Assessing China's Cybersecurity Law

Article *in* Computer Law & Security Review · September 2018

DOI: 10.1016/j.clsr.2018.08.007

COMPUTER LAW & SECURITY REVIEW 34 (2018) 1342–1354

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Assessing China's Cybersecurity Law

Aimin Qi[a], *Guosong Shao*[b,*], *Wentong Zheng*[c]

[a] *School of Law, Chongqing University, Chongqing, China*
[b] *School of Media and Communication, Shanghai Jiao Tong University, 800 Dongchuan Road, Shanghai 200240, China*
[c] *Levin College of Law, University of Florida, Gainesville, FL, USA*

ARTICLE INFO

Article history:

Keywords:
Cybersecurity Law
Cyberspace sovereignty
National security
Personal information
Critical information infrastructure
Free flow of data
Freedom of speech

ABSTRACT

In November 2016, China passed its first Cybersecurity Law, aiming to strengthen cyberspace governance through a number of initiatives, including Internet operator security protection, personal information protection, special protection of critical information infrastructure, local storage of data, and security evaluation for data export. This Article discusses the major concepts and principles of the Cybersecurity Law. It also discusses the tensions and controversies inherent in the law. All in all, the Cybersecurity Law exhibits distinctive Chinese characteristics. It is premised on the concept of cyberspace sovereignty and emphasizes security over free flow of data and freedom of speech. It provides a basic legal framework for cyberspace governance in China, to be supplemented by implementing regulations in years to come.

Cybersecurity is becoming an increasingly significant issue confronting governments and businesses alike around the world. Over the last several years, a series of high-profile cybersecurity incidents helped push the issue to the forefront of public attention. During the 2016 U.S. presidential campaigns, hackers breached the computer systems of the Democratic National Committee and leaked thousands of DNC documents on Wikileaks.[1] In 2017, hundreds of thousands of computers worldwide were attacked by the WannaCry ransomware worm, resulting in billions of dollars in damages.[2] In the same year, Equifax, one of three major credit reporting agencies in the United States, suffered a cybersecurity breach in which highly sensitive personal and financial information for around 143 million U.S. consumers was compromised.[3] In 2018, semiconductor giant Intel revealed that its chips contain a feature that makes them vulnerable to hacking.[4] Most

* Corresponding author: Guosong, Shao, School of Media & Communication, Shanghai Jiao Tong University, 800 Dongchuan Road, Shanghai 200240, China.
E-mail address: gshao@sjtu.edu.cn (G. Shao).

[1] See Tom Hamburger & Karen Tumulty, *Wikileaks Releases Thousands of Documents About Clinton and Internal Deliberations*, The Washington Post (Jul. 22, 2016), https://www.washingtonpost.com/news/post-politics/wp/2016/07/22/on-eve-of-democratic-convention-wikileaks-releases-thousands-of-documents-about-clinton-the-campaign-and-internal-deliberations/?utm_term=.5ad08eddb51b.

[2] See Jonathan Crowe, *WannaCryRansomware Statistics: The Numbers Behind the Outbreak*, Barkly.com (May 2017), https://blog.barkly.com/wannacry-ransomware-statistics-2017.

[3] See Gillian B. White, *A Cybersecurity Breach at Equifax Left Pretty Much Everyone's Financial Data Vulnerable*, The Atlantic (Sept. 7, 2017), https://www.theatlantic.com/business/archive/2017/09/equifax-cybersecurity-breach/539178/.

[4] See Ian Jing Cao, *Intel Says Broad Range of Chips are Vulnerable to Hack, Downplays Impact*, Bloomberg (Jan. 3, 2018), http://www.latimes.com/business/la-fi-intel-chip-flaw-20180103-story.html.

https://doi.org/10.1016/j.clsr.2018.08.007

recently, in March 2018, it was revealed that a data analytics firm harvested personal information of 50 million Facebook users and used the information to help Donald Trump's presidential campaign.[5]

Governments around the world have responded to cybersecurity concerns by tightening cybersecurity laws and regulations. More than ninety countries have enacted special laws to safeguard cybersecurity. Among the major cybersecurity laws are the U.S. Cybersecurity Information Sharing Act (CISA) (2015), the European Union Directive on Security of Network and Information Systems (NIS Directive) (2016) and the Cybersecurity Basic Act of Japan (2014).

