USALI Perspectives

The Didi Case and the Party's Influence over Data Enforcement

Super-regulator CAC sets a chilling precedent

By Angela Huyue Zhang
Published September 20, 2022

In July 2022, the Cyberspace Administration of China (CAC) completed its probe into Didi Chuxing and imposed a USD 1.2 billion fine on the country's leading ride-hailing giant. The case had been launched a year earlier, when the CAC conducted a surprise cybersecurity inspection of Didi just two days after the firm's initial public offering in New York.

The agency's announcement that it was investigating Didi caught many by surprise because the cybersecurity review mechanism was not designed for regulating overseas listings. Instead, it was created to cope with the procurement risks of network products and services by operators of critical information infrastructure.

As it turned out, the CAC's sudden investigation appears to be retaliation for Didi's failure to follow its advice to conduct a thorough cybersecurity check before listing in New York. As a consequence of the CAC's high-profile announcement, investors panicked, generating a massive sell-off of Didi's stock. During the CAC's year-long investigation, Didi lost almost 80% of

its valuation and was forced to delist from the New York Stock Exchange.

To some investors, the record-high fine imposed by the CAC may have come as a relief, as it finally settled the dust for the severely battered tech firm. But the CAC's final penalty decision, which was revealed in a short public announcement, is troubling in many ways. Even though both the Data Security Law and the Cybersecurity Law were mentioned as legal bases for the punishment, the announcement's emphasis was on Didi's excessive data collection practices and privacy infringement.

Indeed, the mega-fine seems to have been mostly levied on the basis of the Personal Information Protection Law (PIPL), which enables Chinese regulators to impose fines of up to five percent of a firm's revenue in the previous year. The PIPL only took effect on Nov. 1, 2021. It thus appears that the CAC leveraged the new data privacy law to punish Didi for cybersecurity violations. Even more concerning is that the agency seems to have retroactively punished the company for conduct going back seven years, long before the PIPL was adopted.

The CAC's moves seem to have violated the basic legal principle of non-retroactivity as well as the requirements of China's Administrative Procedure Law and Administrative Punishment Law. The Didi precedent also quickly established the authority of the CAC as a tough data regulator and set a chilling precedent for all Chinese tech firms.

As I elaborate in my book, *Chinese Antitrust Exceptionalism: How the Rise of China Challenges Global Regulation*, institutional factors such as bureaucratic mission and the culture and structure of an administrative authority play important roles in influencing law enforcement outcomes in China. To understand the outcome in the Didi case, it is essential to examine the CAC, the key administrative authority behind the decision.

The CAC is no ordinary administrative agency. Its predecessor was the State Internet Information Office (SIIO) which was part of the Chinese Communist Party (CCP) Propaganda Department. In 2013, the SIIO was reorganized and renamed in order to streamline information control over China's digital space. Formally, the CAC is also the general office of the Central Cyberspace Affairs Commission, a CCP task force chaired by President Xi Jinping.

The historical origin of the CAC, its dual roles as a CCP organ and administrative agency, and its direct links with the top Chinese leadership afford this agency a very unusual bureaucratic status. Furthermore, unlike most other Chinese

administrative regulators, the composition and operation of the CAC are largely shrouded in secrecy.

As Jamie P. Horsley acutely observes, the CAC "lacks many formal attributes of an administrative agency in the Chinese system, including institutional transparency and accountability. While the general principle that merged party-state entities should be treated as administrative agencies when performing state rather than party functions is gaining traction, the line between those two functions is not always clear."

Given that data is the lifeblood of the platform economy, the CAC has significant scope to expand its bureaucratic bailiwick. In the past two years, this ambitious agency has extended its tentacles from cybersecurity and content control to the regulation of securities offerings, price discrimination, algorithmic recommendations, and many other areas. The Didi case may only be the first of many as this super-regulator deploys its mighty arsenal.

To be sure, the Chinese government has perfectly legitimate reasons to enhance personal information protection for its citizens, given rampant data fraud and personal information leaks. But it is equally important to install sufficient institutional safeguards to ensure due process in administrative enforcement. As the Didi case shows, unchecked regulatory power and arbitrary enforcement will only spook international investors and deter foreign investment. This certainly will not bode well in the years to come for China's dynamic platform businesses and tech innovations.

Angela Huyue Zhang is the director of the Philip K. H. Wong Centre for Chinese Law and associate professor of law at the University of Hong Kong. She is the author of Chinese Antitrust Exceptionalism: How the Rise of China Challenges Global Regulation*, published by Oxford University Press.*

Suggested citation:

Angela Huyue Zhang, "The Didi Case and the Party's Influence over Data Enforcement," *USALI Perspectives*, 3, No. 2, September 20, 2022, https://usali.org/usali-perspectives-blog/the-didi-case-and-the-partys-influence-over-data-enforcement.