China Data Sovereignty

Edward McNicholas
Partner
Ropes & Gray

David R. Chen
Counsel
Ropes & Gray

Mingli Shi
Privacy Attorney
Qualcomm

ROPES & GRAY

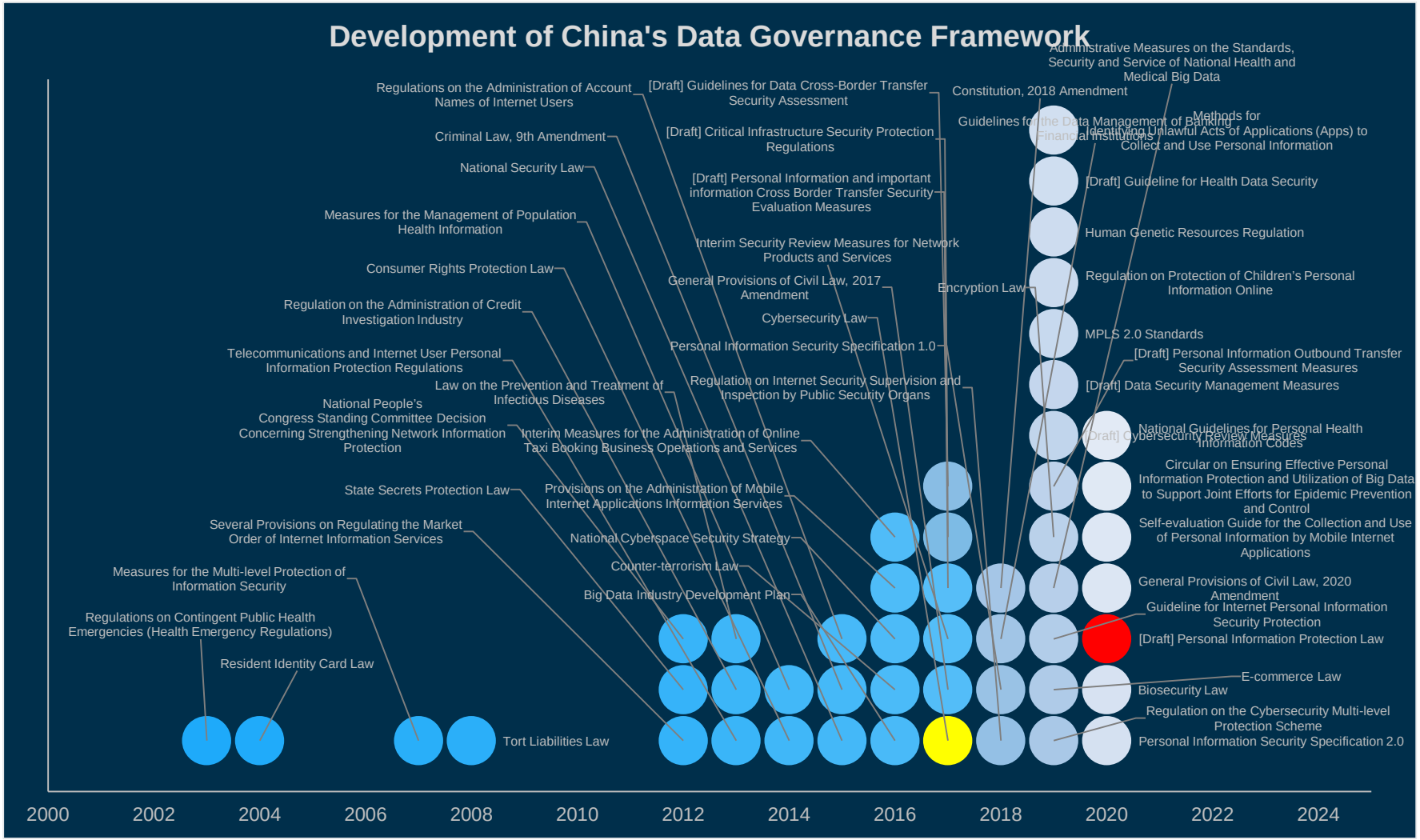
October 1, 2021

China Privacy Legal Regime

- Constitution
- Civil Code
- Criminal Law
- Cybersecurity Law
- Data Security Law
- Critical Information Infrastructure Security Protection Regulations
- **Personal Information Protection Law (PIPL)**
- Regulation on Protection of Children's Online Personal Information

