etc., and data on the supply chain of key system components and equipment;
- national basic data on population and health, natural resources and env., such as genes, geography, minerals, meteorology; and
- other data that may affect the security of national politics, land, military, economy, culture, society, science and technology, ecology, resources, nuclear facilities, overseas interests, biology, space, polar regions, deep seas, etc.

The definition of "important data" nevertheless remains a work in progress. Multiple government agencies tasked with determining what counts as "important data" in their own industries and sectors — be it energy, telecommunications, transportation, finance, etc. — have initiated their own drafting-related inquiries. The automotive and finance sectors are the furthest along in this process. A mature and fixed definition of "important data" might still be quite some time away. A comprehensive and clear-cut and definition of "core data" might be even further away.

China's Data Governance Regime: A Preliminary Conclusion

China is unique in its (farsighted) treatment of data as a standalone "factor of production." The approach to data governance and cybersecurity has been top-down and state-driven in a concerted fashion. The approach is also comprehensive and aims to strike a delicate balance between the, at-times, competing considerations of security, privacy, inclusion, and commerce.

The goal of the central leadership is to chart out the long-term parameters of a deep, liquid and open marketplace, where data elements can be traded seamlessly on the basis of efficiency and trust while guarding against is misuse, abuse or weaponization against the state.

For all its foresightedness, the concerted state-led approach is not without its critics or share of pitfalls either. This primarily stems from the poor communication between the

regulators (including the central leadership) and the regulated. Granted, that Big Tech in China has outgrown its 'regulatory sandbox' age and warrants careful oversight. But the belated swiftness and severity of the regulatory reckoning in the digital sector has been disconcerting.[19]

The pioneering strides made in the development of its data governance and cybersecurity regime notwithstanding, there is much careful work that yet remains to be done in building-out China's national data elements market and date infrastructure system, going forward.

- THE CASE OF THE UNITED STATES -

Federal Laws

Ever since American companies began their trailblazing role in the global digital economy, the United States has vigorously promoted the free flow of data internationally as a basic first principle. Over time, emerging challenges have led U.S. regulators to set standards in various sectors to balance the industry's penchant for growth with concerns such as personal privacy, responsible content moderation, fighting disinformation and protecting national security. However, regulatory efforts have traditionally targeted particular sectors and devolved responsibility for the first level of data governance to the industry itself. Only when a data handler violates data flow rules and standards do data regulators step in and punish them. Thus, enjoying a large leeway by default, American tech giants have generally operated with a considerable degree of freedom — and impunity — in the course of controlling and processing consumer data.

Where U.S. regulators have set standards in commercial data flows, it has tended to be limited to specific sectors or types of data. For example, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 led to broad privacy standards pertaining to storage and access of medical records. The Federal Trade Commission (FTC) also began regulating financial data comparatively strictly in line with the requirements of the Gramm-Leach-Bliley Act (GLBA) of 1999 which established rules on how financial institutions must store and protect customer information. The FTC enforces other federal level frameworks in other sectors but mostly through *post-facto* punitive enforcement measures. Take, for example, the FTC's lawsuit against ad-tech firm Kochava for its alleged sale of precise geolocation data, in violation of the standard to protect customers' sensitive data from exposure.[20] The Federal Communications Commission (FCC) enjoys authority similar to the FTC in the realm of internet service provision, with the power to penalize ISPs for improperly managing customers' personal information.

Aside from these sectoral regulatory measures which address how data handlers should secure customers' personal information (mostly extending from earlier laws passed in the 1990s), commercial data at the federal level has recently been affected by new

restrictions which prioritize national security over a pure *laissez-faire* approach. While industry stakeholders and government have been in agreement on the need for a free and level playing field for much of the past two decades, the growth of sophisticated digital sector rival powers such as China has led to the clamoring for new data flow rules in sensitive sectors like science and emerging technology.

For example, since 2018 "software" and "big data" have been designated as falling under the umbrella of export controls. This means that no sensitive scientific or technological data can be transferred to servers outside of the United States without an export license from the Department of Commerce's Bureau of Industry and Security. The Foreign Investment Risk Review Modernization Act (FIRRMA) of 2018 additionally designates foreign acquisitions and investments in "critical and sensitive data" as subject to a security review. Another move by the federal government away from the *laissez faire* approach came with the 2018 Clarifying Lawful Overseas Use of Data (CLOUD) Act, which allowed law enforcement to access commercial data of U.S.-based communications service providers (CSPs) via warrant or subpoena regardless of whether that data is stored on a server outside the United States.

Industry stakeholders are at this time quite ambivalent over how to balance open data flows with growing concerns over consumer privacy and national security. Several stakeholder proposals,[21] or at least articulations of broad principles,[22] share common themes in how they want their data to be regulated: transparency from companies in how data is being used; customer ability to opt-out of data collection; data security notification requirements; and centrality of the FTC in enforcement.

Despite this growing sensitivity to consumer privacy, Big Tech giants still continue to champion legislation that amount to a denial of a reasonable standard of privacy. One litmus test of industry views on regulating their data collection and use can be seen in their variable support of data privacy laws in California and Virginia. California's law, which somewhat shadows the European Union's strict General Data Protection Regulation (GDPR), grants individuals a right to sue companies for data breaches, ensures an easy way to opt-out of all data collection, and creates a new state agency to enforce these measures. Amazon, Microsoft, and Uber all made large contributions to groups lobbying against the law's passage.[23] Virginia's law, on the other hand, was originally authored by Microsoft with input from Amazon and does not include a private right to sue, preserves a manual opt-out approach, and grants enforcement powers only to the state attorney general.[24] While industry stakeholders are not completely united around weaker legislation (with firms like DuckDuckGo, Yelp, and Spotify supporting California's bill), the biggest players' support for Virginia's law has carried a great deal of weight and most state-level data laws that are in the drafting process mirror Virginia's law rather than California's (see section below on 'State Laws').[25]

America's approach to cross-border commercial data flows will continue in the coming years to be informed by mounting tensions between a historically *laissez-faire* predilection

and coping with the emerging global challenges which occasion more resilience and security-linked government action. While industry stakeholders have promoted legislation that cedes autonomy in a few areas, these appeasements were largely born out of a desire to pre-empt more comprehensive and stricter legislation. While the world of data is no longer monopolized by U.S. companies, the largest stakeholders with significant opportunities to profit from free flows of data are still in favor of an open market, even if that free market leaves them vulnerable to foreign players and popular scrutiny. Nevertheless, while the overall model of regulating commercial data through industry-informed standards and primarily punitive enforcement is likely here to stay, the expansion of the FTC's remit and fervor in cross-border cases is likely to amplify as more and more Americans' data circulate on servers that are physically beyond the reach of U.S. jurisdiction.

Without a comprehensive legislation or legal framework at the federal level, the United States is usually said to have a "patchwork" approach to data protection and privacy laws.[26] Existing federal legislations often focus on specific actors (e.g., government agencies or specific industries) or specific types of data (e.g., financial data or children's online data). In addition, a limited number of states have enacted comprehensive state legislation on data protection, but there is no sign that such state-level legislation will be enacted in all or most U.S. jurisdictions.

