An Introduction to the Chinese Internet Regulation

Chieh-Jan (Simon) Sun[1]

I. Introduction

On April 20th, 1994, the Institute of High Energy Physics at China's Academy of Sciences connected to the World Wide Web through facilities based at Stanford University's Stanford Linear Accelerator Center. 26 years later, about 904 million people in China have access to the internet, which is considered the largest group of internet users in the world as of 2020. More Chinese internet companies have been established, and more U.S. internet companies are trying to enter the Chinese market. It has become increasingly critical to understand how China regulates the internet, including the primary internet regulations and the philosophy behind it.

This article will first introduce a brief history of internet regulation development in China. The article divides the time period before 2016 into three stages, including the stage of building up the foundation, the stage of forming a systematic regulation, and the stage of creating the triple headed regulatory model. Further, to understand the prominent provisions of the contemporary Chinese Internet regulation and the underlying philosophy, this article will provide a thorough dive into the 2016 Chinese cyber security law.

II. A Brief History of the Chinese Internet Regulation

The progress of the Chinese Internet regulation can be categorized into three stages. These stages are divided based on the enactment of the major internet regulations as well as the establishment of prominent government bureaucracies.

A. Stage One: Building up the Foundation

The first stage of the Chinese internet regulation starts from the issuing of "Regulations of the People's Republic of China for Safety Protection of Computer Information Systems" (中华人民共和国计算机信息系统安全保护条例), which is the first Chinese internet law. The law was published on February 18th, 1994, and three related regulations were issued following this regulation, including "Interim Regulations of the People's Republic of China on the Management of International networking of Computer Information " (中华人民共和国计算机信息网络国际联网管理暂行规定) in 1996, "Measures for Security Protection Administration of the International Networking of Computer Information Networks" (计算机信息网络国际联网安全保护管理办法) in 1997, and "Implementation Rules for Provisional Regulations of the Administration of International Networking of Computer Information in the People's Republic of China" (中华人民共和国计算机信息网络国际联网管理暂行规定实施

[1] Chieh-Jan (Simon) Sun is a recent graduate of Duke Law (LL.M. '20) and an incoming S.J.D. candidate at Maurer School of Law, Indiana University (Bloomington). The author wishes to thank Professor David Hoffman for the valuable comments and edits that greatly improved the manuscript and Tianjiu Zuo for helping with collecting the materials.

办法) in 1998. These laws have collectively set out basic principles for internet regulation in China, and those principles can still be seen in modern Chinese internet regulations.

Overall, four main principles have been set out from these regulations. *First*, the country's internet connectivity must come from government owned or controlled facilities. In particular, to carry out international networking of computer information, the connectivity should only be conducted through facilities controlled by the Ministry of Posts and Telecommunications. Individuals are not allowed to use their own facilities for international networking. *Second*, the establishment of new interconnected networks (接入网络) must be approved by the state. These new interconnected networks are different from the traditional interconnected networks (互联网络), which contain the China Public Computer Interconnected Network, the China Golden Bridge Information Network, the China Education and Research Computer Network, and the China Science and Technology Network. New interconnected networks must submit their applications to the Leading Group for Information Technology Advancement after being approved by ministerial level authorities, and shall then submit the applications to the State Council for final approval. *Third*, the government shall formulate a safety grading protection for the computer information system. The goal of this new requirement is to combat cybercrime, data voyeurs, and phishing. These provisions eventually resulted in the publication of the "Classified criteria for security protection of computer information system" by the Ministry of Public Security in 2001, which classifies the information systems into five different grades. The *fourth* principle is the most well-known one, which is defining the content that should not exist on the web. These types of content were first mentioned in the 1997 law, which includes:

1. Information that instigates the resistance and disruption of the implementation of the Constitution, laws and administrative regulations;
2. Information that instigates the subversion of the state political power and overthrow of the socialist system;
3. Information that instigates the splitting up of the country and sabotage of national unity;
4. Information that instigates hatred and discrimination among nationalities and sabotages solidarity among nationalities;
5. Information that fabricates or distorts facts spreads rumors and disrupts social order;
6. Information that propagates feudalistic superstitious, obscenity, pornographic, gambling, violence, murder and terror and instigates crimes;
7. Information that openly insults others or fabricates facts to slander others;
8. Information that damages the reputation of state organs; and

