



Data Sovereignty in Action:

Ant Group and Didi Chuxing Case Studies

Dev Lewis, Digital Asia Hub

Preface	2
Summary	4
Introduction	6
Context	8
Key Stakeholders for Data Governance	10
Framing Data Sovereignty: Security and Economic Development	12
Twin Purpose: Economic Development & Security	12
Controlling Cross-border Data	13
Data Classification	14
Data Ownership: State vs Private Frictions	15
Case 1	
“Nationalizing” Ant Group’s data	16
Data Assets	17
Regulating Ant	17
Data Tension: Monopoly Control over Data	18
Case 2	
Didi Cyber Security Review	20
Data Assets	20
Data Tension: National Security	21
Emerging Data Cultures in China	23
Conclusion	23
References	25
Appendix	30
Sample of Questions	30
Methodology	30
Author	31

Data fuels digital change. It forms the basis for numerous new products and services and can bring about specific advantages such as personalised medicine, autonomous driving, or more efficient administration. While data may be indispensable for the generation of new knowledge and may aid rational decision-making in the spheres of politics, society, and the economy, it brings with it an element of fear stemming from issues such as vulnerable consumers, privacy concerns, and the possibility of algorithm-based decisions being executed independent of human control.

The ability to collect and process ever-increasing amounts of data is a **key to innovation and growth**. For states such as Germany with a globally networked and high-tech economy, this presents enormous opportunities – especially due to the increasing amount of non-personal data made available through industrial processes as well as public sources. However, neither Germany nor Europe is fully exploiting the innovative potential of data for the benefit of society, the economy, science, and the state. The collection and analysis of data does not have to be in conflict with the **European approach to data protection, which marks an important standard for the responsible handling of data** in the global context.

Numerous US and Chinese companies have occupied central strategic positions in the digital economy in recent years. These include cloud systems, digital payment systems, online trading, and Artificial Intelligence (AI). **Despite some notable successes, Europe and Germany still lack a comprehensive vision for the “age of data”.** Nevertheless, in the spring of 2020, the European Commission launched its roadmap for digital policy – a “Data Act” to create a single European data market is planned for 2021.

Against this background, it is worth taking a **comparative look at the Asia-Pacific region** as it is generally considered the region that currently leads in both global innovation and economic growth.

Hence the Konrad Adenauer Foundation’s regional programme “Political Dialogue” based in Singapore started a large-scale study in September 2019 on *Data and Innovation in Asia-Pacific*. We want to turn our gaze away from Silicon Valley to other important “data nations” in order to investigate the ambiguous and not-at-all-clear **connection between the use of digital data and the innovative capacity of economic and social systems**. However, we will not limit our analysis to technical and economic issues as the exploration of this ambiguous connection inevitably involves the fundamental political question concerning the *systemic competition* between liberal-democratic societies and authoritarian development models – in particular, that of the People’s Republic of China – with regard to the manner in which data is attained and used. To put it more pointedly, the question is: in times of omnipresent data generation and its use by increasingly AI-based systems, is the ability to innovate only to be had at the price of the complete disclosure of private data to governments and corporate actors? Or can an alternative approach, one balancing both the protection of basic rights and promotion of innovation, be found?

The study was carried out in collaboration with the National University of Singapore (NUS) and was supported by the country offices of the Konrad-Adenauer-Stiftung in Asia-Pacific. We selected **Hong Kong SAR, India, Japan, the People’s Republic of China, Singapore, South Korea, and Taiwan** as the contexts to be examined. We

looked at the areas of **transport, finance, administration, health, and Industry 4.0** to understand how added value for society and the economy can be created through modern data use.

We aim to contribute to the discussion on how to balance data usage and data protection in order to promote innovation in this digital age.

The following questions guided us in this study:

Narratives

How do companies, state actors, and civil society understand the handling of data – especially personal data – and the ethical assessment of such use? What are the prevailing narratives in each country?

Legal Bases

What are the laws and regulations that apply to the collection, use, storage, provision, disclosure, retention, and disposal of personal and non-personal data? What is the status of the development of legislation for these matters and how do different stakeholders deal with the issues of data protection and data portability between different (private and public) systems?

Ecosystem

Data is part of a larger “innovation ecosystem”. Its potential can only be realised through interaction with other innovation-promoting elements. What specific legal, technological, infrastructural, cultural, and economic aspects of a country shape the respective ecosystems and determine performance?

In Singapore, Japan, and Taiwan, the study is also supplemented by a representative population survey on data culture.

We hope that the diverse pictures presented on the subject of data and innovation in Asia will provide food for thought in Germany, Europe, and Asia itself.

Dr. Peter Hefele

Director Asia and the Pacific

1. **China's digital economy is one of the largest in the world.** Globally, nine of the top 20 technology companies are from China. China's digital economy contributed 39.2 trillion yuan in 2020, about 38.6% of national GDP (Global Times, 2021). China's access to large volumes of data is one of its biggest competitive advantages in the global digital economy.
2. In the past, domestic technology platform companies such as Alibaba, Tencent, Meituan, Didi Chuxing, encouraged by national policies and incentives, have contributed to the rise of digital economy, and played an unprecedented role in the national transformation from a manufacturing driven economy to a services and consumption driven economy.
3. It is until recent years that the Chinese government has shifted its policy and put more focus on tightening control over data flow and ownership since data has been elevated by the state as the fundamental factor of production which is an important and valuable strategic asset both for economic prosperity and national security.
4. The 2017 Cybersecurity Law (CSL), 2021 Data Security Law (DSL), and the expected soon Personal Information Protection Bill will form the foundation of the legal framework in China for regulating data flows and upholding data sovereignty.
5. Under the above legal framework and other related regulations, major technology platforms companies (e.g. Alibaba, Didi, Tencent etc.) have been investigated and were punished due to various violation including anti-trust, national security, finance, labour and consumer rights, and privacy.
6. **Case study 1: Ant Group** (formerly known as Ant Financial), a fintech platform that is the largest mobile payments and financial services provider with over a billion users, was made to suspend its expected world record IPO in November 2020 and was demanded by the authority to reform its business model due to its unfair competition and monopolistic behaviour which includes data monopoly. The Ant case confirms that the Chinese government is setting new standards for how its large data platforms will be managed with a greater role for the state.
7. **Case study 2: Didi Chuxing**, a leading car hailing tech giant, was placed under Cybersecurity Review by the CSL to guard against national data security risks and was forced to remove from app store, not long after Didi went public in the US in July 2021. As the investigation showed, Didi is considered a Critical Information Infrastructure (CII) which collects and generates personal information and important data and is required to undergo a security review if they wish to transfer data cross-borders.
8. In summary, this paper argued the **China's emerging data culture and its intention to uphold data sovereignty and national security by tightening control over domestic and cross-border data flows through evolving legal regimes.**

The global economy is undergoing a transformation widely recognized as the 4th industrial revolution made possible by data driven intelligent systems. Policy makers around the world are searching for new regulatory and governance frameworks to help societies manage the potential and risks these new systems bring to society. China is at the forefront of this challenge. Chinese policy makers are placing more focus on constructing legal regimes to govern data from both a national security and economic development lens. This paper aims to look at China's approach to data governance through the regulatory regimes emerging from efforts to govern its technology platform companies.

Local consumer technology platform companies such as Alibaba, Tencent, Didi Chuxing, encouraged by government national policies, have taken on an unprecedented role in the transformation of the Chinese economy from a primarily manufacturing driven economy to a services and consumption driven economy. In areas such as media and communication, finance, and mobility they can be seen as key infrastructure providers (Hong Shen 2019) with ownership of big data in these areas typical of surveillance capitalist business models observed around the world (Shoshana Zuboff, 2018). Several platform companies actively participated in national development initiatives, such as poverty alleviation, and scholar Julie Chen observed that platforms 'promoted a self-brand as social service providers' invoking techno-utopian visions of benefits to the economy. (Chen Julie, 2020). Now the relationship between platforms, consumers, and the state is going through a major transformation.