That said, there is a head of steam gradually building up on Capitol Hill with regard to passing comprehensive privacy legislation at the federal level. Members of Congress have spent a good deal of time devising federal privacy legislation, and the bipartisan American Data Privacy and Protection Act (ADPPA) is perhaps its best example. The ADPPA grapples with the two questions that have bogged down previous privacy bills: on whether to let private individuals enjoy the right to sue tech companies under the law; and whether a federal privacy statute should or should not override the existing state privacy regulations. Regarding the former, the ADPPA would allow individuals to sue tech companies for violations so long as they notify state and local officials at the time of filing and thereafter wait two years to enable remedial measures to be put in place. This could provide the company or companies breathing room to modify the relevant harmful practices. Regarding the latter, the ADPPA would override only those state rules that directly conflict with the federal law, leaving the other provisions intact.

Looking back, the need for modern-age privacy laws domestically first arose in the 1970s. During that time till the 1990s, a number of laws were enacted to address specific privacy concerns — from the need to confine the government's ability in accessing sensitive information, to sector-specific regulatory needs (e.g., in the financial and in the healthcare industry). Over time, these laws have formed the basis of the patchwork of data and privacy protection domestically, either because they have been interpreted to apply to data and digitized transactions or because Congress specifically enacted later amendments to expand the scope of the laws.

TABLE 1: U.S. Information Privacy Laws Enacted in the 1970s

Background:

- The advent of the Information Age creates the need to protect information privacy.
- The Supreme Court decided to offer limited constitutional protection to information privacy, creating the need for legislative action.

Year	Legislation	Applies To...	Relevant Content
1970	Fair Credit Reporting Act[29]	Consumer credit reports and consumer reporting agencies	Consumer reporting agencies have the duty to investigate information disputed by the consumer, the duty to notify the consumer when an adverse action is taken on the basis of credit reports, and the duty to only disclose information in the credit report for purposes specified in the Act.
1974	The Family Educational Rights and Privacy Act	Educational institutions that receive federal funding	Parents have the right to inspect, review, challenge and limit disclosure of their children's educational records.
1974	The Privacy Act	U.S. government	The Act establishes requirements and guidelines for government agencies in their collection, maintenance, use and dissemination of personally identifiable data of individuals.
1978	Right to Financial Privacy Act	U.S. government	The Act limits the ability of the U.S. government to obtain an individual's financial information, and requires legal notice or the individual's written consent except in law enforcement investigations and other limited exceptions.

Summary:

- The laws primarily focus on government and public sector actors.
- These early laws have helped inform and establish some of the fundamental principles of information privacy in the United States, such as:
  - An individual should have the right to review the sensitive information that is collected, and to challenge the information's accuracy and seek amendments to the information.
  - Sensitive information should only be disclosed for specified purposes and ideally with the (written) consent of the individuals.
  - Sensitive information that is collected should expire after a reasonable amount of time.

TABLE 2: U.S. Information Privacy Laws Enacted in the 1980s and 1990s

Background:

- Deregulation of certain industries, which led to the need for additional safeguards against abuse of individual information.
- Congressional findings on the need to regulate information privacy in select fields, either as a response to specific incidents, e.g. series of abuse of public driver license data, or to rising risks and concerns, e.g. online collection of children's information.

Year	Legislation	Applies To...	Relevant Content
1984	The Cable Communications Policy Act	The cable television industry	Section 631 of the "miscellaneous provisions" stipulates that: • A cable operator should only collect personally identifiable information from consumers when such collection is necessary for providing the cable service. • A cable operator must also provide a written statement to the consumer on how such information is collected and used.
1994	Driver Privacy Protection Act	Public driving license databases	The Act prohibits the disclosure of personal information in the public driving license databases without the express consent of the individual
1996	Health Information Portability and Accountability Act	Patient health information	The US Department of Health and Human Services is authorized to establish national standards to protect sensitive patient health information and to develop privacy and security rules for such purposes.
1998	Children's Online Privacy Protection Act	Collection of children's data online	The Federal Trade Commission is instructed to develop regulations and guidelines for commercial websites and online services regarding the collection, use and disclosure of children's personal information.
1999	The Gramm-Leach-Bliley Act	Financial institutions	The bill requires relevant financial institutions to disclose their information collection and sharing policies to customers and to develop proper procedures to safeguard their customers' sensitive information

Summary:

- The early principles on safeguarding information privacy were expanded and now apply to private actors in specific industries, e.g., the cable television industry and financial institutions, in addition to government and public actors.
- In the 1990s, relevant agencies were increasingly tasked with the responsibility and authority to develop and enforce binding information privacy and security rules for specific industries.

With the rapid growth in the use and commercialization of the Internet in the 1990s, the United States has in the period since enacted a number of laws that specifically address data protection and privacy. These include:

- The **1998 Children's Online Privacy Protection Act**, which directs the Federal Trade Commission (FTC) to develop regulations and guidelines concerning the collection, use and disclosure of children's online data.
- The **E-Government Act of 2002** and the **Federal Information Security Management Act of 2002**, both of which tighten the government's responsibilities with regard to data protection and privacy in the age of electronic transmission and storage.
- The **2009 Health Information Technology for Economic and Clinical Health Act**, which amends the 1996 Health Information Portability and Accountability Act and expands the government's use of health information technology.

As previously noted, comprehensive data protection and privacy legislation has been slow to emerge at the federal level (until recently), despite multiple efforts since the 2000s. As such, the U.S. Federal Trade Commission (FTC) — the United States' primary regulator of consumer rights — has become the primary actor in protecting consumers' data protection and privacy rights. With limited exceptions,[2] the FTC has broad authority to make administrative rulings and enforce remedies against "unfair or deceptive acts or practices," including "unfair or deceptive" data protection and privacy practices. The FTC has ruled, for example, that companies are bound by their data privacy and data security promises,[27] and that a company cannot retroactively apply a materially revised privacy policy to personal data that were previously collected.[28] Furthermore, under the Gramm-Leach-Bliley Act, the FTC is responsible for enforcing its Privacy of Consumer Financial Information Rule, which regulates areas such as the use, disclosure and collection of a consumer's financial information, the privacy notice requirement, and data protection obligations.

In summary, applicable federal laws and regulations on data protection and privacy can be summarized into three categories: First, are information privacy laws enacted from the 1970s to the 1990s, which helped define the notion of "privacy" as well as the principles behind the protection of individual privacy rights, both of which were expanded to data protection and privacy subsequently. Second, are sector-specific data privacy laws in the 1990s and 2000s, which created specific obligations and responsibilities for government agencies as well as with regard to children's online data, health information, and financial information. Finally, given the lack of a comprehensive

2 I.e., common carriers, nonprofits and financial institutions. Although FTC's authority to broadly protect consumer rights does not apply to financial institutions, the FTC is responsible for enforcing its Privacy of Consumer Financial Information Rule (Privacy Rule) under the Gramm-Leach-Bliley Act and thus has authority over data protection and privacy matters concerning the financial institutions.

data protection regime, agency-level efforts, most notably through the FTC, have filled the void via a number of regulatory rulings and other enforcement actions.