China is a late comer on the global cybersecurity scene. Over the past two decades, the rapid growth of the Internet has brought about fundamental changes to the everyday lives of the Chinese people. However, the Internet also poses enormous problems for the Chinese society, including perceived threats to its political, economic, military, and social security as well as the legal rights and interests of citizens.[6] Prior to 2017, China enacted several laws and regulations in response to these problems.[7] However, because of their inherent ambiguity and fragmented jurisdictions, these laws and regulations are insufficient in dealing with the increasing challenges facing cyberspace. In November 2016, China's efforts to strengthen cybersecurity culminated in the enactment of the Cybersecurity Law of the People's Republic of China.[8]

The Cybersecurity Law is the main building block of China's emerging cyberspace strategies.[9] In drafting the Cybersecurity Law, China partially borrowed the legislative experience of the United States, the United Kingdom, and other countries while maintaining distinctive Chinese characteristics. Many of the principles embodied in the law, however, reflect tensions between conflicting goals. Some of the principles are downright controversial, prompting concerns in the international business communities. As an indication of such concerns, more than forty international companies published open letters opposing the law during the law's drafting stage.[10]

This Article provides an in-depth evaluation of China's approach to cybersecurity as embodied in the Cybersecurity Law. The Article proceeds as follows. Part I introduces the legislative background, purpose, and framework of the law. Part II elaborates on major principles of the law. Part III discusses the tensions and controversies which the law is faced with. Part IV concludes the paper.

1. Overview

1.1. *Legislative background*

China built its first connection to the Internet in 1994 and has since become one of the largest Internet markets in the world.[11] As of 2014, China's proportion of the Internet economy to GDP surpassed that of the United States.[12] Today, China has the most Internet users in the world—710 million, compared to 460 million in India and 290 million in the United States.[13]

While enjoying the convenience of search engines, e-commerce, social networks, big data, and cloud computing, Internet users are also exposed to various cyber threats such as hacker attacks, surveillance, and leakage of personal information. China is one of the countries that suffer the most serious threats from the Internet. According to National Internet Emergency Center (CNCERT), there were 126,916 cybersecurity incidents within and beyond the borders of China in 2015, with year-on-year growth of 125.9 percent.[14] The majority of these threats come from inside China, with a total number of 126,424 cases and year-on-year growth of128.6 percent.[15] Some of these incidents have caused significant social impact. For example, in 2013, the personal information of over one million customers of YTO Express, a major courier firm in China, was leaked and sold.[16] In 2014, China's leading

[5] See Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytic in Major Data Breach*, The Guardian (Mar. 17, 2018), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

[6] *See* 国务院新闻办公室 [Press Office of the State Council],《中国互联网状况白皮书》[White Paper on Internet in China], Feb. 26, 2014, http://www.cac.gov.cn/2014-02/26/c_126192365.htm.

[7] These laws and regulations include The NPC Standing Committee Decision on Maintaining Network Security (2000), Regulations on Computer Information System Security Protection (revised in 2011), The Decision on strengthening Network Information Security by the NPC Standing Committee (2012), Regulations Regarding Telecom and Internet Users' Personal Information Protection by the Ministry of Industry and Information Technology (2013), The National Security Law of the P.R.C. (2015), and The Anti-Terrorism Law of China (2015).

[8] See 中华人民共和国网络安全法 [The Cybersecurity Law of the People's Republic of China], http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm [hereinafter *Cybersecurity Law*].

[9] See 《国家网络空间安全战略》[National Cyberspace Security Strategies], http://www.xinhuanet.com/politics/2016-12/27/c_1120196479.htm; 《网络空间国际合作战略》[International Cyberspace Cooperation Strategies], http://www.xinhuanet.com/politics/2017-03/01/c_1120552767.htm.

[10] *See* 全球 40 企业团体致函反对中国网络安全法 [Forty Companies and Organizations Oppose China's Cybersecurity Law],《联合早报》[United Morning Post] (Nov. 12, 2016), http://www.zaobao.com/realtime/china/story20161112-689426.

[11] *See* Jaime A. Flor Cruz & Lucrezia Seu, From Snail Mail to 4G, China Celebrates 20 Years of Internet Connectivity, CNN (Apr. 23, 2014), https://www.cnn.com/2014/04/23/world/asia/china-internet-20th-anniversary/index.html.

[12] 麦肯锡:中国互联网经济占 GDP 比重已超美国 [McKenzie: China Surpasses the U.S. in Internet-to-GDP Ratio], 新浪财经 [Sina Finance] (Jul. 25, 2014), http://tech.sina.com.cn/i/2014-07-25/10509516789.shtml.

[13] Russell Flannery, *What Makes China's Internet Growth So Fast and Volatile?* Forbes (Oct. 10, 2017), https://www.forbes.com/sites/russellflannery/2017/10/10/what-makes-chinas-internet-growth-so-fast-and-volatile/#5d3db66e4852.

[14] 国家互联网应急中心: 2015 年中国网络安全事件超 12 万 [National Internet Emergency Center: Cybersecurity Incidents Totaling Over 120,000 in 2015],《新浪财经》[Sina Finance] (May 25, 2016), http://finance.sina.com.cn/roll/2016-05-25/doc-ifxsqtya6047103.shtml.

[15] Id.