A number of regulatory arms of the Chinese state are introducing new laws and regulations aimed at consumer technology platforms in a range areas including anti-trust, national security, finance, labour and consumer rights, and privacy. In the past 12 months over a dozen companies have been fined or faced business restrictions under the aegis of anti-trust, privacy, and finance. Regulators opened investigations against the country's largest platforms including Alibaba, Meituan, and Didi Chuxing (Technode ChinaTechlash Tracker 2021). In a December 2020 China's top leaders vowed to 'contain disorderly expansion of capital, and ensure fair market competition' (Xinhua, March 2021). An influential Chinese academic in a newspaper opinion page said the age of 'barbaric growth'(野蛮) for technology companies has ended, and a new phase defined by rules and good systems, especially taking aim at platform companies abuse of their monopoly control over data (Fang Xingdong, July 2021). Several of the economic, security, social, and political interests behind this campaign is converging around data governance.

Part one of this paper draws an outline of the scale of China's public and private data ecosystem and the key tensions emerging around data. This is followed by a list of the key stakeholders involved in the creation, collection, processing, and governance of data in the People's Republic of China (PRC).

Part two 'articulating data sovereignty' looks at the evolving legal regimes in China that help shed light on the PRC's thinking of data sovereignty and two case studies that illustrate these laws and policies in action. In particular focus is placed on the Data Security Law (数据安全法) (DSL) set to be enacted on 1 September 2021. Building on the 2017 Cybersecurity Law(CSL) (网络安全法), and other administrative regulations, this new law bring new levels of details around how data is to be governed, including cross-border data flows out of the PRC, and data governance as an economic policy to promote data sharing within the economy. In addition to these laws industry specific regulations in areas such as finance and anti-trust are also discussed here as they pertain to explaining how the PRC is articulating data sovereignty.

Two emerging case studies in particular and reflect how Beijing intends to exert its influence on data flows and de-facto set the definitions and scope of the regulations. Ant Group, a fintech platform that is the largest mobile payments and financial services provider with over a billion users, was made to suspend its expected world record IPO in November 2020, due to concerns from Beijing and regulators. On 3 July 2021 Didi Chuxing, leading mobility tech giant, was placed under Cybersecurity Review “to guard against national data security risks. In the case of Ant a new regime may compel it share its data with a state-owned entity governed by the central bank (Lingling Wei, 2020). In the case of Didi new precedent may be set for a threshold on cross-border data transfers and foreign access to data. Observing these case studies are important because they set precedent and offer insight into how Beijing translates the high-level principles in its laws into implementable policy. The outcomes from both these cases will have far-reaching implications for how data is conceived and regulated not just in China but also globally.

In conclusion this paper will sum up the data cultures emerging in China broadly and what they say about the major trends that will influence the future of the Internet and data flows. In absence of global rules or frameworks for data flows, countries are creating their own models nationally.

Data is gaining recognition as strategic asset that needs to be managed in novel ways. Emerging literature shows that data as a good is different to physical items in that it is non-rivalrous i.e. data can be used an infinite amount of times and is partially excludable i.e. it is not always possible to exclude individuals from access to data (Liu Lizhi, 2021). While ‘data is the new oil’ is popular analogy, data differs from traditional assets such as oil or land in that it is non-rivalrous with increasing returns to scale. Creating the right framework of laws and regulations becomes of prime importance especially for countries with large digital economies.

The EU’s GDPR represents a citizen-centered approach to data flows while still enforcing strict obligations to store data locally and other region-based requirements. The US ‘free and open Internet’ moniker is also undergoing major changes. Today a regulatory movement aimed at curbing the influence of ‘Big Tech’ is in the US mainstream with a recent Executive Order on Promoting Competition in the American Economy calling for the FTC to establish rules on surveillance and accumulation of data (White House Executive Order, July 2021). The US cited ‘access to data by an adversary’ as one of its key concerns over the operation of Tik Tok in the US (White House Fact Sheet, June 2021). There is recognition that a combination of domestic and external changes calls for a change in posture. The conventional ‘open vs closed’ binary lens that has long been used may be waning in relevance to classify and evaluate data governance (Sam Sacks and Amba Kak, 2021).

The age of light regulations for global technology companies is now in the past. While China’s political system may differ from western democracies the challenges are very similar. In this new age of data sovereignty, China’s economic and political success brings legitimacy to its approach to governing data flows and will go on to have a major influence on the evolution of the global Internet.

China's digital economy is one of the largest in the world. Globally, nine of the top 20 technology companies are from China (Sally French, 2018), in time several of the 266 unicorn companies may join this list. Everyday life for majority of Chinese citizens, from commerce and entertainment, to transport and finance, is mediated by these platforms to a degree not matched anywhere in the world. In 2018, 760 million Chinese participated (i.e., consumers) in the "sharing economy" while 75 million participated as service-providers (i.e., gig workers and vendors) (National Sharing Economy Research Center, 2019). Each interaction online produces data: approximately 7.8 trillion gigabytes (GB) of data in 2018, a figure expected to reach 48.6 trillion GB by 2025, surpassing the USA (Roy Sahel, 2018). China's digital economy contributed 39.2 trillion yuan in 2020, about 38.6% of national GDP (Global Times, 2021). China's access to large volumes of data is one of its biggest competitive advantages in global competition in the digital economy (Kaifu Lee, 2017).

In the past five years the Chinese government released a variety of long-term plans for developing global leadership in strategic areas such as artificial intelligence (AI) as well as accelerate development of manufacturing 4.0, Cloud computing, and Blockchain technology, all of which rely heavily on leveraging data. The State Council of China, the country's premier policy planning agency, and the Central Committee of the Communist Party of China (CCP), elevated data as the '5th factor of production' alongside land, labor, capital, and technology, intended to "injecting new impetus to promote high-quality development and foster innovation-driven development" (Ouyang Shijia and Chen Jia, 2021). These steps follow a sustained period of government investment in digitizing in the public sector.

The State Council of China and the Central Committee of CCP, elevated data as the '5th factor of production' alongside land, labor, capital, and technology.

Public data is an indispensable part of 'big data' and local governments across the country too have invested resources towards the digitization and bringing in more data into government bureaucracy. Central and local level governments, following the lead of various national plans such as Big Data, Social Credit System (SCS) and Smart Cities, have invested in infrastructure to operationalize the collection and processing of public data. For instance, cities and provinces have created what are known as Public Credit Information Platforms to 'aggregate data generated from public management functions by various departments and units' (China Copyright Media, 2014). In the last couple of years, more than 46 open government data portals have been set up by governments, intended to include a variety of datasets such as administrative penalties, administrative licenses, land ownership, tender notices, credit rating, corporate credit, foreign business, revocation, credit services and rights protection (Xiao Diyu, 2019). The SCS has catalysed the Chinese government's efforts to digitise and pool public data, particularly within the realm of administrative regulations and laws, towards its use as a form of reputation in government decision-making around allocation of resources and services (Xin Dai, 2018). Local governments have introduced smartphone apps to modernize their relationship with citizens and better collect data. The government of Guangdong, the third largest province by economic size, developed an app *Yue Sheng Shi* to enable residents to access more than 500 municipal and public services online, such as paying social security fees. Between 2018–19 a handful of cities, such as Xiamen, Fuzhou, and Suqian, rolled out city-level personal

credit scores, as part of a pilot program to bring some level of fringe benefits to local residents as a reward for law abiding behaviour (Lewis, 2020). While digitisation within the public sector remains unevenly distributed regionally and within government, these efforts are evidence of the progress the Chinese state has made operationalizing data within the public sector.

An official recently remarked the speed of technological change progresses faster than the law and the state is now moving to address this gap. Over the years various issues around technology platforms and societal harms have steadily grown in size and significance. Data leaks and selling of personal data on black markets, overbearing collection of personal information by companies exposed the need for and lack of adequate legal regulation and proper safeguards. Competition between tech platforms led to companies locking each other out of each other's ecosystems and poor interoperability (Ruima, 2021). There is growing anti-trust regulatory movement in China that seeks to shift China's economy from a stage of rapid growth to 'high-quality development' (Zhuang Rongwen, November 2019).

Most critically for data governance, domestically China's large digital economy continue to resemble a collection of data islands with platform companies in possession of personal and non-personal data being proprietary ownership. Even within the public sector data sharing between regional governments or government bodies is a long standing challenge. This has two economic implications. First, there may be substantial social gains if data is widely shared across firms and countries. Second, on the other hand, if data is not broadly shared, the quantity held by a firm or country can generate a competitive advantage (Liu Lizhi, 2021).

Most critically for data governance, domestically China's large digital economy continue to resemble a collection of data islands with platform companies in possession of personal and non-personal data being proprietary ownership.