Hand-in-hand with the push to legislate a federal privacy law, there is also an on-going effort within Congress to push Big Tech companies to take greater responsibility for the content they spread and the algorithms they use. Key in this regard are efforts to fundamentally reform Section 230 of the Communications Decency Act of 1996, which protects platforms such as Facebook and Google as well as website hosts from legal liability for online content provided by third parties. This 'intermediary liability shield' has come under withering criticism of late from both the political right and the left on two primary counts: first, for the license and cover that it provides to Big Tech platforms, such as Facebook and Google, for their unclear and inconsistent moderation practices. And second, for the proliferation of illicit and harmful content hosted by these Big Tech platforms, which is not taken seriously by them and oftentimes leaves victims without much or any civil remedies.

A number of areas of reform of Section 230 have been suggested. These include incentivizing online platforms to exercise greater oversight related to illicit and harmful content; clarifying the federal government's enforcement role *vis-à-vis* unlawful content; limiting the immunity exemptions provided and/or exempting specific types of harms from the purview of liability protections; setting updated platform and online behavioral standards; as well as creating a data access framework to oversee and regulate algorithm-based automated decision-making systems that are powered by artificial intelligence. Reaching a point of consensus on these reforms has been hard to come by though on Capitol Hill.

State Laws

Following the European Union's adoption of General Data Protection Regulation (GDPR) in 2016, California legislators began to acknowledge that existing California state laws at the time were insufficient to regulate "the proliferation of personal information", given the emerging new technologies and practices. As a result, the State of California enacted the California Consumer Privacy Act of 2018 (CCPA).[30] Effective since 2020, CCPA provides for a comprehensive right to data privacy and protection across all sectors, including an individual's right to know how a business collects, uses and shares his or her personal information, the right to delete personal information collected from oneself, and the right to opt-out of the sale of personal information. On November 3, 2020, CCPA was amended by the California Privacy Rights Act (CPRA). The latter Act imposes additional data protection and privacy obligations on businesses, including by allowing consumers to prevent businesses from sharing select "sensitive personal information." Furthermore, the law also created a California Privacy Protection Agency to implement and enforce California's data privacy laws.

The enactment of CCPA has prompted a number of other U.S. states to enact comprehensive data protection and privacy laws that are more-or-less modelled on the CCPA approach (although the specific level of protection and rights vary). As of mid-2022, six U.S. states have enacted comprehensive data privacy laws.[3] These are:

- 2018 California Consumer Privacy Act and 2020 California Privacy Rights Act
- 2019 New York SHIELD Act
- 2021 Virginia Consumer Data Protection Act (CDPA) (in effect from January 1, 2023)
- 2020 Colorado Privacy Act (CPA) (due to take effect on July 1, 2023)
- 2022 Connecticut Data Privacy Law (due to take effect on July 1, 2023)
- 2022 Utah Consumer Privacy Act (due to take effect on December 31, 2023)

State-level regulators are currently busy drafting the proposed regulations that will breathe life into these privacy and personal information protection laws. A number of written comment due dates and rulemaking hearings are scheduled in the early weeks and months of 2023.

3 To be clear, the 2019 New York SHIELD Act imposes a number of data privacy requirements but focuses primarily on data breach obligations. Legislative efforts to enact a comprehensive data privacy law for the state are currently on-going.

To Keep an Eye On

In comparison with China's or Europe's approach, the U.S. data governance regime, including the personal information protection and privacy regime, can be said to feature both inadequacy and overabundance. On the one hand, the United States' regime is fiercely protective of the right to unimpeded flows — including unimpeded cross-border flows — of data but lacks a comprehensive data protection and privacy regime at the national level. On the other hand, a "patchwork" of federal laws exist which, accompanied by FTC rulings, industry-specific privacy obligations, and agency-level data protection standards, have created both a veritable entanglement of data protection and privacy rules as well as a basis for their extraterritorial application for law enforcement purposes. At the state level meantime, there are a number of enforcement actors and frameworks, although they broadly hew to similar governance and protection principles.

Furthermore, national security considerations have assumed a larger profile. "Connected software applications" that are "designed, developed, manufactured, or supplied by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary [which include China]" are deemed to be a threat to "the national security, foreign policy, and economy of the United States." Pursuant to this determination, the

Biden administration, in June 2021, issued a list of potential indicators of risk relating to connected software applications of foreign origin, as part of its *Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries*. Clearly, the U.S. data governance regime remains a work in progress and the fate of executive branch actions against, say, TikTok and legislative branch measures, such as the American Data Privacy and Protection Act, will be important indicators of the U.S' evolving governance approach to the fast-moving technological and geopolitical developments at the digital frontier.

CHAPTER III

Global Approaches to Data Governance, Cross-Border Data Flow, and Cybersecurity

- THE CASE OF CROSS-BORDER DIGITAL COMMERCE -

On August 18, 2022, the existing members of the Digital Economy Partnership Agreement (DEPA), Chile, New Zealand and Singapore, announced the formation of an accession working group to consider China's application to join the agreement.[31] Chile is to chair the working group. Welcoming the decision, China's Ministry of Commerce (MOFCOM) vowed to conduct substantial negotiations and make full preparations to join the grouping. China had earlier in November 2021 filed an application to join the agreement. The Digital Economy Partnership Agreement is a first-of-its-kind digital economy agreement (DEA) that was signed by Chile, New Zealand and Singapore in June 2020. It contains 16 'modules' that inscribe rules ranging from digital business and trade facilitation to personal information protection to emerging technologies to inclusion, trust-building, transparency and dispute settlement. DEPA is one of a small but growing cluster of standalone digital economy agreements in the Asia-Pacific region — the other ones being the Singapore-Australia Digital Economy Agreement (SADEA) and the U.S.-Japan Digital Trade Agreement — that seek to harness the power of the e-commerce revolution in the Asia-Pacific region.

As per the February 2021 *Asian Economic Integration Report* produced by the Asian Development Bank (ADB), the Asia-Pacific region is in the midst of a historic e-commerce boom with online transactions and services having grown rapidly even prior to the COVID-19 lockdowns.[32] Fully, US$1.8 trillion of the total US$3.8 trillion of revenue earned worldwide by business-to-consumer (B2C) platforms in 2019 (e-commerce, online travel, advertising technology, transport, e-services and digital media) was generated in Asia. E-commerce revenues itself accounted for US$1.1 trillion regionally, with China accounting for 45 per cent of these digital transactions. The other Asia-Pacific countries are not far behind either. The Philippines, Indonesia and Vietnam were among the top five fastest growing e-commerce markets in the world in 2022. Online sales in Asia account for a greater proportion of total retail sales compared to any other major economic region of the world, and the use of digital platforms and their number of users continues to rise. Indeed, more than half of the world's ad-tech exposed internet users (those using social media apps) are based in Asia. Overall, the digital economy is

expected to add US$1 trillion to the region's GDP over the next decade, with the surge in business-to-consumer digital commerce being paralleled by the strong growth of regional cross-border business-to-business transactions.

The explosive growth of digital trade exports — digitally deliverable B2B services exports grew at 16 per cent per annum between 2007 and 2020 in the ASEAN region alone — has spotlighted the imperative to draw up rules and standards to govern these cross-border exchanges. As pointed out earlier, DEPA is one among a growing number of digital rule-making initiatives, either in a standalone capacity or as part of a larger preferential trade agreement such as the Regional Comprehensive Economic Partnership (RCEP) and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). Typically, these digital economy agreements, or digital chapters housed within broader trade agreements, contain provisions that can be clubbed under four heads:

- First, are **provisions that aim to facilitate digital trade**, such as the non-discriminatory and national treatment of digital products and the elimination of customs duties on electronic transmissions. Other measures included in this category are rules related to electronic authentication and electronic signatures as well as rules establishing domestic regulatory frameworks that are not needlessly burdensome. No specific regulatory approach is prescribed as such though.