[16] 圆通快递百万客户信息遭泄露 [Personal Information of 1 Million YTO Express Customers Leaked],《新闻晨报》[Morning News] (Oct. 23, 2013), http://news.ifeng.com/mainland/detail_2013_10/23/30573231_0.shtml.

online travel booking agency, Ctrip.com, disclosed that it found and fixed a security loophole that made users' credit card information vulnerable to hacking.[17]

The burst of these alarming cybersecurity incidents has not only awakened people's awareness of cybersecurity, but also strengthened the Chinese government's determination to improve cyberspace governance. From the perspective of the Chinese government, a comprehensive law dealing with cyber threats is necessary to ensure cybersecurity. In particular, since Xi Jinping became President, he has emphasized the importance of promoting cybersecurity laws on several important occasions, including the World Internet Conference and the meetings of the Central Leading Group for Cyberspace Affairs.

Meanwhile, Chinese scholars have laid the groundwork for a comprehensive cybersecurity law. Over the years, Chinese scholars have explored the definition and implications of cyberspace sovereignty,[18] and have introduced the concept of state territorial network sovereignty.[19] They have also explored issues concerning personal information protection, cross-board data transfer and critical information infrastructure protection.[20] These research efforts offer a solid theoretical foundation for the Cybersecurity Law.

1.2. *Legislative purposes*

Article 1 of the Cybersecurity Law states that the purposes of the law are "to ensure cybersecurity, to safeguard cyberspace sovereignty, national security, and social and public interests, to protect the lawful rights and interests of citizens, legal persons, and other organizations, and to promote the healthy development of the informatization of the economy and society."[21] The Cybersecurity Law embodies the national security principle promulgated in China's National Security Law and considers cyberspace sovereignty as its highest priority. The law accomplishes this goal through its emphasis on protecting the security of network operations, the security of critical information infrastructure, and the security of online information. In the meantime, the Chinese government actively participates in international cyber cooperation to promote the development of the Internet economy while maintaining national cyberspace sovereignty. These legislative purposes reflect a multi-dimensional perspective on cybersecurity that encompasses both security and development interests.

The establishment of the legislative purposes of the Cybersecurity Law was not without controversies. During the law's drafting period, forty-six international organizations from the United States, Europe, Asia, and Oceanic regions signed a letter opposing the draft law and insisted on revising the draft law in accordance with international trade regulations on the assumption that the law would raise trade barriers. Nevertheless, upon consultations with experts, the Chinese government formally passed the law in November 2016. The overseas groups then asked for suspension of the newly enacted law. In spite of these controversies, the Chinese authority insisted on implementing the law and declared that the government would supplement the law with corresponding regulations and standards in time.

1.3. *Legislative framework*

The Cybersecurity Law guides government agencies, commercial organizations and citizens on how to access the Internet. It is a manifestation of the government's will on cyberspace governance. In terms of its content, the Cybersecurity Law has seven chapters and seventy-nine articles, and its framework follows the traditional legislative model-general provisions followed by specific provisions. The general provisions of the Cybersecurity Law stipulate the purpose and scope of the legislation, the national policy on cybersecurity protection, the enforcement authorities, the basic principles of the legislation, and special protections for juvenile Internet users. The specific provisions contain provisions in six areas, including cybersecurity, network operations security, network information security, monitoring and emergency responses, legal liabilities, and supplementary provisions.

It is worth noting that the Cybersecurity Law only provides a general legal framework for dealing with cybersecurity concerns. Its basic function is to build China's cybersecurity legal system, not to solve any specific cybersecurity issues. This inevitably leads to ambiguous and incomplete legal rules. Complementary rules and regulations will be necessary to deal with specific cybersecurity issues. A number of regulations are expected to be promulgated and implemented, including the Critical Information Infrastructure Protection Regulations, Measures on the Security Assessment of Cross-Border Transfer of Personal Information and Important Data, Catalog of Critical Network Equipment and Specialized Cybersecurity Products, and Information Security Technology Guidelines for Data Cross-Border Transfer Security Assessment. These regulations would operationalize the principal provisions of the law and greatly advance the law's legislative goals.

2. Major principles

As China's first basic Internet law governing cybersecurity, the Cybersecurity Law contains several major principles and innovations, such as cyberspace sovereignty, a hierarchical system for cybersecurity protection, a critical information infrastructure protection system, a security assessment system for cross-border data transfers, and a security review system for network products and services. The discussions below highlight these major principles of the law.

---

[17] Zhang Ye, *Ctrip Hit by Security Loophole*, Global Times (Mar. 24, 2014), http://www.globaltimes.cn/content/850298.shtml.

[18] See, e.g., Zhang Xinbao & Xu Ke, 网络空间主权的治理模式及其制度构建 [The Governance Model of Cyber Sovereignty and Its Institutional Implementation],《中国社会科学》[China Social Sciences], 2016(8), 139-158.