- Sectoral regulations and local regulations
  - Credit reporting, financial, health, vehicle, platform governance, e-commerce, …
  - Data Regulations of Shenzhen Special Economic Zone, …
- Implementation rules
  - Measures for Cybersecurity Review, …
- "Soft" Law – national standards, policy guidelines, …
- …

China's Cyber Legal Regime is Complex



Recent China data protection updates

Regulation	Latest Update
China Data Security Law	• Adopted June 10, 2021; will become effective September 1, 2021 • Expands China's export control regime to cover the export of data • Regulates data processing activities (i) in China and (ii) outside of China, if the activities could jeopardize national security, the public interest or the legitimate rights and interests of citizens or organizations in China • Government has greater authority to compel private sector firms to disclose data • Prohibits transfer of "important data" overseas by critical information infrastructure operators (CIIOs) without passing a security assessment by Chinese regulators, and by non-CIIOs without first complying with rules to be formulated by the Cyberspace Administration of China (CAC) • Non-CIIOs are subject to regulation of processing of important data; also required to conduct risk assessments (and to report findings to the government)

Recent China data protection updates

Regulation	Latest Update
China Personal Information Protection Law	• Adopted August 8, 2021; will become effective November 1, 2021 • Regulates the processing and transferring of personal information within China and outside of China in certain circumstances (e.g., for the purpose of providing products or services to persons inside China or analyzing or evaluating the behavior of persons inside China) • Allows China to prohibit transfers of personal information in response to sanctions imposed by other countries or activities that harm the rights/interests of Chinese citizens or endanger national security/public interest • Requires overseas personal information processors to have an office or designated representative in China to be responsible • Imposes data protection requirements on data processors • New obligations on large online platform service providers with large number of users and complex business models, including establishment of independent data oversight body • For overseas transfers of personal information, requires either a security assessment or certification from the Cyberspace Administration of China ("CAC") agreement with a transferee based on a standard contract stipulated by the CAC • Significant penalties

PIPL v. GDPR

Is China converging with or diverging from GDPR (and global privacy trend)?

- Legislative Context and Intent
- Applicable Scope
- Compliance Obligations for Businesses
- Data Subject Rights
- Cross-Border Data Transfer
- Enforcement Mechanism
- …

Recent China data protection updates

Regulation	Latest Update
Draft Amendment Cybersecurity Review Measures	• Current Cybersecurity Review Measures were implemented on June 1, 2020, and require CIIOs to conduct national security assessments and undergo cybersecurity review when procuring network products and services which may present a national security concern. • Proposed amendments announced in July 2021 that would require CIIOs and non-CIIO data processors with the personal information of over 1 million users to undergo a cybersecurity review before listing abroad • Expands cybersecurity review scope to include the risk of core data, important data, or a large amount of personal information being stolen, leaked, destroyed, illegally used, or transferred outside of China or being affected, controlled, or maliciously used by foreign governments after a foreign listing.

Data Sovereignty

- Data Sovereignty: data should be subject to the laws and regulations of the state in which it is generated and processed
- Closely linked to Internet sovereignty: respect of the right for nation-states to determine the rules for the development and regulation of their cyberspace.
- Data sovereignty is manifested in China's data governance regime most prominently in the form of:
  - data localization/cross-border data transfer restrictions
  - security review or government approval requirements for cross-border data transfers or sharing of data with foreign parties

Cybersecurity and informatization are mutually complementary. Security is the precondition of development, development is the guarantee for security, security and development must progress in step.

