Trends & Developments in China's Data Regulatory Regime

Prepared by Samm Sacks for the Canada China Business Council

April 2022

KEY TAKE-AWAYS

- **China's cybersecurity and digital legal and regulatory regime is best understood as an evolving matrix of interlocking parts**, each subject to competing pulls between security and economic development goals, as well as reflecting a web of politics among different government and quasi-government stakeholders.
- Many pieces of this matrix are still evolving, shaped by **internal domestic debates as well as responses to external geopolitics.**
- The main domestic regulatory risks for multinational companies (MNCs) include: **politicized 'blackbox' cybersecurity reviews, blacklisting from handling Chinese personal information (PI), prohibitions on sharing Chinese data with U.S. law enforcement, expanded Chinese government access to data via on-site inspections, on-site security inspections and even raids of facilities, revocation of business and licenses, and intimidation of local staff over content censorship & information access.**
- **MNCs are also at risk of getting caught in the cross-fire of U.S.-China data conflict** as Washington and Beijing increase pressure to localize data and ramp up security assessments focused on cross-border data transfers.

I. CHINA'S DATA REGULATORY REGIME

The State Council designated data as a "factor of production" in 2021—a high-level signal of the Xi administration's intent to data as a critical economic resource on the level of land, labour, and capital.

A spate of laws, regulations, and policies together create a framework that the leadership aims to use as the basis for unlocking the economic value of data, while simultaneously keeping it secure as a national security asset. These twin economic and national security objectives create internal friction, often pulling in different directions, and complicating the business operating environment for companies holding high volumes of data (as discussed in part two below).

Overall, the leadership's vision is for China to engage in secure global digital trade. The goal is to allow less sensitive data to circulate for economic growth, while locking down data deemed most sensitive to national security. This marks an incredibly ambitious vision that will consume the government for years to come. The vision is not to shut off China from the outside world but to create better security within that connection.

The most significant parts of this evolving legal and regulatory framework for data include:

- **Cybersecurity Law (2017)**
  - o The centrepiece of a governance system for "personal information" and "important data" (fleshed out in subsequent developments)
- **Data Security Law (2021)**
  - o Calls for creating a national-level data classification system to organize data by type and level of risk
    - > Establishes additional obligations for categories of data identified as core to national security
  - o Creates a blocking mechanism to prevent access by foreign law enforcement authorities
  - o Fleshes out data security assessment process required for outbound data transfers
- **Personal Information Protection Law (2021)**
  - o Establishes a blacklist whereby companies can be banned from handling Chinese PI if the country of origin is found to be discriminating against China (i.e., a political tool of retaliation)
  - o Creates compliance obligations similar to the European Union's GDPR (e.g., notice and consent, duties for data handlers, minimization, etc.)
- **Data classification guideline (draft)**
  - o Follows Data Security Law with a system for sorting data by level of importance: national core, important, sensitive, internal, and public data and sensitivity
- **Multi-level Protection Scheme (2007; now in the process of being updated)**
  - o New version covers all "network operators" in contrast to previous version focused on state-owned enterprises (SOEs) and government information systems only

- o Companies “negotiate” during MLPS audit process to comply with various security obligations based on the level of risk assessed on a scale of 1-5; systems deemed level three and above potentially subject to difficult obligations including domestic encryption and real-time data access.
- o The MLPS regime overlaps with the critical information infrastructure (CII) regime outlined by the Cybersecurity Law, leading to turf wars and redundancy involving the Ministry of Public Security and Cyberspace Administration of China.

II. BUSINESS IMPACT & UNRESOLVED QUESTIONS

Data governance has become one of the most significant regulatory risks facing all companies operating in China. This risk extends beyond traditional “tech” companies to all sectors with information systems and handling large amounts of Chinese personal and non-personal data, including retail and consumer, manufacturing, healthcare, finance, etc.

The new authorities under the data regime also could be used as tools against U.S. companies and investors as part of geopolitical conflict. The overly broad nature of the requirements would allow these tools to be used in a politicized way should U.S.-China relations deteriorate further, with Canadian firms potentially caught in the cross-fire.

To be sure, China’s data regulatory regime create tremendous uncertainty in the business environment in China, but it still is an open question what these requirements will mean in practice given significant debate inside the government and with domestic industry about the meaning of data ownership and competing pulls of economic and security objectives.

- The most far-reaching data localization requirements as written (especially the stringent Data Security Management Regulation) may or may not be enforced. That regulation will take a year or more to be completed before State Council approval, while the rules that the CAC can issue by itself are still in draft and mainly just establish processes and procedures.
- Despite the immense power of the CAC, there is an intense “negotiation” underway between the security ministries and those who want China to remain “open and embedded in the outside world” which is part of the “vision” of the Chinese leadership. They both need to be accountable to President Xi.
- The decentralized system for identifying important data and CII means that there will be overclassification. The default will be to define most kinds of data as important for national security because if there is a breach or incident, no official will want to be held responsible for under-weighting the sensitivity of the data. In the near-term, we will likely see overclassification of important data, and maybe the government will see it has overreached and walk things back, but that could take a long time and in the interim, be incredibly disruptive for global operations.