[19] See, e.g., Hu Li & Qi Aimin, 论"网络疆界"的形成与国家领网主权制度的建立 [The Emergence of Cyberspace Territories and the Construction of State Territorial Network Sovereignty],《法学论坛》[Law Forum], 2016(2), 59-66.

[20] See, e.g., Qi Aimin, 个人信息保护法研究 [Research on Personal Information Protection Laws],《河北法学》[Hebei Legal Science], 2008(4), 15-33;Liu Jinrui, 我国网络关键基础设施立法的基本思路和制度建构 [The Basic Approach and Institutional Implementation of the Chinese Legislation on Network Critical Infrastructure Protection],《环球法律评论》[Global Law Commentaries], 2016(5), 116-133.

[21] Cybersecurity Law, *supra* note 8, art. 1.

2.1. *Cyberspace sovereignty*

Article 1 of the Cybersecurity Law stipulates that the law's purpose is to protect cyberspace sovereignty. The principle has been proposed for many years in the country. In a white paper released by the Chinese government in early June of 2010, the government states that the Internet is a critical infrastructure of a country, the network within the Chinese territory ought to be under China's jurisdiction, and China's Internet sovereignty should be respected and protected.[22] Afterwards, the sixth United Nations General Assembly issued Document A/68/98 on June 24th, 2013, which passed a resolution drafted by a group of government experts concerning the development of the information and telecommunications industries. Article 20 of Document A68/98 stipulates that national sovereignty and international norms and principles derived from national sovereignty shall apply to information and communication technology activities at the national level, as well as to jurisdiction over information and communications technology infrastructure within the country's territory. According to Fang Binxing, a member of the Chinese Academy of Engineering, this document actually establishes the cyberspace sovereignty of a country.[23]

Furthermore, President Xi Jinping delivered an opening speech to the First World Internet Conference in November 2014, stating that China is willing to work with other countries and regions in the world to improve international cooperation, respect Internet sovereignty, and maintain cybersecurity. This was the first time the Chinese government proposed a concept of cyberspace sovereignty. After that, China released a new National Security Law in July 2015, which in Article 25 clearly defined the concept of cyberspace sovereignty and spelled the goal of building a network and information security system. This finally made cyberspace sovereignty an important component of national sovereignty, protected by China's legal system.[24] In November 2016, the promulgation of the Cybersecurity Law formally established the principle of cyberspace sovereignty, which was supplemented partially by rules on localization of data storage and cross-border data transfers. Besides, with the promulgation of China's Cyberspace Security Strategy in December 2016 and the International Cyberspace Cooperation Strategy in March 2017, the principle of cyberspace sovereignty was officially enshrined in the national cyberspace strategies and became a cornerstone of China's cyberspace policies.

As a natural extension of national sovereignty on the Internet, cyberspace sovereignty requires compliance with the main national sovereignty principles, such as the equality of nations, peaceful settlement of disputes, and respect of other nations' internal affairs. Specifically speaking, cyberspace sovereignty encompasses the following four rights: the right of jurisdiction, the right of self-defense, the right of independence, and the right of equality.

The right of jurisdiction refers to a nation's right to manage the networks within its territory. Article 2 of the Cybersecurity Law provides that "this law applies to the construction, operation, maintenance, and usage of networks, as well as cybersecurity supervision and management within the mainland territory of the People's Republic of China."[25] This provision ensures territorial jurisdiction over network-related matters in China, whether they are civil, criminal, or administrative in nature. According to this provision, individuals whose activities are related to the Internet within the Chinese territory (including Internet service providers, network operators, Internet users, and regulators, etc.), materials (including network infrastructure), network information (including personal information and important data), as well as cyber activities themselves (such as unlawful and criminal cyber activities targeting information system) are all subject to this jurisdiction. Consequently, as long as the cyber activities occur within the territory of mainland China, no matter what identities or nationalities the actors have, they are all subject to the law.

The right of self-defense refers to a sovereignty state's right to defend against cyber-attacks and threats from the outside. Article 5 of the Cybersecurity Law stipulates that "the State takes action to monitor, prevent, and dispose of cybersecurity risks and threats arising both within and without the mainland territory of China. The State protects critical information infrastructure against attacks, intrusions, interference, and destruction. The State punishes unlawful and criminal cyber activities in accordance with the law, preserving the security and order of cyberspace." This provision affirms China's right of defense in cyberspace and allows the Chinese government to monitor, defend against and punish foreign cyber-attacks and threats. Furthermore, Article 75 provides that for those who conduct attacks, intrusions, interference, destructions or other activities for the purpose of endangering the critical information infrastructure of the People's Republic of China, whether they are organizations or individuals, if they have caused serious consequences, the Chinese government shall take measures in accordance with the law to either freeze their assets or to take other necessary punitive measures. In other words, Article 75 implements the right of self-defense specified in Article 5, and provides the legal basis for penalizing overseas cyber-attacks and surveillance.