This is increasingly a source of friction with state policies calling for 'accelerating the share of data resources' within the Chinese economy (MIIT White Paper Big Data). Experiments to facilitate data sharing in the credit sector between leading fintech platforms and state entities failed to deliver desired outcomes. While data governance was an economic priority, it has not yet established a clear data verification system: No systematic social governance rules have been formed to oversee data sharing responsibilities, technological development, data management and data security. Tensions are emerging around the relationship between public and private ownership of data. This tension is discussed in the Ant Group case study. While the global expansions of Chinese company footprint, either through public listings in the United States or through servicing consumers, have put them increasingly at odds with domestic compulsions, a tension scholar Liu Lizhi describes as "the deep versus broad dilemma problem", seen in the Didi Chuxing case study.

Key Stakeholders for Data Governance

Data Processors

Platform Companies (consumer- and business-facing)

- China's consumer- and business-facing platform companies are among the largest in the world and several companies exert monopoly or oligopoly-like control in respective industries: Tencent Holdings (instant messaging and gaming), Alibaba, Ant Group, JD.com, Pinduoduo, Bytedance, Didi Chuxing, Huawei.
- China's industrial Internet (business-facing sectors) are growing fast with consumer giants such as Alibaba and Tencent joined by Huawei and hundreds of business-facing providers of technology solutions in areas such as Big Data, Smart Cities, Artificial Intelligence, Autonomous vehicles, Drones, etc.
- These companies are increasingly seen as operators of critical infrastructure and processors of critical and important data.

Government (city/ province/central)

Information departments of all levels of government in China are the promoters of digital innovation in the public service sector. For example, Guangdong has established the Government Service Data Administration Bureau at the provincial, municipal and county levels, which is responsible for the management of government organisation information and government service informatisation. The central government has a guiding role for local governments in data sharing, data opening, development and innovation.

Data Regulators

Platform Companies

Products and platforms de-facto set rules and standards on what data is collected and processed.

The Office of the Central Cyberspace Affairs Commission (CAC)

- The CAC plays a key policy coordination role with various other industry-specific regulators with growing authority and importance. It is among the newest regulatory actors first formed as part of the administrative office of the Central Cybersecurity and Informatization Commission, which is chaired by Xi Jinping.
- The CAC is responsible for designing and implementing the Cybersecurity Review Measures, based on the CSL and is assigned a policy coordination role in the DSL draft, reinforcing its authority as an interagency tie-breaker and a battleground, as well as a turf war combatant in its own right. (Digi China, 2021).

Ministry of Industry and Information Technology (MIIT) and the State Administration for Industry and Commerce (SAIC)

They are mainly responsible for the approval and supervision of website operating licenses and the supervision and management of network information security technology platforms. MIIT is one of the chief agencies behind national plans such as the AI 2030 strategic plan, Made in China 2025, among other important plans that set the roadmap at a national level.

The Ministry of Public Security (MPS) and the Ministry of National Security (MNS)

The security control departments of the Internet. They are mainly responsible for the monitoring of harmful information online, cracking down on online illegal activities, putting forward a list of blocked websites for harmful information abroad, and notifying relevant departments to block the websites. The MPS has been responsible for criminal investigations of data breaches and is likely to continue in this capacity. Sector-specific regulators largely focus on day-to-day oversight and matters specific to their field. But remaining overlaps could still lead to conflicts, especially if the MPS takes a more hardline security approach in contrast to more commercially oriented regulators, for instance the financial sector power center at the People's Bank of China (New America) and Multi-Layer Protection Scheme certification system (led by MPS).

Data Regulators

State Administration of Market Regulation (SAMR)

SAMR is not a major player in the game of data governance regulations. However, there is an overlap in its remit as the key regulator for enforcing anti-monopoly law on major technology platforms. Big Data is increasingly viewed as a factor that should influence the process of identifying monopolies and to that effect the SAMR will have a role to play in regulations that will target large platform's monopoly control of data.

The Ministry of Finance (MOF) and the People's Bank of China (PBOC)

The MOF and PBOC are key players for regulating financial data which is one of the key industries under the data regulatory scrutiny, as it relates to financial risk as well as private control of financial data by technology firms such as Ant Group examined in this paper.

Framing Data Sovereignty: Security and Economic Development

The Cybersecurity Law (CSL) (网络安全法), which was enacted in 2016 and came into effect in 2017, is the foundational law governing data flows in China.

While a Personal Information Protection Law (PIPL), dealing exclusively with personal privacy, is approaching its third and final reading soon, a new Data Security Law (DSL) exclusively focused on managing data flows, has already been passed and will be enacted in September 2021. Together these three sets of laws are expected to be the cornerstone of data regulations in China on top of which other industry-specific regulations will be built. From these laws together with a growing volume of government documents and administrative regulations, the contours of Chinese government thinking of data sovereignty can be framed.

Twin Purpose: Economic Development & Security

Data is viewed as a resource from both a security and economic lens. Two articles in the DSL highlight this: "The State firmly places equal emphasis on safeguarding data security and promoting data development and use." (数据开发利用) (Article 12). According to a figure who contributed to the drafting of the DSL "the two go hand in hand" (Sam Sacks & Amba Kak, 2021). The level of importance afforded to development is also reflected in the elevation of data as the '5th factor of production' alongside land, labor, capital, and technology.

Regulations and policies around data are increasingly going beyond national security and personal data protection towards economic thinking around improving open competition and innovation. The DSL calls for the creation of a 'data market' to support exchange of data as a resource within the economy, the first law to bring up this concept which is growing over time, captured in Article 17 "The State establishes and completes data exchange management systems, standardizes data exchange activities, and cultivates a data trade market." (数据交易管理制度,规范数据交易行为,培育数

据交易市场)。This suggests that Beijing is paying attention to the economic value of data and productivity gains from freeing up data as a resource and not allowing China's vast data resources to sit idle (Graham Webster, Sam Sacks Qiheng Chen, 2021). The Shenzhen government passed a data regulation that will go into effect on January 1 2022 that requires government to make its data available to public for free and by default with non-sharing by exception (Data Regulations of Shenzhen SEZ 8 July 2020). On 11 July at the sidelines of the World AI Conference in Shanghai a National Data Exchange Alliance was announced between 13 provincial governments to 'jointly promote the construction and development of the data exchange market' (Li Lanqing, July 2021).

This suggests that Beijing is paying attention to the economic value of data and productivity gains from freeing up data as a resource and not allowing China's vast data resources to sit idle.