- Next, are **provisions that seek to limit the scope of governmental measures that could, from an incentives-standpoint, interfere with the growth of cross-border data flows.** Foremost in this regard are measures that prohibit the location of computing facilities in a Party's territory as a condition for conducting business in that territory. Other provisions include the prohibition of data localization and the prohibition of forced transfer of source codes and proprietary cryptographic information (although this is not uniform across digital economy agreements). The aim of these provisions is to eliminate the barriers that impede digital trade growth and flow.

- The third type of **provisions are those that protect the interests of consumers and users.** Typically, these include articles on online consumer protection, personal information protection, and protection against unsolicited commercial electronic messages. The intent here is to provide privacy and personal information security to digital users and thereby enhance their trust in engaging commercially on digital platforms.

- The final category of **provisions are ones that preserve the government's sovereign right to regulate** the digital space and cross-border flows that occur or originate within its borders. Typically, these provisions are interspersed across the relevant agreement or chapter. Foremost, they include security exceptions, prudential exceptions, general taxation-related rights as well as carveouts in the name of regulatory autonomy to pursue "legitimate public policy objective[s]."

All digital economy agreements, or digital chapters within trade agreements, are not created equal or alike. The 'gold standard' agreements among them, such as the Digital Economy Partnership Agreement (DEPA) and the Singapore-Australia Digital Economy Agreement (SADEA),[33] contain more demanding rules and standards compared to their plainer 'vanilla' counterparts, such as the Regional Comprehensive Economic Partnership (RCEP).[34]

A sign is seen at the RCEP (Regional Comprehensive Economic Partnership) Qingdao Pilot Innovation Base for Economic and Trade Cooperation on February 24, 2021 in Qingdao, Shandong Province of China.
(Source: Cui Liu/VCG via Getty Images)

For example:

- Both DEPA and SADEA contain provisions that **place a ban on performance requirements**, such as sharing source code and/or algorithms. Typically, the relevant article declares that neither Party shall require the transfer of, or access to, source code or software owned by a foreign supplier as a condition for market access or domestic sale. This provision is absent in RCEP.

- Both DEPA and SADEA contain provisions that **ban data localization-related requirements,** such as demands that computing facilities processing the relevant data must be based locally. The standard article notes that no Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory. The provision in the RCEP agreement is weaker in this regard. Requiring computing facilities to be located on one's territory as a condition for conducting business is (nominally) barred but blurred by a subsidiary provision that notes that Parties are also at liberty to use location-based measures "to ensure the security and confidentiality of communications."

- Both DEPA and SADEA contain provisions that **prohibit the imposition of regulations that ban disclosures related to encryption products.** Typically, the relevant article declares that with respect to cryptography products that are designed for commercial applications, no Party shall impose or maintain technical regulation or conformity assessment procedures that requires a foreign supplier – as a condition for market access or domestic sale - to partner with a locally entity, transfer a particular technology or production process, or integrate a particular local cryptographic algorithm or cipher. The RCEP agreement does not contain this provision.

- DEPA and SEDEA also **contain stronger language** than RCEP in obliging Parties to enforce domestic laws related to privacy, consumer protection and cybersecurity protections.

Preserving the 'Right to Regulate' within Digital Economy Agreements

The gap between 'gold standard' agreements and 'vanilla' agreements in the digital trade sphere should not obscure from the fact that both types of agreements are typically couched in 'best endeavor' terms as opposed to binding terms. Given the dynamism and fluidity of innovation, processes and practices in the cybersphere, the emphasis in digital economy agreements has been to strike a balance between incentivizing commercial cross-border data flows while preserving the right to regulate these flows. Setting rules and standards in stone that might soon become outdated or difficult to politically modify retroactively has typically been eschewed. Rather, ample policy space to regulate is provided for.

For example:

- Provisions in digital economy agreements that declare that neither Party shall require the transfer of, or access to, source code as a condition for market entry also contain a subsidiary provision that does not preclude a government agency, regulatory body or judicial authority from requiring the foreign Party to preserve or make available the relevant source code for investigation, examination, and judicial or administrative enforcement action.

- Similarly, provisions that place a ban on data localization-related requirements typically do not preclude a government agency from imposing inconsistent measures related to the locating of such computing facilities, so long as the measures are intended to "achieve a legitimate public policy objective" and "do not impose restrictions…greater than are required to achieve the objective".

- Equally, the prohibition of regulations that ban the divulgence of encryption products is accompanied with a subsidiary provision that does not prevent a Party's law enforcement authorities from requiring service providers that use encryption to provide unencrypted communications pursuant to that Party's judicial processes.

This recurrent deference to regulatory policy space is a bow to the dynamic and fast-changing pace of regulation in the digital sphere - be in terms of anti-monopoly protections, privacy and data protections, fintech-related financial stability risk management, development of rules for artificial intelligence (AI) applications or, for the matter, requiring the transparency of the structure, use, and impacts of algorithmic systems. For example, it is now increasingly accepted in the regulatory universe that given that internet platforms rely on artificial intelligence (AI) and machine learning (ML)-based tools for content moderation, ad targeting and delivery, and content ranking and recommendation, it is in the interests of the data-sharing-and-using public that regulations be inscribed that provide vetted researchers access to such platform data so as to ensure accountability of the platforms' algorithmic systems. Rules demanding such access to these algorithmic "black boxes" would have been inconceivable even five years ago.

And contrarily, as cutting-edge regulatory thinking has evolved, language once considered standard, such as the immunity granted to intermediary service providers from civil liability for third-party content, is increasingly being questioned, if not dropped, from the more recent digital economy agreements or chapters. Each of the U.S.-led digital economy agreements or negotiations (the United States-Mexico-Canada Agreement; the negotiated Trans-Pacific Partnership Agreement; the U.S.-Japan Digital Trade Agreement) had contained a provision to the effect that "neither Party shall adopt or maintain measures that treat a supplier or user of an interactive computer service as an information content provider in determining liability for harms related to information stored, processed, distributed, or made available by the service."[35] Fast-forward to the 2020s and neither the Digital Economy Partnership Agreement (DEPA) nor the Singapore-Australia Digital Economy Agreement (SADEA) contains language specifying this liability protection for intermediary service providers. And with the exit of the United States from the TPP agreement in January 2017, the residual parties to the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) dropped the language on intermediary liability protections from their finalized text too.

Truth be told, the balance of opinion is tilting against such liability protections in Washington too. As criticisms mount on both sides of the aisle regarding Section 230 of the Communications Decency Act of 1996 — on which the intermediary liability protection provision is styled, it is only a matter of time until this provision is eliminated in a future U.S.-led digital trade agreement. The digital chapter of the trade pillar of the Indo-Pacific Economic Framework for Prosperity (IPEF) will likely be the first U.S.-led digital trade text to feature an absence of this provision.