This year is the year in which the "13th Five-Year Plan" starts, cybersecurity and informatization work is the most important element in the "13th Five-Year Plan" period.

-- Xi Jinping, April 19, 2016. Speech at National Cybersecurity and Informatization Work Conference.

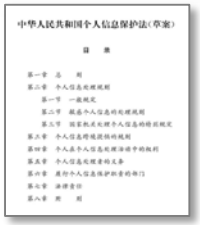
Legal Framework for Data Localization and Cross-Border Data Protection

Laws

5/5/2014
Population Health Information Management Measures

6/1/2017
Cybersecurity Law

7/12/2018
Administrative Measures for National Health and Medical Big Data Standards, Security, and Services



10/21/2020
Draft Personal Information Protection Law (first draft)

4/15/2021
Biosecurity Law

9/1/2021
Data Security Law

2014-2017 | 2018 | 2019 | 2020 | 2021

4/11/2017
Draft *Measures on Security Assessment of the Cross-Border Transfer of Personal Information and Important Data* published for comments

5/28/2019
Draft *Measures for Data Security Management* published for comments

6/13/2019
Draft *Measures on Security Assessment of the Cross-Border Transfer of Personal Information* published for comments

7/1/2019
Regulation on the Administration of Human Genetic Resources

7/10/2021
Draft *of Revision to Measures on Network Security Assessment* published for comments

11/1/2021
Personal Information Protection Law

Rules / Regulations

The list is ongoing…

ROPES & GRAY

Data Localization and Cross-Border Data Transfer Requirements (1)

Cybersecurity Law

Art. 37: The operator of a criminal information infrastructure shall store within the territory of the PRC personal information and important data collected and generated during its operation within the territory of the PRC. **Where such information and data have to be provided abroad for business purposes, security assessment shall be conducted** pursuant to the measures developed by the Cyberspace administration of China together with competent departments of the State Council…

Data Security Law

Art. 31: The Cybersecurity Law shall apply to the cross-border transfer of important data by critical information infrastructure operators collected and produced during their operations within mainland China, and the administrative measures formulated by cyberspace regulators shall apply to **the cross-border transfer by other data processors of important data collected and produced during their operations within mainland China**.

Data Localization and Cross-Border Data Transfer Requirements (2)

Personal Information Protection Law

Chapter III is dedicated to regulate cross-border provision of personal information.


中华人民共和国个人信息保护法

Art. 38 requires at least one of the following conditions be met before the provision: (1) passing a security assessment; (2) undergoing personal information protection certification; (3) concluding an agreement with a foreign receiving party according to a template contract designed by the cyberspace authority; and (4) other conditions provided by laws/regulations.

Art. 39 requires "personal information processors" to notify the individuals about the foreign receiving side's identity, etc. and obtain individuals' separate consent.

Art. 40 requires the passing of a security assessment organized by the state cybersecurity authority for critical information infrastructure operators and data processors handling personal information reaching certain quantities.

Data Localization and Cross-Border Data Transfer Requirements (3)

Biosecurity Law

Art. 53: the state enjoys sovereignty over our country's human genetic resources and biological resources.

Art. 56: requires approval prior to use China human genetic resources to carry out international research collaborations, and transporting, mailing, or carrying China's human genetic resources out of mainland China, **except for international clinical collaborations that do not involve the provision of China human genetic resources out of mainland China conducted for the purpose of obtaining marketing authorization for drugs and medical devices**.

Foreign organizations and individuals, as well as institutions they establish or are actual controllers of, must not collect or preserve human genetic resources within mainland China, and must not provide China human genetic resources outside mainland China.

Regulation on the Administration of Human Genetic Resources

Art. 7: prohibits foreign parties and their controlled entities from collecting or storing China human genetic resources in mainland China, or providing them outside of mainland China.

