Analysis of the Implications of the CCP's New Regulations to Strengthen Network and Data Management

Chia-ling Hung
Assistant Research Fellow

Min-chen Tseng
Research Assistant

Division of Cyber Security and Decision-Making Simulation

1. News Highlights

The Cyberspace Administration of China (CAC), together with 12 other departments, jointly revised and released the "Regulations on Network Security Review" ("Security Regulations") with 23 articles,[1] which take effect February 15, 2022. The Security Regulations include situations where the processing of data by network platform operators affects or may affect national security in the scope of review. The CAC, together with the Ministry of Industry and Information Technology (MIIT), the Ministry of Public Security, and the State Administration of Market Supervision, also jointly issued the "Regulations on the Recommendation of Algorithms for Internet Information Services" ("Algorithm Regulations") with 35 articles, which take effect March 1, 2022. It focuses on requiring technology enterprises to comply with business ethics and principles of fairness when implementing "algorithms," such as not using algorithms to create fake user accounts or create other false impressions,

1. The 12 departments include National Development and Reform Commission, Ministry of Industry and Information Technology, Ministry of Public Security, Ministry of State Security, Ministry of Finance, Ministry of Commerce, People's Bank of China, State Administration of Market Supervision, State Administration of Radio and Television, China Securities Regulatory Commission, State Secrets Bureau, and State Cryptography Administration. "State Internet Information Office and Other 13 Departments Revised and Issued 'Regulations on Network Security Review'," *Cyberspace Administration of China*, January 4, 2022, https://www.12377.cn/wxxx/2022/295c592b_web.html.

and all information must be filed with the CCP authorities within 10 working days.[2]

2. Security Implications

2-1. Strict review of listing overseas of online platforms

The CAC originally published the "Measures for Security Review of Internet Products and Services (for trial implementation)" in May 2017 and published the "Security Regulations (draft for comments)" in 2019, and formally promulgated the regulations in April 2020,[3] focusing on the "Critical Information Infrastructure" (CII) with a relatively simple scope. Only 15 months later, the Security Regulations were amended again to meet the implementation of the "Data Security Law" on September 1, 2021. The new version of the Security Regulations added "Internet platform operators" and "critical information infrastructure operators" as two key targets for scrutiny, and listed three "shall" and one "must" (as shown in the attached table) to emphasize that "overseas listing of platforms with user data of millions is subject to 'cybersecurity examination'". The "examination" focuses on the risk of critical core data or massive personal information being influenced, controlled, or maliciously manipulated by foreign governments before and after the enterprise goes public abroad, which could "affect or may affect national security". Since the new Security Regulations do not specify which industries and the scope of scrutiny, they would apply to almost all large Internet and technology-related enterprises in China; and it will take longer than before to determine whether national security is affected in terms of regulations and business perspective, causing a lot of anxiety for online platform enterprises that wish to go public abroad.

2-2. Controlling online opinions through strict scrutiny of algorithm business model

As the world economy becomes

2. Regulations on the Recommendation of Algorithms for Internet Information Services," *People.com*, January 4, 2022, http://politics.people.com.cn/BIG5/n1/2022/0104/c1001-32323657.html.
3. Regulations on Network Security Review Require Online Platforms with Over a Million Users Must File for Security Review Before IPO Abroad," *China Times*, January 4, 2022. https://www.chinatimes.com/realtimenews/20220104001732-260409?chdtv.

"Internet platform-centric", the CCP is aware of the common problems of Internet platforms using algorithms to censor information, make excessive recommendations, manipulate search results and rankings, and forged "likes" as well as "shares" that seriously affect online opinions. In order to keep the chaos under control, the CCP promulgated the Algorithm Regulations that monitor a wide range of technology companies that provide algorithm recommendation services, such as food delivery, taxi hailing, and e-commerce, and prohibit these platforms from evading supervisory and management responsibilities by claiming "technology neutrality".[4] In addition, online platforms are required to inform users of the status of their recommendation services in a conspicuous manner, and to file the platforms with "public opinion attributes" or "social mobilization capabilities" in the hope to solve the long-term data transparency and misuse problems through this "general disclosure" and "selective filing" approach.[5] Although the CCP claims that the purpose of the new regulations is to promote fairness and transparency in online recommendation services and stipulates that service providers should "adhere to mainstream values" and "actively communicate with positive energy" to the information consumers, but in fact, it's giving warning messages to online media companies: they should avoid spreading opinions unfavorable to the state or manipulating information to influence people's judgment, which will be seen as disrupting public order by indirectly challenging "ideological security" and even attempts to challenge the ruling power of the CCP.