The right of independence refers to the right of operating a nation's networks independently, without being subordinate to the power of other countries. So far, there are only thirteen DNS Root Name Servers in the world, and the United States owns ten of them. Theoretically speaking, if the United States blocked a certain country's domain name on the root server, the country's top domain name websites would instantly disappear on the internet. In this sense, the United States has a global monopoly on the Internet, and the rest of the world cannot achieve complete independence in the cyberspace. It is thus argued that cyberspace sovereignty should represent an independent form of a country's sovereignty. A country is

[22] Press Office of the State Council, *supra* note 6.

[23] Zhi Zhenfeng, 网络主权植根于现代法理 [Cyberspace Sovereignty Has Rootes in Modern Legal Jurisprudence], 《光明日报》 [Guangming Daily], Dec. 17, 2015.

[24] See《中华人民共和国国家安全法》[The National Security Law of the People's Republic of China] art. 25, http://www.npc.gov.cn/npc/xinwen/2015-07/07/content_1941161.htm.

[25] Cybersecurity Law, *supra* note 8, art. 2. Note that the Cybersecurity Law applies only in mainland China, not in Hong Kong, Makau, and Taiwan.

within its rights to manage issues concerning cybersecurity, to formulate relevant laws and regulations, to protect its information systems and information resources against outside threats, interference, attacks or damages, as well as to protect the lawful rights and interests of citizens in cyberspace. In sum, countries should respect one another's cyberspace sovereignty and should not interfere with other counties' internal affairs.

The right of equality requires countries to access and connect to one another's Internet on an equal basis. The right of equality ensures that different countries have equal jurisdiction over their own network systems, and that the management of one country's network does not do harms to another country's networks. However, because of the borderless and interdependent nature of the Internet, the Internet policies initiated by the United States may benefit its own interests at the expense of developing countries. This gives the United States much more power in comparison with other countries in global Internet governance. In view of this situation, Article 7 of the Cybersecurity Law proposes to promote a peaceful, secure, open, and cooperative cyberspace, and to establish a multilateral, democratic and transparent Internet governance system.[26] China's International Cyberspace Cooperation Strategies also provides that "countries, big or small, strong or weak, rich or poor, are all equal members of the international community and are all entitled to equal participation in developing international order and rules in cyberspace through international governance mechanisms and platforms, to ensure that the future development of cyberspace is in the hands of all peoples."[27] These provisions demonstrate the Chinese government's advocacy for an equal and orderly cyberspace.

2.2. *Network operators' security obligation*

According to the Cybersecurity Law, network operators are defined as network owners, managers or service providers.[28] This definition represents an expansion of the scope of network operators. Specifically, the definition of network operators not only includes traditional telecom operators, but also covers all entities that can provide products and services through the Internet, such as entities providing information or website design services as well as individuals or organizations operating websites. Notably, Article 2 of the Cybersecurity Law specifies that all network operators, whether they be foreign-funded or domestically-funded, should all take responsibility for performing their legal obligations.[29]Similarly, Article 10 stipulates that "the construction and operation of networks, or the provision of services through networks, shall be done in accordance with the provisions of laws and administrative regulations, and in accordance with the mandatory requirements of State standards. They should also adopt technical measures and other necessary measures to safeguard cybersecurity and operational stability, effectively respond to cybersecurity incidents, prevent cybercrimes and unlawful activity, and preserve the integrity, secrecy and usability of online data."[30] The Cybersecurity Law specifies the following obligations for network operators:

2.2.1. *Hierarchical system for protecting cybersecurity*

China implemented a hierarchical information security protection system before it promulgated the Cybersecurity Law. In 1994, the State Council promulgated the Rules on Protection of Computer Information Systems to provide for a hierarchical protection system. In 1999, the Ministry of Public Security issued the Guidance for Classifying Protection Levels for Computer Information Systems. The Guidance provides for five levels of security protection for computer information systems: user self-protection, system audit, security tagging, structured protection, and access verification protection. These five protection levels impose increasingly higher requirements in terms of access control, identity authentication, and data integrity. In 2007, the Ministry of Public Security, together with other relevant ministries, formulated the Measures on Hierarchical System for Information Security Protection, which stipulates that the protection level for a computer information system should depend on the importance of the information system to national security, economic development, and social life, and the adverse impact of the security breach on national security, social order, public interests, as well as lawful rights and interests of the citizens, legal persons, and other organizations. This provision classifies security protection of information systems into five levels, and requires operators and users of information systems to use products that conform to national standards, to formulate safety rules, and to conduct self-assessment and inspection of security risks.