9. Other information that violates the Constitution, laws and administrative regulations.

B. Stage Two: Forming a Systematic Regulation

The starting point of the second stage is the publication of "Regulation on Internet Information Service of the People's Republic of China "(互联网信息服务管理办法) by the State Council on September 25th, 2000. The enactment of this regulation indicates that China had entered the era of more systematic approach to Internet regulation.

There are three crucial parts of this regulation—*first*, the establishment of building the licensing and filing systems. The law divides internet information services into two categories: profitable internet information services and non-profitable internet information services. The state establishes a *licensing system* for profitable internet information services and a *filing system* for non-profitable internet information services. In addition, any entity who intends to provide internet information service related to news, publication, education, medical and health care, pharmaceuticals and medical equipment, etc., before applying for licenses for filing for the record, shall obtain approval from the competent industry authorities as required by relevant laws and administrative regulations.

Second, a more precise categorization of the nine types of content that internet information service providers shall not produce, copy, publish or distribute: (1)against the Cardinal Principles set forth in the Constitution ; (2)detrimental to State security, State secrecy, State power and national unification; (3)detrimental to State honor and interests; (4)instigating ethnic hatred or discrimination and detrimental to national unity; (5)detrimental to State religious policy, propagating heretical or superstitious ideas; (6)disseminating rumors, disrupting social order and stability; (7)disseminating obscenity, pornography, force, brutality and terror or crime-abetting; (8)humiliating slandering others, trespassing the lawful rights and interests of others; (9)other contents forbidden by laws and regulations. These requirements are a modification of the fourth principle mentioned above, with the same concepts but with more precise descriptions and categorizations. This provision became the so-called "nine-prohibited-content" (九不准) requirement as the same legal text can also be seen in other regulations.

Third, a more inclusive approach toward *information service providers* to regulate content online. *To start with*, telecommunications administrative authorities shall *publish* the names of internet information service providers who have obtained a service license or have filed their activities on the record. This is known as the *public disclosure system*. *In addition*, a *record tracking system* is created and certain obligations are imposed on internet information service providers. An internet information service provider who provides news, publication or electronic bulletin boards shall keep records of relevant information such as the publishing date and the internet address or domain name; an internet information

service provider who provides internet connection service shall keep records of the connection time, account number, the internet address or domain name, and the telephone number of their users. Such records shall be kept for 60 days and provided to relevant authorities for checking when so requested. *Finally*, in response to the nine illegal content mentioned above, when an internet information service provider finds illegal content that is being transmitted in its website, it shall terminate the transmission immediately. The service provider shall also keep records and report to relevant authorities.

C. Stage Three: Creating the Triple Headed Regulatory Model

The marking point of this stage is 2008, as the "triple-headed" regulatory model (三驾马车) was established. That year, the number of internet users in China has reached 2.53 billion people, which was considered the most in the world. Fifty different agencies were regulating the internet, and the major challenge for the Chinese government was to coordinate various agencies governing the vast amount of internet users. Eventually, three prominent agencies become responsible for most of internet regulation, and the "triple-headed" regulatory model was created.

The Ministry of Industry and Information Technology (MIIT) (工业和信息化部) was established in 2008, and the Cyberspace Administration of China (CAC) (国家互联网信息办公室) was established in 2011 and reconstructed in 2014. At the same time, the Ministry of Public Security (MPS) (公安部) had been actively regulating cybercrime since the 2000s. The three agencies have separate responsibilities. The MIIT is responsible for the administration of China's industrial branches and information industry. The CAC is in charge of cyberspace security and internet content regulation. The primary functions of the agency are directing, coordinating, and supervising online content management and handling administrative approval of businesses related to online news reporting. The MPS had functional departments for areas such as intelligence, police operations, prisons, and political, economic, and communications security, which primary goal for the internet is combating cyber-criminal activities and responsible for running the so-called "Great Firewall of China" system.