4. In Chapter 2, Article 6: "Regulations on Network Security Review" proposes that providers of big data computing recommendation services should "adhere to the mainstream value actively communicate with positive energy"; Article 7: "clarify the main responsibility of algorithm recommendation service providers" to build a platform accountability system; Article 9: "establish a functional feature database for identifying illegal and undesirable information".

5. Chapter 4, "Supervision and Management," requires that providers of big data computing recommendation services with "public opinion attributes" or "social mobilization capabilities" should provide information to the CCP authorities within 10 working days from the date of service provision, and cooperate with the authorities to carry out "security assessment" as well as "supervision and inspection work" in Article 24.

3. Trend Observation

3-1. Chinese companies caught in confrontation between China and US

In the first half of 2021, 35 Chinese companies went public on the US stock market with a record-high US$12.3 billion raised in financing.[6] However, the CCP authorities have been conducting cybersecurity audits to Didi Chuxing Technology, Full Truck Alliance Group (a truck-matching information platform), and BOSS Recruiting (a recruitment website and mobile phone app) on the grounds of "national security" since July 2021. In the second half of the year, under pressure from the CCP, Little Red Book (an online shopping and social networking platform), Hello Inc (a bike-sharing service provider), Qiniu Cloud (a cloud computing company), and Keep (a fitness app) withdrew their US IPO (or fundraising/stock offering) plans; and Himalaya (an online audio sharing platform) as well as Huolala (a logistics business) simply cancelled their IPO plans in the US. The Security Regulations further underline the CCP regulators' restrictive attitude towards overseas IPOs. Since the CCP has data collection methods and regulations that are different from or even contradict those of other countries, overseas companies are also forced to make choices under the CCP's strict data security regulation framework. For example, LinkedIn, a talent social networking site, and Yahoo, a search engine company, withdrew from the Chinese market or changed their business direction in October 2021 due to "changes in the business environment".[7]

While the CCP tightens its control over data, the US is also becoming more stringent on incoming Chinese companies. The US Securities and Exchange Commission (SEC) officially announced the implementation of the Holding Foreign Companies Accountable Act (HFCAA) on December 2, 2021, which requires foreign companies listed in the US to file documents with the SEC to prove

6. "Chinese stocks in the US set off a second listing in Hong Kong," *Economic Daily News*, July 8, 2021. https://money.udn.com/money/story/11038/5585910.
7. "LinkedIn to Shut Down Service in China, Citing 'Challenging' Environment," *New York Times* Chinese, October 15, 2021

that they are not owned or controlled by foreign governments.[8] The more a Chinese company listed abroad is subject to the jurisdiction and investigation of foreign regulators, the more likely it will be also subject to cybersecurity scrutiny by Chinese regulators for "national security" reasons, which will further affect its trustworthiness overseas, creating a vicious cycle. The new regulations are expected to make it extremely difficult for Chinese companies, especially those in the Internet industry, to list on the New York Stock Exchange (NYSE) or Nasdaq in the future.[9] Ordained by Chinese President Xi Jinping, the official opening of the Beijing Stock Exchange on November 15, 2021, is intended to urge Chinese companies to leave the US and list locally instead to facilitate the financial disconnection between the US and China and create a "Chinese Nasdaq". The new regulations do not prohibit listing in Hong Kong since the city is not considered a foreign territory under the "one country, two systems" concept, a large number of Chinese technology giants may give priority to listing in Hong Kong to be exempted from cyber security scrutiny. Under such a policy, it is expected that more Chinese companies will choose to stay domestic or list in Hong Kong; but Hong Kong is not what it used to be, it remains to be seen whether Chinese technology enterprises can really stay under the cybersecurity radar of the CCP.