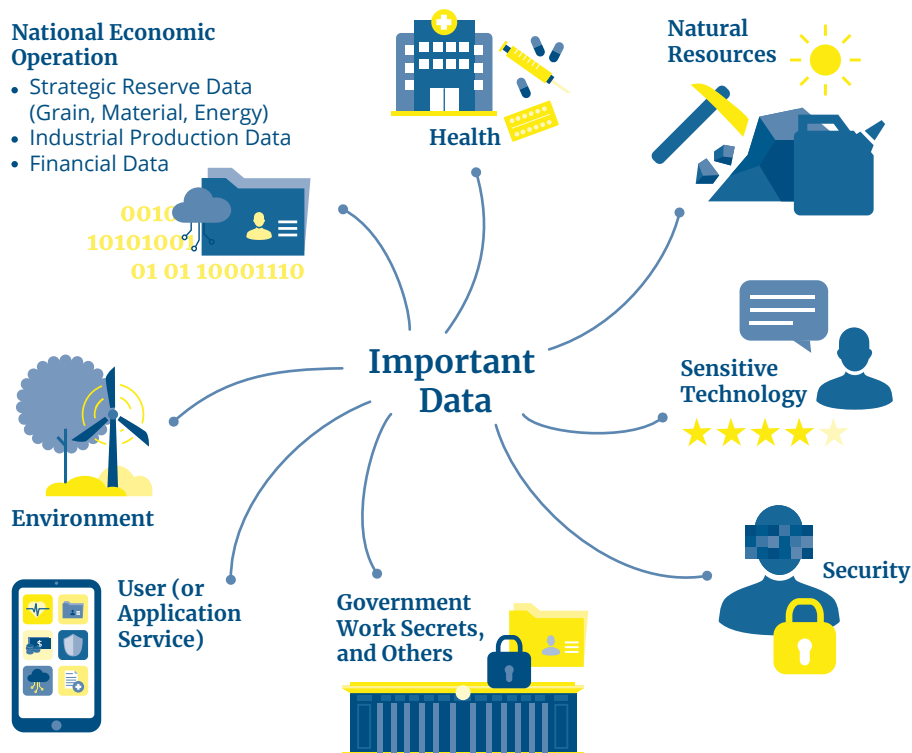
Controlling Cross-border Data

The CSL calls for the establishment of a data security review system for data activities that effect national security (Article 22) and export controls on data belonging to controlled agencies to carry out international duties and safeguard national security (Article 23). Understandably, global attention was attracted by the mention of regulating cross-border data flows due to implications for foreign companies operating in the PRC. The concept of regulating cross-border flows was a relatively novel idea at that time when data sovereignty as a concept had yet to enter mainstream global media discourse. The CSL itself provided little details about how that would be implemented and parts of the law that pertained to cross-border flows were not expected go into effect until a later period giving authorities more time to formulate solutions. Proposed amendments to Cybersecurity Review Measures added as considerations for assessing national security risks (*Article 10*): "risk that core data, important data or large amounts of personal information are stolen, leaked, damaged, or illegally used or imported...the risk that after foreign listing CII (Critical Information Infrastructure), core data, important data, or large amounts of personal information are affected, controlled, or maliciously used by foreign governments". One of the first cases of the application of these reviews with Didi in July 2021 is discussed later in this paper.

Data Classification

A key tenet of the CSL is the introduction of hierarchies in classification of data. The CSL introduced the idea of ‘important data’. The DSL added a further level of detail introducing ‘data types’ and ‘data grades’ as types of classification and takes a next step forward by calling for a framework for the formation of data classification that would delineate the different types of data for different treatments under different laws. A forthcoming “important data” standard led by Zuo Xiaodong (an influential cybersecurity expert and vice president of the China Information Security Research Institute), will aim to define what constitutes important data at a more granular level.

In an article shared some elements of his thinking that serves as a preview. Luo Xiaodong gave a set of basic classification methods for important data. He suggested dividing important data into eight categories. One example he suggested is shown below.



Scholars Sam Sacks and Amba Kak observe that the meanings of the term ‘important data’ is the subject of intense debate domestically over the question of a broad or narrow definition. In the future data classification in China could consist of overlapping schemes made up of both laws and sector-level standards.

Data Ownership: State vs Private Frictions

'Big data' is discussed as a potential determined for defining monopoly status in the digital economy as part of the developing anti-trust regulatory campaign. Rustling beneath the surface there are important debates within government and academia around the role of personal data in society, its relationship between citizens, who are the legitimate owners (people or companies or the state), and the challenge of unlocking wider societal benefits from data. One scholar at Xiamen University, Zhao Yanqing, openly questioned whether platform's ownership of data is equal to exclusive right to process data. He called for the State play a more decisive role in the operations and leadership of platforms (公进民退) through various forms of shareholder participation in the newly carved out 'big data' platform entities. The 'application' entities remain privately owned. According to Zhao platforms have the right to provide services and develop applications but the data itself belongs to the people. Zhejiang University scholar Fang Xingdong writes exclusive access to data is seen by some as non-competitive behaviour (Fang Xingdong, July 2021).

Rustling beneath the surface there are important debates within government and academia around the role of personal data in society, its relationship between citizens, who are the legitimate owners (people or companies or the state), and the challenge of unlocking wider societal benefits from data.

The regulatory approach to Ant Group, the leading fintech company and holder of important financial credit data reflect the nature of several of these debates.

Case 1

“Nationalizing” Ant Group’s data

Ant Group (formerly known as Ant Financial; referred hereafter as ‘Ant’) is a financial-technology platform company formally founded as an independent entity in 2014 – although it’s origins date back to the creation of a payment network Alipay as a part of Alibaba Group in 2004. Today Ant has over 1 billion users – including 751 million monthly active users – and is one of the largest technology platforms reporting a revenue of US\$10.5 billion netting a profit of \$3 billion during the first half of 2020 (Stella Yifan Xie, Jing Yang, August 2020). Ant can be considered an indispensable provider of financial infrastructure in China (Hong Shen, 2019).

Ant’s service offerings can be divided into four segments all packaged within its main app Alipay:

1. **Payments:** Alipay is the largest mobile payment network in China with an estimated 44% market share in China handling US\$ 40.8 trillion worth of transactions in 2020 (Jane Zhang, January 2021).
2. **Lending:** Its lending services allow consumers defer payments through monthly installments (*Huabei*) and borrow small to large sums of money (*Jiebei*) usually aimed at small businesses. Over a 400 million people use these services which make up 15% of China’s consumer lending market (Economist, 2020)
3. **Asset Management and Insurance:** Ant began by offering a money market fund (*Yue’r bao*) for consumers to park any excess funds offering higher interest than traditional banks. Yue’r Bao is now the world’s largest money-market by size and is joined by thousands of 3rd party offerings by other companies on Alipay.
4. **Risk Assessment:** Sesame Credit, a credit rating system for all users based primarily on Alipay transaction data captured through the Alibaba-Ant ecosystem of products and services. The Sesame Credit score is a determinant to access of services and borrowing and lending within the platform.

Data Assets

Ant's data assets from its 1 billion users can be split into the following categories:



- Consumer payment data
- Business payment transactions
- Consumer and business credit and loan repayment
- Investment and insurance purchases

Mobile payments in urban China are ubiquitous used for nearly every payment transaction a person makes in both online and offline settings. With Ant making up nearly half of the entire Chinese mobile payment market the data generated from the interactions between the hundreds of millions of consumers, vendors, and businesses within its ecosystem gives it a unique vantage point into the Chinese economy and lives of Chinese citizens. Access to this data also drives Ant's financial products and services, which generate the bulk of its revenue.

Regulating Ant

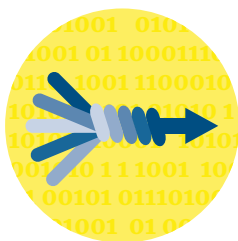
Ant's rise raises a variety of regulatory questions around its role as a privately owned platform that performs a critical public utility and has proprietary ownership of important data of Chinese citizens and businesses. Is Ant a tech company or a bank? Is Ant a monopoly? What are the risks it may pose to the financial systems?

Ant is now at the center of an on-going tug of war with government regulators. The outcome of these processes will go on not just to define how fintech is regulated but also how ownership and usage rights of data in China is thought off. The questions and concerns have persisted for several years, however, on-going regulatory decisions have been accelerated due to events surrounding Ant's now suspended world record breaking initial public offering (IPO) in Hong Kong and Shanghai which was expected to raise more than \$30 billion fetching a market capitalisation of US\$ 313 billion in November 2020.

Days before Ant was meant to go public, the Shanghai STAR stock exchange announced the IPO would be suspended, following which Ant froze its Hong Kong IPO (Anshuman Daga, 4 November 2021). This announcement was made after China's top financial regulators called in founder Jack Ma and Ant's executives for meetings and new draft regulations on regulating online lending by the PBOC were released publicly (Reuters, November 2020). Officially, concerns around risks to China's financial system were raised and the involvement of the PBOC in drafting the related regulations reflects this (Xinhua, December 2020). Prior to the suspension of the IPO several senior officials from within China's banks and financial regulators penned op-eds calling for more supervision over fintech, blaming technology companies for using data to gain unfair advantages, tricking consumers into debt, and posing serious system risks to the financial system if left unregulated (Eliza Gkritski, November 2020).

As part of financial risk, concerns around Ant's monopoly position and open competition were raised, bringing in Ant's data moat. Future supervision of Ant will include "resolutely breaking monopolies, rectifying, investigating and punishing unfair competition to safeguard a sound market order" (Xinhua, December 2020).

Reports citing unnamed government advisors claimed authorities want to 'break the company's monopoly over data' with one plan considered would require Ant feed its data into a nationwide credit-reporting system run by the central bank (Lingling Wei, January 2021). These mooted solutions come after years of unresolved tension between Ant and the PBOC over data sharing and reflect the legal and regulatory thinking around emerging data and anti-monopoly regulation discussed in the earlier section.



Data Tension: Monopoly Control over Data

Ant's data includes 44% of all mobile payment transactions as well as credit and lending for hundreds of millions of individuals and businesses. These data sets are difficult for the China's central bank to include in its own supervision efforts and hinders its own efforts at building a credit score system, and requisite for a functioning borrowing and lending system. For instance, the PBOC launched the second generation of its personal credit score reports and claims to now have financial data of one billion people, 26 million companies and entities, and 3,500 banks and financial entities.