Given this background, the State's adoption or maintenance of measures that may be inconsistent with the practice of cross-border data flow but are "necessary to achieve a legitimate public policy objective" — with the ambit of what constitutes a "legitimate public policy objective" continually evolving — is now a stylized or established principle in digital economy agreements. And these "legitimate public policy objective[s]" subsist over-and-above the standard general and security exceptions, including the exception to protect one's own "essential security interests", that are typically embedded in trade agreements, and which have been a part-and-parcel of the global trade system since the inception of the General Agreements on Tariff and Trade (GATT) regime in the late-1940s.

BOX 2: Digital Services Taxation – A Carved-out Sphere of Regulation

In June 2020, the United States Trade Representative (USTR) launched Section 301 investigations into the digital services taxes (DSTs) adopted by or on the anvil in Austria, Brazil, the Czech Republic, the European Union (EU), India, Indonesia, Italy, Spain, Turkey, and the United Kingdom.[36] In USTR's view, these taxes amounted to "unfair trade practices" which:

1. discriminated against U.S. digital companies
2. were inconsistent with the principles of international taxation, including due to their extraterritorial application as well as their application to revenue rather than income
3. and burdened or restricted U.S. commerce.

As per the (Section 301) statute, the threshold for wrongdoing in a Section 301 investigation is unreasonability. An "unreasonable" foreign trade practice can simply be one that is unfair "while not necessarily in violation of...the international rights of the United States." Once such a trade practice is found to be "unreasonable", the President is authorized to impose unilateral measures, including a tariff measure, to counter the effects of the infringing foreign trade practice.

The push to impose digital services taxes on the part of many advanced and developing country governments derives from their desire to tax the revenues and profits of transnational corporations that operate in business-to-consumer (B2C) digital economy sectors within their jurisdictions. The prevailing sentiment is that the revenue and profits derived by Big Tech and other multinational corporations from consumers in these jurisdictions is not adequately taxed and reallocated back to their jurisdictions. With a view to marking a first step to remedy this failing, 136 countries under the aegis of the Organization for Economic Cooperation and Development (OECD) signed a two-pillar taxation deal in October 2021 that allocates some taxing rights over transnational corporations from their home countries to the markets where they have business activities and earn profits — regardless of whether these firms have a physical presence there.[37]

The important takeaway to note in the context of this chapter's discussion is that digital taxation is a standalone area of regulation. It is administered by finance ministries/treasury departments and is for the most part managed at an arms-length distance from the other ministries that cover the trade, commerce, or digital affairs portfolios. And the standard digital economy agreement (DEA) typically, too, observes that "nothing in the [relevant DTA] shall apply to taxation measures" or "affect the rights and obligations of either party under any tax convention".

On a separate but related note, there is an on-going moratorium in place on non-imposition of customs duties on electronic transmissions (which encompass everything from software, emails, digital movies and music to videogames) under the aegis of the World Trade Organization (WTO). This moratorium has been in effect since 1998 and has been renewed every two years. The most recent renewal was at the 12th WTO Ministerial Conference (MC12) in Geneva in June 2022.

(The Lack of) Multilateral Rulemaking on Digital Commerce

The endeavor to memorialize digital trade-related request-offer commitments at the multilateral level into binding or best endeavor rules has for the most part been much less successful. The World Trade Organization's (WTO) global e-commerce negotiations have been on-going for the better part of almost 25 years, yet there is little to show in the form of concrete deliverables. At the Second Ministerial Conference in May 1998, a Declaration on Global Electronic Commerce was adopted, leading in turn to the establishment of a Work Program by the General Council (the WTO's highest decision-making body) in September 1998.[38] Regular discussions on proposed e-commerce rules within various WTO bodies, functionally grouped together under four tracks, have been conducted since then.

These are:

- **Liberalization track** – Non-imposition of customs duties on electronic transmissions; non-discriminatory treatment of digital products; free cross-border transfer of information by electronic means; prohibition of data localization; market access.

- **Facilitation track** – Electronic signatures and authentications; electronic documentation /paperless trading; access to electronic payment solutions.

- **Trust and Reliability track** – Personal information protection; protection against unsolicited commercial electronic messages; protection of trade secrets, including source codes and proprietary algorithms.

- **Transparency track** – Public notice regarding regulatory measures; technical assistance and capacity building.

Discussions have also been conducted in parallel among a group of like-minded WTO members under the Joint Initiative on E-Commerce. Under the Joint Initiative, negotiations are being conducted on the trade-related aspects of digital commerce by a group of 86 members (as of January 2021), accounting for over 90 per cent of global ecommerce trade. Australia, Japan and Singapore are the co-convenors of the initiative. The issues raised are grouped under six main themes: enabling electronic commerce; openness and electronic commerce; trust and digital trade; cross-cutting issues; telecommunications; and market access.

On a separate track, the G20 countries are also engaged on the issue. At the June 2019 G20 Summit under the chairpersonship of Japan, an "Osaka Declaration on the Digital Economy" was issued, and an "Osaka Track" framework encapsulating "Data Free Flow with Trust" (DFFT) was launched.[39] DFFT aims to "achieve free flow of data

while securing public trust in protection of privacy and security." A permanent digital governance body or secretariat to administer the 'free flow of data with trust' has been proposed by Japan, as part of its 2023 G7 chairpersonship. Although appealing in concept, DFFT failed to garner a critical mass of support as well as produce concrete results. India, Indonesia and South Africa did not even sign the aforementioned "Osaka Declaration on the Digital Economy", and the focus of the recent past and present Indonesian and Indian G20 presidencies' digital transformation efforts is geared towards equity (reducing digital divides, improving competition/anti-trust policies, digital capacity-building assistance, etc.) rather than on the liberalization of flows with trust.

The failure at the multilateral level to deliver concrete commitments on cross-border data flows stems in part from the unwieldy process of decision-making in a consensus-driven organization of 160-plus members at varying stages in their national development. More pointedly however, the failure also stems from the fact that the major economic blocs represented at the WTO — the U.S, the European Union and China — come to the table with differing approaches not just to the liberalization of e-commerce but, just as importantly, to its regulation. The United States, for example (as note earlier), takes an aggressive stance on digital market access and light touch regulation. Such regulation is more-or-less *laissez-faire* on domestic and cross-border flows (with the Federal Trade Commission tasked though with prosecuting malfeasance domestically). No material distinction is made between the handling of personal and non-personal data (although this could change with the passage of federal privacy legislation). And the cross-border flow of data is subject to only narrow security exceptions, such as the denial of transfer of sensitive data to foreign adversaries and the unconditional access for law enforcement to the data of U.S. jurisdictional subjects that is stored overseas.

On the other hand, the regulatory approaches of the European Union and China to the data governance trifecta of commerce, security, inclusion, and privacy is much more prescriptive.[40] This is particularly noticeable in the area of privacy and personal information protection. While most non-personal data is more-or-less allowed to freely cross borders, personal data can only flow freely across borders if the destination State is deemed to possess an 'adequate' data protection regime with in-built safeguards. The security assessment through which such data must pass, particularly with regard to 'important data', is also wider-ranging and more stringent (although it is not targeted at any particular adversary country, as such). Until greater harmony in domestic regulatory frameworks is achieved, especially in their respective security and privacy frameworks, the effort to inscribe liberalized cross-border digital trade flow-related rules at the multilateral level will continue to remain a heavy lift for all parties concerned.

