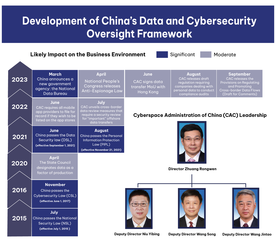
Commentary

THE ASIA GROUP

Key Trends in China's Data Policies



Key Takeaways

- Information and communications technology policy in China is now predominantly shaped by national security issues. Beijing has constructed a set of laws and rules that strictly control internet data and determine how companies and other organizations may use, manage, and transfer data domestically and overseas.
- The result is a vague patchwork of rules, definitions, and requirements that have become a major headache for both Chinese and foreign businesses, especially those that operate globally.
- The top goal for the Beijing government is to fully control the information space, to ensure ideological conformity and strengthen social stability.
- The Cyberspace Administration of China (CAC) has been, and will continue to be, central to the development, execution, and enforcement of Beijing's policies, even as other parts of the government attempt to tamp down some of the most onerous provisions of China's strict approach.
- The future direction of policy may be shaped by whether or not China's topmost officials identify tight data rules as a contributor to China's sluggish economic performance.

Cyberspace Administration of China (CAC) Overview

The CAC, which was founded in 2011 as the country's internet regulator and enforcer, is not a typical administrative agency in the executive branch of the government. Instead, the CAC is a party-state entity, closely intertwined with the Chinese Communist Party (CCP), and thus holds more power than most ministries under the leadership of Premier Li Qiang and the State Council. This arrangement adds to the challenges posed to companies, both domestic and foreign, operating in China.

Beijing in recent years has further expanded the CAC's role to include policy formulation and enforcement of cybersecurity, data security, privacy regulations, and network platforms. These authorities are based on the 2015 National Security Law, the Cybersecurity Law (CSL), Data Security Law (DSL), and the Personal Information Protection Law (PIPL). The CAC collects data and information that enable it to monitor and control China's online ecosystem through security assessments of cross-border data flows, algorithm registrations, and filing requirements.

The CAC's Expansive Powers

When the CAC identifies organizations that are non-compliant with China's framework of laws governing cybersecurity, the agency can enforce substantial punitive measures – and potentially expel companies from China.

In some cases, the CAC has been able to challenge and overrule other ministries' recommendations and decisions. The CAC attracted international attention in 2021 when the agency launched its first-ever cybersecurity review against China-based ride-hailing company DiDi Global. The CAC halted DiDi's overseas initial public offering, temporarily suspended new user registrations, ordered China's app stores to remove DiDi. It eventually fined DiDi USD 1.2 billion for unspecified violations of laws. This all came after Didi had obtained all necessary approvals from other ministry-level agencies in China, including the securities regulator.

More recently, in April 2023, the CAC initiated a review of products sold in China by the U.S. semiconductor firm Micron. In May, the CAC announced that Micron products failed a cybersecurity assessment and subsequently banned operators of China's critical infrastructure from purchasing Micron products.

The CAC gives President Xi Jinping a key tool for expanding ideological control domestically – and serves as a model of tight internet governance for other countries, especially those in the developing world in Africa and the Pacific Islands under authoritarian rule. The CAC has partnered with China's main intelligence agency, the Ministry of State Security, and state media organizations, such as Xinhua and CGTN, on international surveillance and propaganda as part of Xi's ambition to "tell the China story better."

What to Watch Next

The CAC will likely soon finalize its draft Regulations on Network Data Security Management Regulations, initially **released** in 2021. The regulations cover a wide range of topics: (1) identifying which companies need to perform cybersecurity reviews; (2) establishing personal information and "important data" protections; (3) updating data breach notification and cross-border transfer requirements; and (4) restricting virtual private networks (VPNs) used to bypass China's "Great Firewall." The regulations also aim to establish a data classification and hierarchical protection system based on the data's impact on national security and public interest, or the rights and interests of individuals and organizations.

Persons or entities that process data inside China will need to comply with the finalized regulations. The regulations are likely to also cover certain entites conducting activites overseas that process the data of China-based individuals or organizations – such as data processing for the purpose of providing products or services to the China market and analyzing the behavior of individuals and organizations in China.

TAG Take

The Didi and Micron investigations reflected the CAC's increased power and demonstrate three of the government's and CCP's top priorities: (1) limiting private firms' collection of personal information, especially data that poses a challenge to the CCP and the state's control of such data; (2) addressing "national security" concerns in line with Beijing's response to U.S. and others' technology denial efforts, and (3) helping the CCP further tighten censorship to support Beijing's need to ensure social stability – a key concern amid increasing economic challenges both at home and abroad.

For some of China's most senior policymakers, security concerns have outweighed economic growth priorities – suggesting that CAC regulations and enforcement activities will continue posing challenges for firms, both foreign and domestic, operating in China's digital space. Whenever China's top state and CCP officials feel more insecure about "foreign forces" or their own ability to maintain domestic stability, the CAC may be more willing to take aggressive action.

At the same time, the CAC's broad but sometimes vague scope of jurisdiction allows the agency considerable flexibility on when and how to take oversight action, in line with top policymakers' perception of security. As China's economy faces continued headwinds, President Xi and other senior policymakers may decide to adjust cybersecurity policies, at least marginally, if they fear too much capital flight.

The CAC – as a mostly domestically-focused regulator – lacks deep experience engaging with multinationals and foreign counterparts, but it is showing signs that it may become more open to engagement with foreign companies. The CAC's controversial and hastily introduced 2022 cross-border data security assessment requirements illustrated the agency's struggle to simultaneously ensure data security and a stable, attractive business environment. Facing complaints from multinationals about the cross-border data flow requirements, the CAC began soliciting comments on the provisions in September 2023, and may in the end waive security assessments for data export for certain activities and circumstances – suggesting that some officials want to better balance data security concerns with economic concerns.

*This report was prepared by **Nicola Ying Fry**, **Jie Ma**, **David Hathaway**, **Claire Chao**, and **George Chen**, **Jason Trinh** prepared the graphic.*

THE ASIA GROUP

Washington DC • New Delhi • Hanoi • Shanghai • Tokyo

2000 Pennsylvania Avenue NW, Suite 1000, Washington DC, 20006

THEASIAGROUP.COM