The Cybersecurity Law legally confirms the hierarchical system for protecting cybersecurity, which requires network operators to act in accordance with the hierarchical system for cybersecurity protection. Specifically, operators have the following obligations under the hierarchical system: establishing internal security management systems and operational procedures, ascertaining the responsible entities who are in charge of network security, taking technical measures to prevent computer viruses, network attack, network intrusion, and other forms of behavior that endanger network security; taking technical measures to monitor and record all network operating activities and cybersecurity incidents, preserving relevant weblogs for not less than six months as required, and taking measures to categorize, duplicate, and encrypt important data.[31] With the enactment of the Cybersecurity Law, the Chinese government is expected to promulgate implementing rules to strengthen the hierarchical protection system.

2.2.2. *Security review of network products or services*

To prevent cybersecurity incidents and improve the security of network products and services, the Cybersecurity Law sets out clear rules on network product or service providers' security obligations. Article 22 of the law stipulates that network

[26] Cybersecurity Law, *supra* note 8, art. 7.
[27] International Cyberspace Cooperation Strategies, http://www.gocatti.com/archives/3639.
[28] Cybersecurity Law, *supra* note 8, art. 76.
[29] *Id*. art. 2.
[30] *Id*. art. 10.
[31] Cybersecurity Law, *supra* note 8, art. 21.

products and services shall comply with the relevant mandatory national standards. Network product or service providers shall not install malicious programs. Upon discovering that their products or services have security flaws or vulnerabilities, they shall immediately adopt remedial measures and promptly inform users and report to the competent authorities. They shall continuously provide security maintenance for their products and services, and shall not terminate security maintenance within the legally required period or the period agreed upon by the parties. These requirements are minimal requirements that any network product or service providers have to meet. By comparison, in July 2017, Singapore released a draft Cyber Security Act that would establish a dual licensing scheme that imposes different qualification requirements for investigative cybersecurity service providers as opposed to non-investigative cybersecurity service providers.[32] This latter approach would increase the entry barrier to the cybersecurity industry and improve overall security level, and will prompt firms to hire specialized personnel to maintain network security. However, this approach might lead to the loss of market competitiveness, especially for small businesses, due to excessive network security maintenance costs.

In addition to the above general obligations, the Cybersecurity Law also imposes a testing and certification scheme for critical network equipment and cybersecurity products. Article 23 of the law provides that critical network equipment and cybersecurity products shall comply with the national standards and mandatory requirements, and be inspected and certified by a qualified institution, before being sold or provided. This requirement is different from the general requirement for network products and services in that it requires security inspection and certification. In response to allegations by foreign institutions that this requirement will increase business costs and trade barriers, the Chinese government plans to formulate a catalog of critical network equipment and cybersecurity products and to promote inter-accreditation of security inspection and certification results, so as to facilitate the review process. At present, the Chinese government has issued the first edition of the catalog of critical network equipment and cybersecurity products, which includes key equipment like routers, servers, anti-spam product safety database systems, and other special products.

The Cybersecurity Law also targets the network products and services security purchased by critical information infrastructure operators. Article 35 of the law requires that network products or services purchased by critical information infrastructure operators that might impact national security shall undergo a national security review organized by the state cybersecurity authorities and relevant departments of the State Council. According to this Article, network operators or network products or services providers need to submit relevant contents to the Chinese government for review purposes, which might include software source code protected by intellectual property laws, encryption algorithms, design details, and trade secrets, etc. Many overseas network operators including Microsoft, Intel, and IBM are concerned that China will take advantage of this provision and force them to hand over core technologies and trade secrets. If these business secrets are obtained by competitors or criminals, it will cause them a huge loss.[33] In light of this concern, one provision was added to the final version of the Cybersecurity Law, which prohibits information obtained by cybersecurity authorities from being used for purposes other than protection of cybersecurity.[34] Strict legal liabilities will be imposed for violations of Article 30.[35] This might alleviate foreign companies' concerns to some extent. In addition to the national security review, Article 36 of the Cybersecurity Law also requires that when purchasing network products or services, critical information infrastructure operators shall sign a security and confidentiality agreement with the provider, clarifying duties and responsibilities for security and confidentiality. Due to the importance and complexity of network security review, the Chinese government has also promulgated Provisional Measures on Security Review for Network Products and Services to implement the security review provisions of the Cybersecurity Law.