Art. 21 and 22: allows foreign parties and their controlled entities to use China human genetic resources in scientific research and clinical trials, but only under international research collaborations with Chinese parties, but requires pre-approval or pre-notification (in the case of clinical trials)

Art. 28: security assessment is required if provision of China human genetic resources to foreign parties and their controlled entities may damage public health, national security, or social interests. China human genetic resources provided to foreing parties and their controlled entities must be provided for record filing

Cross-Border Data Transfer Restrictions (5)

5/28/2019
Draft Measures for Data Security Management

Network operators need to assess security risks and obtain competent authorities' approval before providing important data* overseas.

(Art. 28)

*"Important data" is defined as data, once leaked, may directly impact national security, economic security, social stability, public health and safety, such as unpublished government information, large-population based data, gene/health, geography, and mineral resource data. **"Important data" typically does not include business operation and internal management data and personal information.** (Art. 38(5))

6/13/2019
Draft Measures on Security Assessment of the Cross-Border Transfer of Personal Information

Network operators need to report security assessment on cross-border transfer of personal information to the provincial cyberspace administration authority and provide relevant materials.

(Arts. 3 & 4)

7/10/2021
Draft Measures on Network Security Assessment

Applies to critical information infrastructure operators.

(Art. 2)

Operator possessing more than 1 million users' personal information need to report to the cyberspace authority for network security review before going public in foreign jurisdictions.

(Art. 6)

Key Takeaways

Multi-Ministry Approval-Based Regime

- Relevant laws and regulations create an approval-based regime governing cross-border data transfer that involve multiple ministries and administrations, with the coordination of the Cyberspace Administration of China.

中共中央网络安全和信息化委员会办公室
Office of the Central Cyberspace Affairs Commission

中华人民共和国科学技术部
Ministry of Science and Technology of the People's Republic of China

中华人民共和国国家互联网信息办公室
Cyberspace Administration of China

中华人民共和国国家卫生健康委员会
National Health Commission of the People's Republic of China

Increasingly Broad Coverage

- Data transfer restrictions apply from "critical information infrastructure" operators to "personal information processors."

Key Takeaways

Key Questions

- What constitutes “critical information infrastructure”?
- What constitutes “important data”?
- What constitutes human genetic resources data?
- How do the laws/regulations address employee data/business information/financial information generated in the ordinary course of business in China but stored on MNC’s foreign servers?

Prohibition on Sharing Data with Foreign Judicial or Law Enforcement Agencies

Data Security Law, Art. 36

- The competent authorities of the People's Republic of China shall, in accordance with the relevant laws and international treaties and agreements concluded or acceded by the People's Republic of China or under principles of equality and mutual benefit, handle the requests made by foreign judicial or law enforcement authorities for the provision of data.
- Without the approval of competent authorities of the People's Republic of China, no organization or individual within the territory of the People's Republic of China may provide foreign judicial or law enforcement authorities with data stored within the territory of the People's Republic of China.

Personal Information Protection Law, Art. 41

- The competent authorities of the People's Republic of China shall, in accordance with the relevant laws and international treaties and agreements concluded or acceded by the People's Republic of China or under principles of equality and mutual benefit, handle the requests made by foreign judicial or law enforcement authorities for the provision of personal information stored within the territory of the People's Republic of China.
- Without the approval of competent authorities of the People's Republic of China, no personal information processor may provide foreign judicial or law enforcement authorities with personal information stored within the territory of the People's Republic of China.

Key Points

Key Takeaways

- A request by a foreign judicial or law enforcement authorities for data stored in China must be made to the relevant Chinese authorities. Measures detailing to whom requests should be made and how Chinese authorities will process such requests are expected to be issued.
- Prohibition applies to data (including personal information) stored in China.
- Prohibition applies to organizations and individuals located in China, and potentially personal information processors located outside of China that are subject to the PIPL.
  - Chinese affiliates of foreign organizations cannot directly provide data stored in China to foreign judicial or law enforcement authorities
  - Foreign entities that store data in China cannot directly provide such data to foreign judicial or law enforcement authorities
- China-sourced data that is exported or stored outside of China is not subject to the prohibition, but must have been exported or stored outside of China in compliance with China data localization and cross-border transfer requirements.