Initially some fintech firms, including Ant, were given temporary credit reporting licenses by the PBOC in 2016 however they were not renewed. Ant's Sesame Credit is a market leader and China's first company using online 'big data' for credit scoring in 2015, and several Internet companies also have their own scores, joined by a growing number of specialized credit risk companies, such as Supetech (Alibaba Group, 2015). Sesame Credit was seen primarily as a commercial score that prioritized user consumption on its platform and the PBOC was hesitant to allow it to act as a formal credit reporting agency. These firms continue to provide credit scoring schemes for their own commercial schemes. To bridge gaps between public and private entities, the PBOC set up an entity called Baihang Credit (百行征信) that began operations in March 2018, consisting of 8 fintech companies, including Ant and Tencent, each owning 8% along with the Internet Association which holds 33%. **Baihang is self-described as a market-based and aggregates data from private companies in China and issues its own credit risk report** (About us, Baihang Credit). On 11 January 2020 it publicly released a pilot version of its personal credit report and claims to have partnerships with 1,070 companies, including mostly peer-to-peer (P2P) firms, with data that includes more than 71.4 million borrowers and 112 million credit accounts. (Yuandian, January 2020). However, Ant and Tencent have not been as forthcoming with sharing data within Baihang.

Ant had agreed to provide some information to a state backed database on its 500 million customers who have taken out loans. However, despite the setup of Baihang with Ant as a founding shareholder, comprehensive data sharing has yet to materialize. Media reports in 2019 raised the issue that Tencent and Alibaba are refusing to co-operate with Baihang and are withholding access to customer loans data (Yuan Yang, Nian Liu, September 2020). More recent reports say Ant only submitted limited data sets to the PBOCs Credit Reference Center.

Ant is now at the center of regulatory scrutiny that includes both the PBOC and SAMR, the main anti-trust regulator, which recently placed a US\$ 2.5 billion fine on Alibaba and Tencent for monopolistic behavior (Xinhua, 14 December 2020). In December an investigation into Ant involved both the PBOC and SAMR. As a company it firmly falls within the scope of an operator of CII and handling 'important data'. In December the investigation into Ant by the PBOC put forward requirements for Ant: "First, return to its origin of payment business, enhance the transparency of transactions, and strictly prohibit unfair competition ... Second, operate personal credit rating business with a legal license and compliant with laws and regulations, and protect the privacy of personal data ... third establish a financial holding company in accordance with the law" (PBOC, 27 December 2020).

What a new and reformed Ant will look like will become clearer in the coming months and beyond. In April Ant announced it will apply to become a regulated financial entity and place all of its financial related information in this regulated entity overseen by the PBOC. In forums and media there has been discussion about Ant broken up into two entities including a 'big data' platform entity that would be jointly run by the state [Zhao Yanqing, November 2020]. It remains to be seen what the new entity will look like and what it will mean operationally for Ant's data. A new set of draft rules on monopolies from the PBOC shared in January say if an investigation confirms monopoly status the PBOC can recommend a range of corrective actions ranging from suspension of a serve to the 'breaking up of an institution by "business type"'. The PBOC definition for a monopoly is any nonbank payment provider with a market share of 50% in electronic payments making Ant very much within its scope with 55.59% of the third party mobile payments as of the second quarter of 2020 (Xinhua, 21 January 2021).

The Ant case study so far confirms that the Chinese government is setting new standards for how its large data platforms will be managed with a greater role for the state. Jack Ma had famously said if the banks don't change he will disrupt the banks. Having successfully achieved this, the phase for disruption appears to be giving way to regulation. The rules created for Ant Group will ultimately be imposed on all other companies in finance but also other industries.

Jack Ma had famously said if the banks don't change he will disrupt the banks. Having successfully achieved this, the phase for disruption appears to be giving way to regulation.

Case 2

Didi Cyber Security Review

Didi Global is China's largest mobility technology platform offering app-based services operating in 4000 cities across 16 countries, employing 15 million drivers, and serving with 393 million users (Didi Prospectus, 2021). Didi is ubiquitous in China making up 85% of the app-based hiring market offering a range of transportation services from a variety of private taxis, bike sharing, public transit, carpooling, food delivery, logistics, and financial services. Didi is also developing autonomous vehicle technology with a dedicated R&D subsidiary that completed two funding rounds raising US\$ 825 billion (Caixin July 2021). Didi went public on the US Stock Exchange on July 1 raising US\$ 4.4 billion. the largest Chinese IPO in the US since Alibaba in 2014.



Data Assets

- **Payments:** payment transactions of its 393 million Chinese consumers
- **Mobility:** ride data of passengers including locations, real-time mobility data of traffic across China (25 million rides per day).
- **Mapping:** geography, location data, high resolution maps as part of autonomous driving research.

The next day, on July 2, the Cyberspace Administration of China (CAC) announced an investigation into Didi "to guard against national data security risks, safeguard national security, and ensure public interest" (CAC, 2 July 2021). Under the terms of the investigation Didi would be suspended from onboarding any new users or drivers until the investigation concluded. Its main Didi app, along with 24 other of its applications serving drivers, freight service, and others, were removed from all app stores, including access to Didi's mini programs within Wechat and Alipay. Existing

users would be allowed to continue using Didi without any change. Later the CAC announced an on-site investigation of Didi took place at their Beijing headquarters including 6 other regulatory bodies the State Administration for Market Regulation, the ministries of public security, state security, transport and natural resources, and the State Administration of Taxation (Nikki Sun, July 2021).

The investigation into Didi sheds light into the black box of how the CSL and newly enacted DSL will be enforced to manage cross-border data flows. It will also have major implications for large Chinese technology companies and the Chinese government weighs national security concerns.

Data Tension: National Security

This is the first investigation into a company under the “Cybersecurity Review Measures” listed in the CSL and thus sheds important light into how these measures are being applied.

The original list of “Cybersecurity Review Measures” were released publicly in June 2020 with a focus on CII operators procuring ‘networked products and services’ such as “core network equipment, high-performance computers and servers, large capacity storage devices, large scale databases and application software, cloud computing services, cybersecurity equipment, and other important network products and services that have importance influence on the security of CII” (Cybersecurity Measures, Digi China). While data risks are an implied focus, for instance, vulnerabilities in the hardware supply chain allow for data theft, the purported focus of the measures was cybersecurity and supply chain integrity not data flows. Any doubt around the focus on data flows was dispelled a few days later when the CAC announced new proposed draft amendments to the Cybersecurity Review measures on July 10.

The new draft includes the following amendments relevant to data flows:

- The newly enacted DSL is added as the legal bases (along with CSL)
- “Data handlers conducting data handling activities” is added to the scope alongside CIIs procuring networked products and services.
- The following factors are added as considerations for assessing national security risks (*Article 10*): “**risk that core data, important data or large amounts of personal information are stolen, leaked, damaged, or illegally used or imported ... the risk that after foreign listing CII, core data, important data, or large amounts of personal information are affected, controlled, or maliciously used by foreign governments**”.
- Firms handling the personal data of more than 1 million users need to report for review from CAC before an IPO overseas and the China Securities Regulatory Commission (CSRC) has been added as a regulatory body.

This investigation can be seen as confirmation that Didi is considered a “CII operator”. According to Article 37 of the CSL, CII operators are required to store personal information and important data collected and generated during operations within territory of China and to undergo a security review by corresponding authorities if they wish to transfer data across borders.

The high sensitivity around foreign listing and data sharing is clear. The new regulations now de-facto require for any technology company listing to undergo an up-to three-month review first. This is also borne out of the fact that in the same week two more Chinese tech companies Boss Zhipin and Yunmanman and Huochebang – two truck-booking apps with recent IPOs in the US were placed under a similar investigation and ordered to stop registering new users.

Up until now, the implications for the CSL were mainly felt domestically with most fines and investigations targeting illegal behavior within China. With the Didi investigation China's threshold for cross-border data flows and sensitivity to data is clear. If China's focus since the advent of the Internet has purportedly been towards keeping foreign companies and information outside China, the Didi case may be a landmark shift to keeping data within China from leaving the PRC.