- THE CASE OF GLOBAL CYBERSECURITY NORMS -

On September 24-25, 2015, ex-President Barack Obama hosted President Xi Jinping for a State visit at which the two heads of state exchanged views on a range of global, regional, and bilateral topics. Among the key deliverables coming out of the State visit was a bilateral commitment on cybersecurity, particularly concerning malicious cyber activities.[41] Both sides agreed that neither country's government would conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors. Both sides also committed to make common efforts to further identify and promote appropriate norms of state behavior in cyberspace within the international community. A high-level joint dialogue mechanism on fighting cybercrime and related issues was established to implement the understanding, with the U.S. Secretary of Homeland Security and the U.S. Attorney General co-chairing the dialogue at Washington's end and a ministerial level appointee supported by the Ministry of Public Security, Ministry of State Security and the Ministry of Justice chairing the dialogue at Beijing's end.

The September 2015 understanding was the high point in U.S.-China cybersecurity ties. It has been a downward slide ever since, particularly once the Trump administration was elected to office. The bilateral effort to jointly identify and promote appropriate norms of state behavior in cyberspace within the international community has essentially remained stillborn. In its place, a plethora of inter-governmental and non-governmental initiatives have filled the gap with a view to address the challenges posed by 'cyber insecurity', with a particular focus on proscribing the exploitation of commercial information technology (IT) systems by malicious state and non-state to conduct malevolent and harmful cyber activities. The following are some of the more prominent intergovernmental and non-governmental working groups, initiatives, and proposals that have focused their attention on strengthening international cybersecurity norms.

1. **The UN Open-Ended Working Group (OEWG) on Information and Telecommunications (ICT) in the Context of International Security:** In March 2021, the OEWG on ICT published a final consensus report on responsible state behavior in cyberspace.[42] Noting that developments in ICT technologies have implications for all three pillars of the United Nations' work (i.e., peace and security, human rights, and sustainable development), the report went on to recommend a number of voluntary, non-binding norms spanning a range of issue areas.

These issue areas being:

- existing and potential threats in the sphere of information security and possible cooperative measures to address them;
- means to further development of rules, norms and principles of responsible behavior of States;

- how international law should apply to the use of ICTs by States;
- confidence-building measures;
- capacity-building measures; and
- the possibility of establishing a regular institutionalized dialogue with broad participation under the auspices of the United Nations.

A key recommendation put forth in this regard was that States should not conduct or knowingly support ICT activities that are contrary to their obligations under international law and which intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure used to provide services to the public. And furthermore, that States should continue to strengthen measures to protect of all critical infrastructure from ICT threats and increase exchanges on best practices with regard to such critical infrastructure protection.

2. **The Paris Call for Trust and Security in Cyberspace:** The Paris Call is a joint private-public effort initiated in November 2018 by French President Emmanuel Macron during the Internet Governance Forum held at UNESCO and the Paris Peace Forum.[43] The Call aims to bring together stakeholders from across cyberspace to work together to adopt responsible online behavior and implement principles that are applicable in the physical world. In this regard, a vision of regulation in cyberspace was also proposed along with nine specific proposed principles for adoption.

The nine principles of the Paris Call for Trust and Security in Cyberspace are:

- **Principle 1. Protect individuals and infrastructure** – prevent and recover from malicious cyber activities that cause significant, indiscriminate, or systemic harm to individuals and critical infrastructure.
- **Principle 2. Protect the Internet** – prevent activity that intentionally and substantially damages the general availability or integrity of the public core of the internet.
- **Principle 3. Defend electoral processes** – strengthen the capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities.
- **Principle 4. Defend intellectual property** – prevent ICT-enabled theft of IP, including trade secrets or other confidential business information, with the intent of providing illicit competitive advantages to companies or the commercial sector.
- **Principle 5. Non-proliferation of malicious software and practices** – develop ways to prevent the proliferation of malicious software and practices intended to cause harm.
- **Principle 6. Strengthen digital lifecycle security** – strengthen the security of digital processes and products and services throughout their lifecycle and supply chain.

- **Principle 7. Support cyber hygiene** – support efforts to strengthen an advanced level of cyber cleanliness and good practices among all actors.
- **Principle 8. No private hack back** – take steps to prevent non-State actors, including the private sector, from hacking – be it for their own purposes or on behalf of other non-State actors.
- **Principle 9. Promote international cyber norms** – promote the widespread acceptance and implementation of international norms of responsible behavior as well as confidence-building measures in cyberspace.

At this time of writing, the Paris Call is supported by 81 States as well as numerous private sector entities and civil society organizations.

3. **The Global Commission on the Stability of Cyberspace (GCSC):** The GCSC was launched in February 2017 and concluded its activities in December 2021 after the publication of its CyberStability Paper Series. The aim of the Commission was to promote mutual awareness and understanding among the various cyberspace actors and communities that were working on issues related to international cybersecurity. By linking the dialogues on international security with the new communities created by cyberspace, the GCSC sought to support policy and norms coherence related to the security and stability in, and of, cyberspace. In November 2019, the Global Commission on the Stability of Cyberspace laid out an extensive final report that called for the embrace of four guiding principles (Responsibility; Restraint; Requirement to Act; Respect for Human Rights) and six recommendations.[44]

These recommendations are:

1. State and non-State actors should adopt and implement norms that increase the stability of cyberspace by promoting restraint and encourage constructive action.
2. State and non-State actors, consistent with their responsibilities and limitations, must respond appropriately to norms violations, ensuring that those who violate norms face predictable and meaningful consequences.
3. State and non-State actors, including international institutions, should increase efforts to train staff, build capacity and capabilities, promote a shared understanding of the importance of the stability of cyberspace, while taking into account the disparate needs of different parties.
4. State and non-State actors should collect, share, review, and publish information on norms violations and the impact of such activities.
5. State and non-State actors should establish and support communities of interest to help ensure the stability of cyberspace.
6. A standing multistakeholder engagement mechanism must be established to address cyber stability-related issues — one where States, the private sector (including the technical community), and civil society are adequately involved and consulted.

The UN Open-Ended Working Group (OEWG), the Paris Call for Trust and Security in Cyberspace, and the Global Commission on the Stability of Cyberspace (GCSC) are just some of the more prominent initiatives in the area of global cybersecurity governance. While these initiatives have achieved a critical mass of participation, they have — akin to the case of multilateral rulemaking in the digital commerce realm — failed to yield concrete results in terms of actionable deliverables. Their proposals are typically couched in voluntary non-binding terms and will remain so for the foreseeable future.

At a time when multilateral governance is under greatest strain since the end of World War II, it is hard to see how materially significant progress can be achieved in this regard in the short-to-medium term among the major key developed and developing country players and non-government actors. Global rulemaking on cybersecurity in the interim will necessarily have to evolve via a patchwork of rules and standards that are enforced nationally by the major economic players and pluralized regionally by them thereafter, perhaps. It is imperative that the private sector be brought in as an integral participant too in these consultations so that both the private and public sectors could work hand-in-hand to jointly protect technology systems and critical infrastructures from attack.