As different entities have different goals, there are several concerns among the three bodies. The *first* concern happens within the scope of the MIIT's mission. The purpose of MIIT often overlaps with the two other governmental agencies, as any action can facilitate the development of the information industry. The *second* concern comes from CAC being a relatively young agency. MIIT and the MPS have been responsible for internet regulatory affairs since the early years and have accumulated lots of experiences. The lack of experience of the CAC may cause the insufficiency of control. Also, most internet regulation only authorizes MIIT and MPS on governmental affairs, and only a limited number of new rules would authorize CAC on specific tasks. The *third* concern

arises in the imbalance of resources among different agencies. The CAC and the MPS both have agencies established from the national level to the local level. However, the MIIT does not have much lower body entities. This difference in the number of agencies creates an insufficiency of governing resources and power of the MIIT.

III. Cyber Security Law of the People's Republic of China

A. Introduction

The "Cyber Security Law of the People's Republic of China" (中华人民共和国网络安全法) was issued on November 7th, 2016, and came into effect on June 1st, 2017. The significance of this regulation is that the issuing authority is the Standing Committee of the National People's Congress, and its level of authority is "Law" instead of administrative regulation. This law indicates that China is entering the fourth stage of internet regulation as it is currently the highest authority of internet regulation in China. It is critical to examine the regulation thoroughly to understand the contemporary Chinese internet regulation philosophy and the regulatory approach.

B. Internet Sovereignty

The spirit of Internet Sovereignty is explicitly mentioned in the first article of the law, which states as follows: "This Law is developed to guarantee cybersecurity, safeguard *cyberspace sovereignty*, national security and public interest, protecting the lawful rights and interests of citizens, legal persons, and other organizations, and promoting the sound development of economic and social information." As there are different definitions of what it means by Internet Sovereignty, they all overlap with one central concept- the protection of *critical information infrastructure*. In other words, the territorial limit of Internet Sovereignty reaches the critical information infrastructure built in the nation. The regulation on critical information infrastructure is, therefore, the critical concept of "Cyber Security Law of the People's Republic of China".

President Xi has set "Internet Sovereignty" as one of the four principles of internet regulation in his speech during the World Internet Conference in China in 2015. President Xi quoted the "sovereign equality of states" principle from the United Nations and emphasized that this principle should be applied not only between countries in a physical matter but also on a virtual matter - The internet. President Xi declared that the ultimate goal of Internet Sovereignty is to respect the development, regulatory model, internet public policy of different countries, and not to pursue network hegemony.

President Xi made this remark in 2015, right after the "Edward Snowden Leak" in 2013, and the Hong Kong "Occupy Central with Love and Peace" protest in 2014. Those incidents made the Chinese government realize two things. *First*, the internet has become a battlefield for different nations as the U.S. National Security Agency (N.S.A.) has been carefully monitoring the Chinese government's activities online and classified documents are leaked. *Second*, the internet has become a forum where different ideologies

are spread, and prominent social movements can be stirred up. In a general matter, distinguishing features of the cyber world such as anonymity, decentralization, and de-stratification make the Communist Party worry that the virtual-world might affect real-world orders, and reshape or weaken the existing communist regulatory regime. The Communist Party is concerned that people might identify themselves with virtual sovereignty order, which will damage the ideology shaped by the communist party. Thus, Internet Sovereignty became a reasonable response toward all of those concerns for the Communist Party to gain more control over the web and create new orders.

C. Network Information

To protect network information, according to article 10, technical measures shall be taken for the construction and operation of the network or the provision of services through the system. The compulsory requirements of national standards are to ensure the safe and stable operation of the network, effectively respond to cybersecurity incidents, prevent illegal criminal activities committed on the web, and maintain the *integrity*, *confidentiality*, and *availability* of network data. Confidentiality, integrity, and availability of data are known as the CIA Triad, which is considered as the foundation of information security. Confidentiality means that "data, objects, and resources are protected from unauthorized viewing and other access." Integrity means that "data is protected from unauthorized changes to ensure that it is reliable and correct." Availability means that "authorized users have access to the systems and the resources they need."