The influence of geopolitical context and on these measures should also be taken into consideration. Over the last few years policies from both the PRC and the US are increasingly aimed at cutting exchange of capital between Chinese and American companies as part of a so called 'de-coupling' between the US and China. A number of prominent Chinese companies across industries have been added to US 'blacklists' preventing access to US companies and financial markets in general. China's Ministry for Commerce added 23 items to its 'export control list' including 'personal information push services based on data analyses' (Reuters, August 2020). This announcement was made at a time when Tik Tok was in negotiation with divesting its US business to American investors under the terms of then US president Trump. The heightened concerns around foreign IPOs may be linked to the new "Holding Foreign Companies Accountable" Act passed into US law late 2020 and would involve sharing data to comply with this law that requires foreign companies to comply with domestic accounting and reporting regulations.

At the time of writing the Didi investigation has only just begun with a provision for up-to 90 days period of investigation according to the latest Cybersecurity Review amendment. The manner in which these new amendments were announced suggests that it is not inconceivable in the coming weeks and months more rules influenced by the Didi investigation will be introduced. The CSL and DSL spell out a range of punishments from large fines to suspensions of operations. An escalation of measures around handling of important data may conceivably go on to include the national identity the investors in major companies. Didi shareholders include prominent foreign investors such as Softbank and Uber. Other companies such as Alibaba and Tencent have a significant equity owned by foreign investors. Chinese technology companies have traditionally flouted Beijing's strict laws on foreign investment through a convoluted legal structure known as Variable Interest Entity (VIE). Such a move by the Chinese state to legally crackdown on such arrangements would be an extreme measure that would bring considerable economic pain to all involved, including China. On the data governance front, sharing data custody and ownership with State Owned Enterprises, the model emerging with Ant Group, may also be applied to Didi. As the largest mobility platform in China now listed in the US the fate of Didi will be watched closely by investors and policy makers in China and around the world. The outcome will have implications for China's tech ecosystem and global data governance.

Emerging Data Cultures in China

The phase of unregulated, fast growth in the consumer technology sector in China, where private technology companies were encouraged with a relatively free reign to expand and innovate has now firmly transitioned into a regulatory phase. The 2017 Cybersecurity Law, 2021 Data Security Law, and expected soon Personal Information Protection Bill will form the bedrock of the legal regime governing the Internet and data flows in China. Industry-specific regulations will gradually add more levels of detail. While national security was once the starting point it is now also joined by the desire to purpose data flows for economic development. Data is now recognized within the Chinese state bureaucracy as fundamental economic factor of production which further incentivizes policy makers to better utilize China's vast data resources to unlock wider economic gains and benefit for society. China's anti-trust regulator is scrutinizing China's large platforms tasked with protecting consumers from harm, and promoting fair competition. Large fines have been levied on several companies and future regulations on anti-monopoly behaviour may target companies perceived to be data monopolies. At the political layer the Communist Party of China's monopoly on political power and control within the PRC is always a factor in debates about private vs public capital and ownership go back to the founding of the PRC and the reform and opening up period in 1978. The on-going investigations into Ant Group and Didi are discussed in this paper offers a window into how China will implement existing regulations or draft new ones that will go on to be applied to the rest of the industry.

Ant Group is recognised as a key infrastructure provider in China's financial technology industry and presents several challenges for the Chinese government. Identifying the key risks to China's financial industry and applying the necessary fixes without hampering the very innovations that defines the company is not straight forward. Jack Ma in his speech at the Bund Summit in Shanghai in 2020 called for new paradigms and ideas instead of relying on frameworks of the past. The Ant case study also represents the unique tension between the Chinese party state and private industry and the importance of data in the equation. The type of formal arrangements that Ant enters to with authorities with respect to sharing or opening its data will go on to influence similar arrangements in other industries. While the investigation into Ant reflects the domestic dynamics and data flows and risks, the Didi case reveals the dynamics of cross-border data flows and national security.

While the investigation into Ant reflects the domestic dynamics and data flows and risks, the Didi case reveals the dynamics of cross-border data flows and national security.

Didi is the first company to be investigated under the Cybersecurity Measures and fresh changes are being made to expand the scope to cross-border data flows. While the investigation has only just begun new draft rules already reveal the sensitivities of foreign listings and perceived threat of data being misused by foreign governments. It remains to be seen how this may retroactively be applied to Chinese companies already traded on US markets however this will certainly affect companies with future plans to IPO in foreign markets and as a consequence their market valuation and ability to raise capital. Naturally, there will also be implications for foreign companies operating in these sensitive industries within China, with either blanket bans or high compliance and restrictions. This case is a good example of the

“deep versus broad” dilemma that Chinese companies face according to Liu Lizhi i.e. it is necessary to build deep political connections in the Chinese market but which then takes a toll on their global expansion. This is felt more acutely going forward as the US-China “de-coupling” escalates.

For decades laws and regulations for the Internet were seen as an anti-thesis to the foundational values of the Internet especially in the US which promoted the idea of ‘free and open’ Internet. Several events in the recent past such as Edward Snowden’s NSA leaks expose of US government surveillance, the Cambridge Analytica-Facebook illicit use of personal information, and a growing number of several cyber hacks has shown that technology companies, just like companies in all other industries, must be regulated. While the EU was a relative early to introduce the GDPR it lacks large home-grown technology companies within its own jurisdiction to be able to enforce its values and laws. China was among the first to recognized the concept of data sovereignty. However its modern legal system does not have a long history of formulating laws and regulations for a market economy. Chinese policy makers continue to simultaneously look globally for best practices to inform their own emerging model for regulating data flows domestically and cross-border. These models should be studied carefully by global companies and policy makers.

China was among the first to recognized the concept of data sovereignty. However its modern legal system does not have a long history of formulating laws and regulations for a market economy.

- A Ant Group** (2021, July 11). Ant Group – About Us. Retrieved from <https://www.ant-group.com/en/about>.
- C Chen, Julie Yujie** (2020, April 2). The Mirage and Politics of Participation in China's Platform Economy. *Javnost – The Public* 27, no. 2: 154–70. Retrieved from <https://doi.org/10.1080/13183222.2020.1727271>.
- China Law Translate** (2014, June 14). [Translation] Planning Outline for the Construction of a Social Credit System (2014–2020) China Copyright and Media. Retrieved from <https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/>.
- Choudhury, Saheli Roy** (2019, February 14). As Information Increasingly Drives Economies, China Is Set to Overtake the US in Race for Data. CNBC. Retrieved from <https://www.cnbc.com/2019/02/14/china-will-create-more-data-than-the-us-by-2025-idc-report.html>.
- Cyberspace Administration of China (CAC)** (2020, April 16). 《网络安全法》实施两周年：发挥立法作用提供执法依据-中共中央网络安全和信息化委员会办公室. Retrieved from http://www.cac.gov.cn/2020-04/16/c_1588583174366842.htm.
- Cyberspace Administration of China (CAC)** (2021, July 10). 国家互联网信息办公室关于《网络安全审查办法（修订草案征求意见稿）》公开征求意见的通知-中共中央网络安全和信息化委员会办公室. Accessed July 13, 2021. Retrieved from http://www.cac.gov.cn/2021-07/10/c_1627503724456684.htm.
- Cyberspace Administration of China (CAC)** (2021, July 2). 网络安全审查办公室关于对“滴滴出行”启动网络安全审查的公告-中共中央网络安全和信息化委员会办公室. Retrieved from http://www.cac.gov.cn/2021-07/02/c_1626811521011934.htm.
- D Daga, Anshuman** (2020, November 5). “Timeline: Key Events behind Suspension of Ant Group’s \$37 Billion IPO.” *Reuters*, sec. Business News. Retrieved from <https://www.reuters.com/article/uk-ant-group-ipo-suspension-events-idUKKBN27K1A0>.
- Dai, Xin** (2018). Toward a Reputation State: The Social Credit System Project of China. *SSRN Electronic Journal*. Retrieved from <https://doi.org/10.2139/ssrn.3193577>.
- E Eliza, Gkritski** (2020, November 9). The Unsigned Op-Eds That Foreshadowed Ant Group Fiasco · TechNode. TechNode. Retrieved from <http://technode.com/2020/11/09/china-voices-the-unsigned-op-eds-that-foreshadowed-ant-group-ipo-suspension/>.
- Emma, Lee** (2020, March 9). Brands Turn to Livestreaming as China Stays Home. TechNode. Retrieved from <https://technode.com/2020/03/09/insights-brands-turn-to-livestreaming-as-china-stays-home/>.
- Emma Rafaelof, Rogier Creemers, Samm Sacks, Katharin Tai and Kevin Neville** (2021, July 2). Translation: China’s ‘Data Security Law (Draft)’. New America. Retrieved from <http://newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-data-security-law-draft/>.