CHAPTER IV

Devising Purpose-Fit Law and Norms to Address the Digital Challenge

Though the field of artificial intelligence (AI) was still in the wilderness when Isaac Asimov put forward his "Three Laws of Robotics" in 1950, the "Three Laws" did become one of the most important principles that underlie today the logic of artificial intelligence more than half a century later. AI is closely related to data governance and security, which also needs its set of matching laws so that the digital universe can be administered securely, efficiently, and fairly. The institutionalization of such rulemaking and governance practices is not only beneficial to companies and industries, but also of benefit to states too. A number of patterns are observable from the study of China's and the United States' approaches to data flow, data governance and cybersecurity as well as the prevailing global approaches in this regard.

A. Data Governance and Security: Serving the Healthy Development and Global Prosperity of the Information Industry

First, the wave upon wave of globalization brought on by the information technology revolution has closely linked the world together. After some three decades of the digital sector's 'Wild West' style development, it is clear now though that regulation and compliance on data governance and security is lagging significantly. Currently, from network infrastructure hardware providers to social network service providers and from mobile phone manufacturers to smart car manufacturers, more and more industries and enterprises continue to suffer from data governance and security mishaps. Only by clarifying data governance and security can the development of these industries be channeled towards a more beneficial industrial and social direction.

In the United States, data governance can be traced back to the 1980s, when a series of protective rules in vertical fields such as health information and the safety of children's online information were successively issued. With the development of technology, these rules were adapted and applied in new ways to the era of Big Data. However, China's data governance system, which has mostly been developed in short period of the past decade, has taken aim at these Big Data-era rules from its very inception and implementation of these rules is already ongoing in various subsectors. The differences in the order of formation of data governance systems in China and the United States

notwithstanding, both of them aim to make data play a more standardized role in order to better promote the development of the industry and society at large.

B. Managing the Differences between Bilateral and Multilateral Transnational Data Governance and Security

As shown in previous studies, there are many differences between China, the U.S. and the EU in the terms of their frameworks of current data governance and security policy. Issues arising from data collection and use may become potential areas of dispute between China and the United States. In this regard, it is important to strengthen communication and mutual trust, and properly manage possible conflicts. From a U.S. government report in 2021 alleging that Chinese government sponsored cyberattacks on U.S. natural-gas pipeline operators, to China's claim last year that the U.S. National Security Agency (NSA) had stolen more than 140 GB of data in a cyberattack on China's Northwestern Polytechnical University, data security-related problems are increasingly playing themselves out in bilateral relations in a low-intensity confrontational manner.

In the field of cyber security, Washington regards Beijing as a threat, while China expresses strong dissatisfaction and firm opposition. Therefore, a common "stimulus-response" pattern has formed. Currently, it is difficult to avoid such data disputes completely, but it is feasible to agree on bottom line rules of data security in a way to maximize common bilateral interests and limit the relevant disputes to the information and communication technology (ICT) sphere — and thereby prevent their spillover and intensification of impacts within the broader bilateral relationship.

C. Seeking Cooperation on Data Governance and Security

Both China and the United States are not only major victims of cyberattacks but also major formulators of global data governance and security rules. Therefore, a strong convergence of interest for mutual cooperation exists. Cooperation on data governance and security is long-term. Driven by technology, the data field is developing and changing rapidly and cooperation is also required to be established to keep pace with these on-going changes. Spheres of cooperation on data governance and security is extensive and can be advanced in many areas, such as the protection of critical infrastructure and personal information, the storage and retrieval of enterprises' overseas data, as well as supply chain security. When cooperation is hindered in one field, it makes sense to seek it in other fields. Given the imperatives of sovereignty, the collaboration between data governance and security can be fragile, and security and regulation require constant adjustment in order to preserve and sustain a fine balance.

Not unlike the "Three Laws of robotics", the aspiration is that this and other similar research endeavors will help lay the foundations and pave the way for the formation of new, purpose-fit norms and rules that elegantly address the digital policy challenge, both bilaterally and at the global level.

Endnotes

1 *Work Programme on Electronic Commerce, Draft Ministerial Decision of June 16, 2022,* WT/MIN(22)/W/23, World Trade Organization, June 16, 2022, https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/MIN22/W23.pdf&Open=True.

2 国家互联网信息办公室发布《数字中国发展报告（2021年）》["Digital China Development Report (2021)" released by the Cyberspace Administration of China], *China Netcom*, August 2, 2022, http://www.cac.gov.cn/2022-08/02/c_1661066515613920.htm?mc_cid=3f85920c5d&mc_eid=2ad92c1a19.

3 "Xi stresses need to build basic data systems, enhance administrative division management," *Xinhua*, June 23, 2022, https://english.news.cn/20220623/8325a1f677c2422cb3a2a2def07e8388/c.html.

4 "Some Views on Basic Systems for Data" [关于构建数据基础制度若干观点], National Development and Reform Commission (NDRC) [国家发展和改革委员会], March 21, 2022, https://interpret.csis.org/translations/some-views-on-basic-systems-for-data/.

5 Taige Hu and Changhao Wei, "NPCSC Amends Anti-Monopoly Law, Revises Sports Law & Adopts New Law to Protect Black Soil," *NPC Observer*, June 30, 2022, https://npcobserver.com/2022/06/30/npcsc-amends-anti-monopoly-law-revises-sports-law-adopts-new-law-to-protect-black-soil/.

6 Rogier Creemers, Graham Webster, and Paul Triolo, "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)," *Digichina*, June 29, 2018, https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/.

7 Rogier Creemers and Graham Webster, "Translation: Cybersecurity Review Measures (Revised) – Effective Feb. 15, 2022," *Digichina*, January 10, 2022, https://digichina.stanford.edu/work/translation-cybersecurity-review-measures-revised-effective-feb-15-2022/.

8 Lingling Wei and Keith Zhai, "Chinese Regulators Suggested Didi Delay Its U.S. IPO," *The Wall Street Journal*, July 5, 2021, https://www.wsj.com/articles/chinese-regulators-suggested-didi-delay-its-u-s-ipo-11625510600.

9 中华人民共和国数据安全法 [Data Security Law of the People's Republic of China], The National People's Congres of the People's Republic of China, June 10, 2021, http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml.

10 Ken (Jianmin) Dai and Jet (Zhisong) Deng, "China Personal Information Protection Law (PIPL) FAQs," *Bloomberg Law*, April 6, 2022, https://pro.bloomberglaw.com/brief/china-personal-information-protection-law-pipl-faqs/.

11 *Data Security Business Advisory: Risks and Considerations for Businesses Using Data Services and Equipment from Firms Linked to the People's Republic of China,* U.S. Department of Homeland Security, June 11, 2022, https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf.

12 NCSC Director William Evanina, *Keynote Remarks as Prepared for Delivery,* International Legal Technology Association (ILTA) LegalSEC Summit 2019, June 4, 2019, https://www.dni.gov/files/NCSC/documents/news/20190606-NCSC-Remarks-ILTA-Summit_2019.pdf.

13 Camille Fischer, "The CLOUD Act: A Dangerous Expansion of Police Snooping on Cross-Border Data," *EFF Deeplinks Blog*, February 8, 2018, https://www.eff.org/deeplinks/2018/02/cloud-act-dangerous-expansion-police-snooping-cross-border-data.

14 Zack Whittaker, "US government pushed tech firms to hand over source code," *ZD Net*, March 17, 2016, https://www.zdnet.com/article/us-government-pushed-tech-firms-to-hand-over-source-code/.