2.2.3. *Network real-name system*

China started to enact a network real-name system more than ten years ago. In 2003, many local authorities supervising Internet cafes all over China required all Internet users to provide personal identity cards for real-name registration. In 2004, the Ministry of Education released Opinions on Further Strengthening the Management of Campus Networks in Higher Education, which clearly proposed the implementation of the real-name system on the networks of higher education institutions. By March 2005, led by Tsinghua University's Shuimu Tsinghua BBS, a group of major universities began to shift to intra-school communication platforms based on a real-name system. Subsequently, China's local governments like Hangzhou and Beijing also promulgated rules and regulations concerning the real-name system. In 2012, China released the Decision of the NPC Standing Committee on Strengthening the Protection of Online Information, which requires network service providers to obtain real identity information from their customers when they provide Internet access, landline or mobile phone services, and information dissemination services. In accordance with this provision, the State Internet Information Office promulgated the Internet User Account Name Management Regulations in 2015. Similarly, Article 7 of the Administrative Regulations on Mobile Internet Information Services, released in June 2016, also requires mobile Internet application providers to obtain customers' real identity information. The Cybersecurity Law affirms the real-name principle. Article 24 of the Cybersecurity Law provides that network operators handling network access and domain registration services for users, operators handling stationary or mobile phone network access, and operators providing users with information publication or instant messaging services, shall require users to provide real identity information when signing agreements with

[32] See Cybersecurity Bill, July 2017, https://www.csa.gov.sg/~/media/csa/cybersecurity_bill/draft_cybersecurity_bill_2017.ashx?la=en.

[33] Georges Haour, *Why China's new cyber-security law is bad news for business?* Fortune (Dec. 1, 2016) http://fortune.com/2016/12/01/china-cybersecurity-law-business/.

[34] Cybersecurity Law, *supra* note 8, art. 30.

[35] *Id*. art. 73.

users or confirming provision of services. Where users do not provide real identity information, network operators must not provide them with relevant services.[36] This was the first time that a real-name system was formally written in the law with the aim to stem widespread illegal phenomena in the cyberspace such as rumors, defamation, invasion of privacy, and telecommunications frauds. However, the real-name registration system may cause real damage to privacy. In December 2001, for instance, six million individuals' usernames and passwords for the CSDN website were posted online. After that, the same situation happened to Renren, Douwan, 178.com, 7K7K smart games, and other well-known websites.[37] It is argued that if users were not forced to register with their real identities on those websites, the information leaks would not cause real harm to users.

2.3. *Protection of personal information*

In the information age, data has become a basic social resource. The establishment and improvement of personal information protection laws and other relevant regulations have become an important task for all the nations in the era of big data. China started late in enacting personal information protection. According to incomplete statistics, there are more than 100 laws concerning personal information in China. Besides the Decision of the NPC Standing Committee on Strengthening the Protection of Online Information and the General Principles of Civil Law of the People's Republic of China, other personal information protection provisions are scattered in criminal laws, administrative regulations, departmental regulations and judicial interpretations. These laws and regulations suffer from low efficiency, lack of coverage, overlapping jurisdiction, and failure to provide effective legal protection for personal information. The Cybersecurity Law provides legal protection for personal information specifically, and this is the first time that China has defined and protected personal information under the law besides the General Principles of Civil Law of the People's Republic of China. The Cybersecurity Law has the following highlights:

2.3.1. *The scope of personal information*

Personal information is defined under the Cybersecurity Law as various information recorded in electronic or other means that can lead to the identification of a natural person, including but not limited to the natural person's name, date of birth, identity card number, personal biometric information, address, telephone number and so on.[38] This definition is largely in line with the current mainstream view of personal information in China.[39] Article 4 of the European Union's latest General Data Protection Regulations (GDPR) also adopted a similar concept of identification. According to this definition, personal information must be identifiable. It should be noted that even if a piece of information cannot be identifiable individually, it is still personal information if it can identify the identity of a natural person when combined with other information. With the improvement of identification technology and the continuous integration of data, information that was previously unable to identify individuals may be identified again, which makes the definition of personal information more dynamic and situational.[40] Therefore, information that may be able to identify individuals should be combined with specific application scenarios and technical conditions to determine whether it constitutes personal information. However, if a network operator has implemented an anonymous processing of personal information so that a particular person cannot be identified, the information will no longer be considered personal information and will be allowed to be offered to others without the permission of relative users.[41] This provision thus provides a legal basis for enterprises to take advantage of and share data by means of anonymity.

2.3.2. *The principles of personal information protection*

Although China already has a large number of rules on the collection, processing and use of personal information, the Cybersecurity Law is the first one that confirms the principle of personal information protection in the form of law. Article 41 of the law provides that network operators should collect and use personal information in lawful manners, disclose how they collect and use personal information, and make clear the purpose, manner and scope of the collection and use of information. Network operators shall not collect personal information unrelated to the services provided by them, shall not collect and use personal information in violation of laws and administrative regulations and agreement of both parties, and shall deal with personal information in accordance with the provisions of laws and administrative regulations and the agreement with the users. This provision draws upon the relative provisions of the European GDPR of 2016 as well as the U.S. Consumer Privacy Protection Act of 2015, and establishes the international principles for the collection, use and handling of personal information of network operators, i.e., the principles of openness, informed consent, clear purpose, and limitation of purpose.