- F Fang, Xingdong** (2021, July 6). 方兴东: 中国互联网企业需补上‘合规’欠账. Global Times. Retrieved from <https://finance.sina.com.cn/tech/2021-07-06/doc-ikqci-zyk3929049.shtml>.
- G French, Sally** (2018, May 31). China Has 9 of the World's 20 Biggest Tech Companies. MarketWatch. Retrieved from <https://www.marketwatch.com/story/china-has-9-of-the-worlds-20-biggest-tech-companies-2018-05-31>.
- Gao, Henry** (2021, July 9). Data Regulation with Chinese Characteristics, n.d., 29.
- Graham, Webster** (2021, July 2). Translation: CAC Announces ‘Cybersecurity Review’ of Ride-Hailing Giant Didi, Just After Its IPO | DigiChina. Digi China. Retrieved from <https://digichina.stanford.edu/news/translation-cac-announces-cybersecurity-review-ride-hailing-giant-didi-just-after-its-ipo>.
- Graham Webster & Rogier Creemers** (2020, May 28). A Chinese Scholar Outlines Stakes for New ‘Personal Information’ and ‘Data Security’ Laws (Translation). New America. Retrieved from <http://newamerica.org/cybersecurity-initiative/digichina/blog/chinese-scholar-outlines-stakes-new-personal-information-and-data-security-laws-translation/>.
- Graham Webster, Qiheng Chen and Samm Sacks** (2021, July 9). “Five Important Takeaways From China’s Draft Data Security Law.” New America. Retrieved from <http://newamerica.org/cybersecurity-initiative/digichina/blog/five-important-takeaways-chinas-draft-data-security-law/>.
- H Han Wei** (2021, July 10). Update: Didi Hit With 25 More App Removals as China Ramps Up Sanctions. Retrieved from <https://www.caixinglobal.com/2021-07-10/didi-hit-with-25-more-app-removals-as-china-ramps-up-sanctions-101738427.html>.
- J Jane, Zhang** (2021, January 21). Alipay and WeChat Pay’s Monopoly Status Remains Unclear in New Regulation. South China Morning Post. Retrieved from <https://www.scmp.com/tech/policy/article/3118724/do-fintech-giants-alipay-and-wechat-pay-have-monopoly-power-chinas-new>.
- K Kaifu, Lee** (2018). *AI Superpowers: China, Silicon Valley, And The New World Order*.
- L Lewis, Dev** (2019, September 25). “All Carrots and No Sticks: A Case Study on Social Credit Scores in Xiamen and Fuzhou.” Berkman Klein Harvard University. Retrieved from <https://medium.com/berkman-klein-center/social-credit-case-study-city-citizen-scores-in-xiamen-and-fuzhou-2a65feb2bbb3>.
- Li, lanqing** (2021, July 11). 全国数据交易联盟成立，多方共同推动数据要素市场发展 – 21财经. Retrieved from https://m.21jingji.com/article/20210711/herald/2058822c2b304668919017dbe505ac9c.html?utm_source=pocket_mylist.
- Lingling, Wei** (January 5, 2021). Chinese Regulators Try to Get Jack Ma’s Ant Group to Share Consumer Data – WSJ. Wall Street Journal, January 5, 2021. Retrieved from <https://www.wsj.com/articles/chinese-regulators-try-to-get-jack-mas-ant-group-to-share-consumer-data-11609878816>.

Liu, Lizhi (2021, March). The Rise of Data Politics: Digital China and the World. *Studies in Comparative International Development* 56, no. 1: 45–67. Retrieved from <https://doi.org/10.1007/s12116-021-09319-8>.

M Matthew Walsh, and Flynn Murphy (2021, July 5). Update: After Didi, Two More Freshly Listed Companies Fall Under Security Probe. Retrieved from <https://www.caixinglobal.com/2021-07-05/after-didi-two-more-freshly-listed-companies-fall-under-security-probe-101736013.html>.

O Our New World (2021, June 16). Our New World. Retrieved from <https://www.bondcap.com/report/onw>.

P Peoples Bank of China (2021, December 27). 中国人民银行副行长潘功胜就金融管理部门约谈蚂蚁集团有关情况答记者问. Retrieved from <http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/4153479/index.html>.

People's Government of Guangdong Province (2021, July 11). 广东省人民政府关于印发广东省数据要素市场化配置改革行动方案的通知 广东省人民政府门户网站. Retrieved from http://www.gd.gov.cn/xxts/content/post_3342648.html.

R Reuters, Scott Murdoch and David Stanway (2021, April 10). China Fines Alibaba Record \$2.75 Bln for Anti-Monopoly Violations. Reuters, sec. Retail & Consumer. Retrieved from <https://www.reuters.com/business/retail-consumer/china-regulators-fine-alibaba-275-bln-anti-monopoly-violations-2021-04-10/>.

S Sam Sacks, and Kak, Amba (2021). Shifting Narratives and Emergent Trends in Data-Governance Policy. AI Now Institute. Retrieved from <https://chinaindianetworked.substack.com/p/cin-21-how-to-nationalise-ant-financials>.

Shen, Hong (2019). Platform as Infrastructure and the Rise of Ant Financial in China, 18.

Shoshana Zuboff (2017). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*.

T State Council (2020, April 9). 中共中央 国务院关于构建更加完善的要素市场化配置体制机制的意见_中央有关文件_中国政府网. Retrieved from http://www.gov.cn/zhengce/2020-04/09/content_5500622.htm.

The White House (2021, July 9). "FACT SHEET: Executive Order on Promoting Competition in the American Economy," Retrieved from <https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/09/fact-sheet-executive-order-on-promoting-competition-in-the-american-economy/>.

The White House (2021, June 9). FACT SHEET: Executive Order Protecting Americans' Sensitive Data from Foreign Adversaries. Retrieved from <https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/09/fact-sheet-executive-order-protecting-americans-sensitive-data-from-foreign-adversaries/>.

Translate, China Law (2020, May 8). 关于做好新冠肺炎疫情常态化防控工作的指导意见. *China Law Translate* (blog). China Law Translate. Retrieved from <https://www.chinalawtranslate.com/normalizing-covid-19-prevention-and-control-work/>.

- U UPDATE 1** (2020, November 3). UPDATE 1-China Issues Draft Rules to Regulate Online Micro-Lending Business. *Reuters*, sec. Consumer Financial Services. Retrieved from <https://www.reuters.com/article/china-lending-idUSL1N2HP035>.
- W Wang, Zichen** (2021, December 28). Detailed Breakdown of PBoC Deputy Governor's Q&A on Ant Group – Too Technical to Be Persecution. *Pekingnology*. Retrieved from <https://pekingnology.substack.com/p/detailed-breakdown-of-pboc-deputy>.
- X Xia Xutian 夏旭田 and Jiao yifei 缴翼飞** (2021, July 15). 数据安全上升为多国国家战略: 去年全球数据泄露超过过去15年总和, 中国数据安全市场2023年或近百亿. *Data Law Alliance*. Retrieved from http://mp.weixin.qq.com/s?__biz=MzlyNjUxOTQ0MQ==&mid=2247511577&idx=2&sn=6577245de099ad538baece3901aae843&chksm=e86ddee7df1a57f1453c88a1e92a86bc0a83a0916e61f516a29ef0743accfef4ee5c40947cf#rd.
- Xinhua** (2017, September 6). 广东网信办对腾讯公司违反《网络安全法》有关规定处以最高罚款 腾讯回应: 深入整改-新华网. Retrieved from http://m.xinhuanet.com/gd/2017-09/26/c_1121722779.htm.
- Xinhua** (2021, January 21). 我国非银行支付机构条例要来了! 反垄断监管将强化-新华网. http://www.xinhuanet.com/fortune/2021-01/21/c_1127006357.htm.
- Xinhua** (2021, January 21). China's Market Watchdog Fines 3 Top Firms for Anti-Trust Breach – Xinhua | English.News.Cn. Retrieved from http://www.xinhuanet.com/english/2020-12/14/c_139589198.htm.
- Xinhua** (2021, March 5). China to Strengthen Anti-Monopoly Push, Prevent Disorderly Capital Expansion – Xinhua | English.News.Cn. Retrieved from http://www.xinhuanet.com/english/2021-03/05/c_139784906.htm.
- Xu, Kevin** (2020, November 10). Jack Ma's Bund Finance Summit Speech. *Interconnected*. Retrieved from <https://interconnected.blog/jack-ma-bund-finance-summit-speech/>.
- Y Yang, Stella Yifan Xie and Jing** (2020, August 25). Inside Ant Group's Giant Valuation: One Billion Alipay Users and Big Profit Margins. *Wall Street Journal*, sec. Markets. Retrieved from <https://www.wsj.com/articles/jack-mas-ant-group-files-ipo-listing-documents-11598349802>.
- Yang, Yuan and Nian Liu** (2019, September 19). Alibaba and Tencent Refuse to Hand Loans Data to Beijing. *Financial Times*. Retrieved from <https://www.ft.com/content/93451b98-da12-11e9-8f9b-77216ebe1f17>.
- Yu, Jing Yang and Xie** (2021, June 23). WSJ News Exclusive | Jack Ma's Ant in Talks to Share Data Trove With State Firms. *Wall Street Journal*, sec. Markets. Retrieved from <https://www.wsj.com/articles/jack-mas-ant-in-talks-to-share-data-trove-with-state-firms-11624442902>.