15 "China to severely punish illegal activities in securities market," *Xinhua*, July 6, 2021, http://www.xinhuanet.com/english/2021-07/06/c_1310046367.htm.

16 数据出境安全评估办法 [Measures for Data Export Security Assessment], *China Netcom*, July 7, 2022, http://www.cac.gov.cn/2022-07/07/c_1658811536396503.htm.

17 国家互联网信息办公室关于《网络数据安全管理条例（征求意见稿）》公开征求意见的通知 [Notice of the Cyberspace Administration for Public Comments on the "Data Security Management Regulation (Draft for Comment)"], *China Netcom*, November 14, 2021, http://www.cac.gov.cn/2021-11/14/c_1638501991577898.htm.

18 Aline Blankertz and Julian Jaursch, "What the European DSA and DMA proposals mean for online platforms," *Brookings TechStrem*, January 14, 2022, https://www.brookings.edu/techstream/what-the-european-dsa-and-dma-proposals-mean-for-online-platforms/.

19 Dr. Sara Hsu, "China's Regulatory Clampdown on Big Tech," Institute for China-America Studies, November 1, 2021, https://chinaus-icas.org/research/chinas-regulatory-clampdown-on-big-tech/.

20 Patrick McGee, "US regulator sues data broker over sale of location information," *Financial Times*, August 29, 2022, https://www.ft.com/content/c37668b7-d2f7-4784-99eb-a06255d78cc8.

21 "Framework for Responsible Data Protection Regulation," Google, September 2018, https://services.google.com/fh/files/blogs/google_framework_responsible_data_protection_regulation.pdf.

22 "The 10 Principles of Data Privacy," U.S. Chamber of Commerce, September 21, 2021, https://www.uschamber.com/technology/data-privacy/the-10-principles-of-data-privacy.

23 Lulu Chang, "Amazon, Microsoft, Uber donate to oppose the California Consumer Privacy Act," *Digital Trends*, June 17, 2018, https://www.digitaltrends.com/computing/tech-opposes-california-privacy-act/.

24 Todd Feathers, "Big Tech Is Pushing States to Pass Privacy Laws, and Yes, You Should Be Suspicious," *The Markup*, April 15, 2021, https://themarkup.org/privacy/2021/04/15/big-tech-is-pushing-states-to-pass-privacy-laws-and-yes-you-should-be-suspicious.

25 Ibid.; Diane Bartz, "U.S. bill to rein in Big Tech backed by dozens of small and big companies," *Reuters*, June 13, 2022, https://www.reuters.com/technology/dozens-companies-small-business-groups-back-us-bill-rein-big-tech-2022-06-13/.

26 *Data Protection Law: An Overview*, R45631, Congressional Research Service, March 25, 2019, https://crsreports.congress.gov/product/pdf/R/R45631.

27 Daniel J. Solove and Woodrow Hartzong, *Breached!: Why Data Security Law Fails and How to Improve It*, Oxford: Oxford University Press, 2022.

28 "Facebook, Inc., In the Matter of," FTC File Number 092 3184, Federal Trade Commission, April 28, 2020, https://www.ftc.gov/legal-library/browse/cases-proceedings/092-3184-182-3109-c-4365-facebook-inc-matter.

29 *Fair Credit Reporting Act*, 15 U.S.C. §§ 1681-1681x, Federal Trade Commission, August 2022, https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.

30 "California Consumer Privacy Act (CCPA)," Office of the California Attorney General, https://oag.ca.gov/privacy/ccpa.

31 "Digital Economy Partnership Agreement Joint Committee commences Accession Working Group for China," Ministry of Trade and Industry of Singapore, August 18, 2022, https://www.mti.gov.sg/Newsroom/Press-Releases/2022/08/Digital-Economy-Partnership-Agreement-Joint-Committee-commences-Accession-Working-Group-for-China.

32 *Asian Economic Integration Report 2021: Making Digital Platforms Work for Asia and the Pacific—Highlights,* Asian Development Bank, 2021, https://www.adb.org/sites/default/files/publication/674421/aeir-2021-highlights.pdf.

33 "DEPA text and resources," New Zealand Ministry of Foreign Affairs & Trade, 2020, https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement-depa/depa-text-and-resources/; "Singapore-Australia Digital Economy Agreement (SADEA)," Ministry of Trade and Industry of Singapore, 2022, https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/The-Singapore-Australia-Digital-Economy-Agreement.

34 "Regional Comprehensive Economic Partnership (RCEP)," ASEAN Secretariat, 2019, https://rcepsec.org/legal-text/.

35 "U.S.-Japan Digital Trade Agreement Text," Office of the U.S. Trade Representative, October 7, 2019, https://ustr.gov/countries-regions/japan-korea-apec/japan/us-japan-trade-agreement-negotiations/us-japan-digital-trade-agreement-text.

36 "Section 301 – Digital Services Taxes," Office of the U.S. Trade Representative, https://ustr.gov/issue-areas/enforcement/section-301-investigations/section-301-digital-services-taxes.

37 "International community strikes a ground-breaking tax deal for the digital age," Organisation for Economic Co-operation and Development, August 10, 2021, https://www.oecd.org/tax/beps/international-community-strikes-a-ground-breaking-tax-deal-for-the-digital-age.htm.

38 "Work Programme on E-Commerce," World Trade Organization, 2022, https://www.wto.org/english/tratop_e/ecom_e/ecom_work_programme_e.htm.

39 *Osaka Declaration on Digital Economy*, World Trade Organization, June 2019, https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/pdf/special_event/en/special_event_01.pdf.

40 Deborah Elms, *Digital Sovereignty: protectionism or autonomy?*, Hinrich Foundation, September 2021, https://static1.squarespace.com/static/5393d501e4b0643446abd228/t/615f394c5533a623afeac00b/1633630545286/Digital+sovereignty+protectionism+or+autonomy+-+Hinrich+Foundation+-+Deborah+Elms+-+September+2021.pdf.

41 "FACT SHEET: President Xi Jinping's State Visit to the United States," The White House, September 25, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

42 *Open-ended working group on developments in the field of information and telecommunications in the context of international security: Final Substantive Report,* A/AC.290/2021/CRP.2, UN General Assembly, March 10, 2021, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

43 "Paris Call: For trust and security in cyberspace," Paris Call, November 12, 2018, https://pariscall.international/en/.

44 *Advancing Cyberstability: Final Report*, Global Commission on the Stability of Cyberspace, November 13, 2019, https://hcss.nl/wp-content/uploads/2019/11/GCSC-Final-Report-November-2019.pdf.

The Institute for China-America Studies (ICAS) is an independent think tank in Washington D.C. ICAS focuses on the evolving dynamics in the U.S.-China relationship to promote greater collaboration and mutual understanding through sincere exchanges of fresh ideas, objective policy-oriented research, and fair assessments of this critical bilateral relationship.

We aim to provide a window into the worldviews of both the United States and China, and thereby serve as a vehicle to promote greater understanding between these two countries and societies.

中研中心究美 ICAS
Institute for China-America Studies

1919 M St. NW, Suite 310
Washington, DC 20036
(202) 968-0595 | www.chinaus-icas.org

国观智库 GRANDVIEW INSTITUTION

3 Nanliuxiang St, Xicheng District
Beijing, China 100052
(+86) 010-6215-8609 | www.grandview.cn