The regulation then carefully defines what it means by "illegal network information." According to article 12, any individual or organization using the network shall comply with the Constitution and laws, follow public order and respect social morality, and shall not endanger cybersecurity. Also, they shall not use the network to conduct any activity that endangers national security, honor and interest, incites to subvert the state power or overthrow the socialist system, incites to split the country or undermine national unity, advocates terrorism or extremism, propagates ethnic hatred or discrimination, spreads violent or pornographic information, fabricates or disseminates false information to disrupt the economic and social order, or infringes upon the reputation, privacy, intellectual property rights or other lawful rights and interests of any other person. The basic regulatory model of "illegal information" in the cyber security law and the "nine-prohibited-content" mentioned above are the same. The difference appears in the description of the legal concept, as contemporary issues such as terrorism, false information, privacy, and intellectual property rights are included in the text.

D. Security Requirement for Network Operators

The third chapter of the regulation regulates the general legal obligation for network operators. Under article 76, a "network operator" means the owners and administrators of the network and network service providers. The applicable scope of

"network operators" include traditional telecom operators; internet firms; financial institutions that collect citizens' personal information and provide online services (such as banking institutions, insurance companies, securities companies and foundations); providers of cybersecurity products and services; enterprises that have websites and provide network services. In general, enterprises and institutions that provide services and conduct business activities through networks may also be considered network operators.

The obligations for network operators are regulated through ten provisions. There are *four* prominent requirements governed by law. *First*, the state shall implement rules for a cybersecurity graded protection system. (Article 21) Network operators shall ensure that the network is free from interference, damage or unauthorized access, and prevent network data from being divulged, stolen or falsified. It is worth noting that scholars have pointed out that as the cybersecurity graded protection system is not equivalent to the first-stage computer information grading system, the two systems do correlate with each other.

Second, network products and services shall comply with the compulsory requirements of relevant national standards. (Article 22) When a provider discovers any risk such as security defect and vulnerability of its network products or services, it shall immediately take remedial measures the requirement of notification when the discovery of data breaches. However, there are concerns that the legal terminology is quite vague, as the article does not strictly define what it means by "immediately." The law does not provide any specific deadlines or guidance on how to notify users and authorities.

Third, network operators shall require users to provide accurate identity information when signing agreements with users or confirming the provision of services. (Article 24) This is known as the *real-name registration system*, which can be first seen in the *second* stage of internet regulation. The difference between these two stages is the responsible entity, which in the *second* stage the obligation is imposed on the information service providers; in the *fourth* stage, it is imposed on the users. The mechanism is called "real name in private, voluntary in public" (后台实名，前台自愿), which means that the users would have to register the service with their real name, but would be able to display their user name however they would like. Users without a verified real name could only browse the internet and could not post or repost content. Through the real-name registration system, the government agency has the ability to monitor all Chinese content on the web, and has laid the foundation for the future "social credit system."

Fourth, network operators shall provide technical support and assistance to public security authorities and state security authorities in legally safeguarding state security and investigating crimes. (Article 28) However, this provision might mean providing "backdoor access" to the government as the article does not specify what such "technical

support and assistance" will entail. Besides, providing "technical support and assistance" to the Chinese government may infringe on their intellectual properties or their users' privacy rights.

E. Critical Information Infrastructure

Network operators which are considered as Critical Information Infrastructure are subject to a heightened standard of care and scrutiny, which is regulated through the second section of the third chapter of the law. As stated before, imposing obligations on critical information infrastructure is the implementation of the spirit of Internet Sovereignty. Under Article 31, critical information infrastructure means public communications and information services, energy, transport, water conservancy, finance, public facilities, and e-government affairs.

According to Article 34, critical information infrastructure operators shall fulfill the following security protection obligations:

1. Establishing specialized security management institutions and designating persons in charge of security management, and reviewing the security background of the said persons in charge and personnel on crucial positions.
2. Conducting cybersecurity education, technical training, and skill assessment for employees on a periodical basis.
3. Making disaster recovery backups of critical systems and databases.
4. Making emergency response plans for cybersecurity incidents and organizing drills on a periodical basis.
5. Performing other obligations prescribed by laws and administrative regulations.