Yuan Ruiyang, Qian Tong and Matthew Walsh (2021, April 10). Update: Alibaba Fined \$2.8 Billion in Landmark China Antitrust Ruling – Caixin Global. Retrieved from <https://www.caixinglobal.com/2021-04-10/alibaba-fined-28-billion-in-landmark-china-antitrust-ruling-101688439.html>.

Yu, Sun and Tom Mitchell (2021, April 23). China's Central Bank Fights Jack Ma's Ant Group over Control of Data. *Financial Times*. Retrieved from <https://www.ft.com/content/1dbc6256-c8cd-48c1-9a0f-bb83a578a42e>.

Z Zhai, Lingling Wei and Keith (2021, July 5). WSJ News Exclusive | Chinese Regulators Suggested Didi Delay Its U.S. IPO. *Wall Street Journal*, sec. Business. Retrieved from <https://www.wsj.com/articles/chinese-regulators-suggested-didi-delay-its-u-s-ipo-11625510600>.

Zhao Yanqing (2021, March). 如何让蚂蚁的大数据国有化?. *China Credit*. Retrieved from http://chinacreditinfo.com/news_view_3_389.aspx.

孙朝 尤一炜 樊文扬 (2021, June 30). 首设核心数据管理制度, 最高罚一千万! 数据安全法焦点解读. 隐私护卫队. Retrieved from http://mp.weixin.qq.com/s?__biz=MjM5NDYNTQyMQ==&mid=2649168939&idx=1&sn=-4c3510a34fb70dcb5c01a507e48cb0f&chksm=be9da68989ea2f9fc563bad360fe13158e5a67c6dd758d8c0fdc50e74baa2255198864dff7ff#rd.

尤一炜 (2020, June 6). 明确重要数据分类是当务之急 专家: 拟出台重要数据识别指南国标_左晓栋. 南都个人信息保护研究中心. Retrieved from www.sohu.com/a/399418454_161795.

史宇航 (2021, July 10). 解读: 数据安全法的机构合规义务. 互联网安全内参. Retrieved from http://mp.weixin.qq.com/s?__biz=MzI4NDY2MDMwMw==&mid=2247497963&idx=1&sn=60c53e0a523f5ec8e8b51b965dbfacf8&chksm=ebfabfcbdc8d36dd0d79b6b54eb73bc58f3883cefa86f7707a004c6c75b7e137d0893a97c30b#rd.

国信办 (2021, July 9). 【资讯】国信办通报Keep等129款App违法违规收集使用个人信息情况. Weixin Official Accounts Platform. Retrieved from http://mp.weixin.qq.com/s?__biz=MzU1NDY3NDgwMQ==&mid=2247503340&idx=2&sn=017cde7009684a936c3d55b17df11391&chksm=fbdd72f2ccaafbe4d6af38925e013b7f4a974b78099e10a1e9fc15228537dff676189f37ab7e#rd.

臧俊恒杨东 (2021, July 9). 霸气滋戾气: 超级平台扼杀了什么. *Half monthly discussion*. Retrieved from http://www.banyuetan.org/jrt/detail/20210709/1000200033134991625563363051490786_1.html.

Sample of Questions

Semi-structured interviews were conducted with questions broadly aligned with three themes:

1. How the regulation of data affects innovative capacities
2. Data cultures, or perceptions around data and innovation
3. How data creates value or values

A sample of questions for each theme follows:

Regulation	<ul style="list-style-type: none"> • To what extent do you think the laws and regulations around data protection have been helping or hindering the innovation capabilities of firms and organisations? • Do you see the legal landscape, as in the laws and regulations in specific, or the legal framework, changing in the next few years? • How can the current laws and regulations, including the legal framework, be improved so that the innovation capabilities of organisations can be further enhanced?
Data cultures	<ul style="list-style-type: none"> • How is personal data seen in China? For example, do people see it as something that they need to protect? Or as byproducts of economic transactions? • How might perceptions of personal data and privacy have an impact on innovation? For example, what types of data would be considered taboo to share, and in what contexts?
Data and value creation	<ul style="list-style-type: none"> • What do you think is the value that organisations bring when they are successful in managing their data, including analysing, storing, protecting, and sharing their data? • How do you think frameworks like the GDPR affect domestic and trans-border operations, and to what extent do you think a similar framework would be feasible in China?

Methodology

This project adopted a case study approach, with data collected from semi-structured expert interviews and published documents. Various interviews were conducted with various experts, ranging from academics, lawyers and representatives from internet companies. A content analysis on selected documents such as press releases and public consultation papers was also conducted, where the documents were coded according to themes such as value associated with data, principles of data governance and partnerships in data sharing.

Dev Lewis is a Fellow and Program Lead at Digital Asia Hub, an independent, non-profit Internet and society research think tank. He is also a Global Governance Futures 2035 Fellow. Dev holds a bachelor's degree in international relations from Roger Williams University in the US and a Master's in China Studies from Yenching Academy at Peking University. His interests lie at the intersection of technology, politics, and policy, especially in Asia. Dev's work revolves around building cross-national exchange in people and ideas, which he does through research and writing, lectures, creating workshops and conferences, and translating for think tanks, investment firms and tech companies in India and China. His work has been featured on Sup China, Harvard Berkman Klein Centre, Nesta, Sixtstone, Quartz, and Konrad-Adenauer-Stiftung.

Editors

Christian Echle
Director Regional Programme Political Dialogue Asia
christian.echle@kas.de

Ming Yin Ho
Programme Manager for Digital Transformation
mingyin.ho@kas.de

Konrad-Adenauer-Stiftung e. V.
Regional Programme Political Dialogue Asia
Arc 380
380 Jalan Besar, #11-01
Singapore 209000
www.kas.de/singapore


Imprint

Published by:
Konrad Adenauer Stiftung Regional Programme
Political Dialogue Asia, Singapore, 2021

Design and typesetting: yellow too Pasiok Horntrich GbR
Pattern: iStock by Getty Images/Nadiinko

Printed with financial support from the German Federal Government.

ISBN 978-981-18-4822-3



Data fuels digital change. The ability to collect, process, and make available ever-increasing amounts of data is a key to innovation and growth.

This report is one of the series surveying seven different Asian territories to deepen understandings of innovation and data policies, and contribute to debates about data governance and data protection. The study was carried out in collaboration with the National University of Singapore (NUS). We selected Hong Kong SAR, India, Japan, the People's Republic of China, Singapore, South Korea, and Taiwan as the contexts to be examined. We looked at the areas of transport, finance, administration, health and smart cities to understand how innovation is driven in the context of relationships among key stakeholders such as citizens, civil societies, government agencies, private sectors and research institutions.

This report analyses China's emerging data culture, especially China's strategy to uphold data sovereignty and national security by tightening control over domestic and cross-border data flow through evolving legal regimes. Through the case studies of Ant Group and Didi Chuxin, we seek to understand the dynamics that shaped the innovation and data policies in China.