3-2. Effectiveness of first algorithm regulations remain to be seen

With the widespread use of artificial intelligence (AI), Internet companies turn information of millions of users into product recommendations through sophisticated algorithms to generate enormous profits today. In recent years, governments including the US and India have attempted to enact regulatory measures to prevent AI abuse but were caught in a legislative stalemate; and most countries hesitate to impose

8. "International Economy: SEC Finalizes Accountability Law for Foreign Companies, Didi Announces Delisting from the US," *China Times*, December 3, 2021
9. "Beijing Stock Exchange Opens with 81 Companies in First Transactions," *Radio France Internationale*, November 15, 2021. https://www.rfi.fr/tw/ 中國 /20211115- 北京證交所開張 -81 家企業首批交易。

punitive regulations as they might hinder economic growth and technological innovation. Europe was once a pioneer in data-related legislation that regulates large US technology companies, but now the EU countries are still exploring the regulation for AI technology due to different economic constraints and regulatory concepts. Since the end of 2020, the CCP has launched a series of crackdowns on online enterprises, such as financial services, taxi services, and data management, and started to conceive control plans for algorithms in September 2021. It's the world's first systematic legal document for such regulations and has attracted attention from the international community.

The CCP had previously adopted a successful European approach to data regulation; but with the release of China's first governance regulation focusing on algorithms, it is clear that its legislature has explored new possibilities that Europe and the US will be closely observing the effectiveness of the CCP's subsequent regulation. In particular, Chapter 3 of the Algorithm Regulations on user rights protection followed the common consumer consensus to provide the "right to know" about the status of recommendation services, and the "right to choose" to turn off recommendation services without providing personal information. If the implementation of Algorithm Regulations is a success, the US and European countries may consider adopting this approach to some extent. For the development of AI technologies such as algorithms , however, an open, innovative Internet environment and a free, tolerant atmosphere are crucial. Although data is a key resource for computing power to evolve, technology platforms in China are still receiving more restrictions on data processing as the Chinese authorities constrain the environment of innovation and cut incentives for technology development for local consumer technology companies. To China's goal of becoming the world's technological powerhouse, this is contradictory.

Table: The key amendments of the Security Regulations

Article 2 Article 5 Article 6 Two key targets for scrutiny	1. Critical information infrastructure operators: (i) The purchaser of network products and services should anticipate the national security risks that may arise after they are put into use. (ii) Products and services that affect or may affect national security should be reported to the Office of Network Security Review for examination. (iii) For procurements applied for cybersecurity audits, critical information infrastructure operators should require product and service providers to cooperate with cybersecurity audits through procurement documents, agreements, and other papers.
	2. Internet platform operators: Overseas listing of platforms with user data of over one million must declare cybersecurity examination. (Article 7)
Article 8 4 types of review filing Materials	1. Declaration forms 2. Analytic reports on products that affect or may affect national security 3. Procurement documents, agreements, contracts to be signed or listing application documents to be submitted for IPO 4. Other materials needed for cybersecurity audits
Article 10 7 types of reviews focused assessment of national security risk factors	1. Risks of illegal control, interference or damage to the critical information infrastructure from the use of products and services. 2. Risks of disruptions in the supply of products and services could jeopardize the business continuity of critical information infrastructures. 3. Security, openness, transparency, diversity of sources, reliability of supply channel, and risk of supply disruption due to political, diplomatic, and trade factors. 4. Compliance of product and service providers with Chinese laws, administrative regulations, departmental rules and regulations. 5. Risk of theft, leakage, destruction, illegal use, or illegal exit of core data, important data, or large amounts of personal information. 6. Risk of product sales causing critical information infrastructure, core data, important data or a large amount of personal information to be influenced, controlled or abused by foreign governments, as well as the risk of network information security. 7. Other factors that may jeopardize the security of critical information infrastructure, network security and data security.

Source: "Regulations on Network Security Review," Cyberspace Administration of China, January 4th, 2022. http://www.cac.gov.cn/2022-01/04/c_1642894602182845.htm.

(Originally published in the 48th "National Defense and Security Biweekly", February 25, 2022, by the Institute for National Defense and Security Research.)

(The contents and advice in the assessments are the personal opinions of the authors, and do not represent the position of the Institute for National Defense and Security Research.)