Additionally, according to Article 35, where critical information infrastructure operator's purchase network products and services, which may affect state security, they shall pass the state security inspection organized by the national cyberspace administration in conjunction with the State Council's relevant departments. As the law does not clearly define what types of procurements may "affect national security" and how a company can pass a "security inspection", it is important to follow the future interpretations of this provision by the government.

Finally, according to Article 37, personal information and related data collected and produced by critical information infrastructure operators during their operations within the territory of the People's Republic of China shall be *stored within China*. This provision is known as the "data localization" requirement, which is the most prominent provision of this section. It is worth noting that, China's data localization requirement is quite comprehensive, relative to the data localization requirements in Germany, Australia, and India. The provision would create a significant effect on foreign companies with operations in China that store or transfer data overseas. Article 37 will result in new

compliance costs for multinationals, which typically rely on cross-border flows of business data.

F. Network Information Security

There are eleven provisions in this section of the law, and there are three prominent parts among those regulations. *First*, according to article 41, to collect and use personal information, network operators shall follow the principles of legality, rightfulness and necessity, disclose the rules for collection and use, explicitly indicate the *purposes*, *means* and *scope* of collecting and using information, and obtain the *consent* of the persons whose information is collected. Network operators shall not collect personal information irrelevant to the services provided by them, shall not collect or use personal information in violation of the provisions of any law or administrative regulation or the agreement of both parties, and shall dispose of personal information preserved by them in accordance with the provisions of laws and administrative regulations and agreements with users. This section is mainly regulating companies privacy policies and is the establishment of the "*minimum sufficient principle*" (最少够用原则), which means the collection of personal information should not exceed the basic needs. As the concept is still quite vague, a clear interpretation of this provision shall be followed by "the Measures for the Determination of the Collection and Use of Personal Information by Apps in Violation of Laws and Regulations."

Second, modern cybercrime issues such as wire fraud, illegal information, and malware are regulated through Article 46, Article 47, and Article 48. In terms of *wire fraud*, according to Article 46, it is prohibited set up any website or group chat for committing fraud, teaching others how to commit a crime, producing or selling any prohibited or controlled article, or committing any other illegal or criminal activity, and shall not use the network to release the information involving commission of any illegal or criminal activity such as fraud, and the production or sale of any prohibited or controlled article. As a massive amount of *illegal information* flows on the internet, according to Article 47, network operators shall strengthen the management of information released by their users and shall immediately react to prevent the information from spreading, preserve relevant records, and report it to the competent department, if it finds any information of which the release or transmission is prohibited by any law or administrative regulation. To combat *malware attacks*, electronic information sent, or application software provided by any individual or organization, must not install malicious programs, and must not contain information for which laws and administrative regulations prohibit the publication or transmission.

Third, in response to the development of technology, a new complaint and reporting system for network information security is required by law. According to article 49, network operators shall establish a complaint and reporting systems for network

information security, disclose the ways for filing complaints and reports and other information, and accept and handle complaints and reports related to network information security in a timely manner. The purpose of this provision is to use the internet as a leverage to provide more legal assistance to the public, and to speed up the process of accepting complaints and reports.

IV. Conclusion

After 26 years of development, China created internet laws covering almost every aspect of the cyber world, including content moderation, cyber security, cybercrime, and privacy policy. There is a clear pattern behind the different stages of development, as the regulation on prohibited content is very similar among every step of regulation, and both the prototype of the 2016 Chinese cyber security law's graded protection system and real-name registration system can be found in internet regulations in early stages. Simultaneously, to cope with the rapid growth of internet users and the characteristic of the internet, the invention of the triple-headed regulatory model and the emphasis on Internet Sovereignty became a unique way for the Chinese government to respond. Governing nine hundred million people on the web is not an easy task, and it is fascinating to see how the Chinese Internet law will evolve.