2.3.3. *Providing institutional space for the development of the big data industry*

According to the personal information protection law, legislators should promote the free flow and reasonable use of information while protecting the individual's interests.[42] Law should not become a stumbling block to the development of the big data industry, which is also the purpose of 13th Five-year Plan of the National Economic and Social Development

[36] *Id*. art. 24.

[37] CSDN 600 万用户数据泄露多个网站遇类似事件 [6 Million Customers' Data Leaked at CSDN], 网易科技 [Netease Technology] (Dec. 23, 2011), http://tech.163.com/11/1223/02/7LU5RGHI000915BF.html.

[38] Cybersecurity Law, *supra* note 8, art. 76.

[39] See Qi Aimin, 拯救信息社会中的人格——个人信息保护法总论 [Saving Personalities in the Information Age—General Comments on Personal Information Protection Laws] 北京大学出版社 [Peking University Press] (2009).

[40] Paul M. Schwartz & Daniel J. Solove, The PII Problem: Privacy and a New Concept of Personally Identifiable Information, 86 N.Y.U. Law Review 1814 (2014).

[41] Cybersecurity Law, *supra* note 8, art. 42.

[42] Qi Aimin, 信息法原论——信息法的产生与体系化 [The Origins of Information Law] 武汉大学出版社 [Wuhan University Press] (2010).

of the PRC and the State Council Action Plan for the Promotion of Big-data Development. Article 42 of the Cybersecurity Law provides that network operators shall not disclose, tamper with, or destroy collected personal information, and shall not provide personal information to others without the agreement of the users. In addition, the Article establishes the principle of data security, requiring network operators to take technical and other necessary measures to ensure the safety of users' personal information collected, and to prevent the disclosure, damage and loss of information. In case of personal information leakage, damage, and loss, immediate remedial measures should be taken to inform the users and report to the relevant authorities. This provision is consistent with the international community's approach to network security incidents and is of great significance in effectively curbing personal information leakage in China. At the same time, this provision provides an exception where the information is unable to identify a particular person. This exception is arguably beneficial to the development of the big data industry.

2.3.4. *Right to correct and delete*

Article 43 of the Cybersecurity Law provides that if a person discovers that a network operator violates the laws, administrative regulations, or the parties' agreement in collecting and using his personal information, he shall have the right to require the network operator to delete his personal information. If the network operator collects and stores his personal information incorrectly, he has the right to require the network operator to delete or correct it. This provision partially draws upon the right to correction under Article 16 and the right to be forgotten under Article 17 of the European GDPR. It is worth noting that the right to deletion was written into law for the first time. In the big data era, the right to deletion will help network users strengthen their control of personal information. However, the right to correction and deletion is only part of the personal information rights. In the future, China should speed up the enactment of a unified personal information protection law and add the right of inquiry, blockade and opposition, so as to build a better system of personal information rights.

2.3.5. *Prohibition against sale of personal information*

In both theory and practice, personal information is protected as personality rights, which require that personal information not be sold. China's 2009 amendments to the Criminal Law expressly prohibits the sale of personal information, but its scope is limited to State organs or personnel of financial, telecommunications, transportation, education, medical and other institutions. This limitation does not effectively curb sales of personal information. For this reason, the 2015 amendments to the Criminal Law Amendment broadens the scope and applies it to any organizations or individuals, and also integrates it into the crime of infringing upon citizens' personal information. With social concerns being aroused by the Xu Yuyu incident, the Supreme People's Court of China and the Supreme People's Procuratorate jointly released the Interpretation of Several Issues Concerning the Application of Law in Criminal Cases of Infringing Upon Citizen's Personal Information in May 2017, and made detailed stipulations on the definition and sentencing of the crime of infringing upon citizens' personal information. In this respect, Article 44 of the Cybersecurity Law stipulates that no individuals or organizations shall steal or illegally acquire personal information or sell or illegally provide personal information to third parties. This provision is a reaffirmation of the protection of personal information in the Criminal Law, and also provides the basis for claims of personal information infringement.

Unfortunately, the Cybersecurity Law has a weaker penalty for illegal acts. According to Article 64 of the law, network operators who violate the above-mentioned personal information protection requirements will be fined no than 10 times the illegal income. In accordance with Article 83 of the European GDPR, if the operator violates the regulations concerning personal data protection, the Data Protection Agency will impose fines of 2% of the company's global turnover capped at 10,000 EUR or 4% of the company's global turnover capped at 20,000 EUR, depending on the nature of the offenses.[43] The GDPR is called the most stringent data protection regulations in history. By comparison, China's punishment is relatively weak. There are still doubts about whether personal information protection can meet the expectations. In addition, although Article 45 of the Cybersecurity Law provides that government authorities and their staff members must not disclose or sell personal, private, or business confidential information that is acquired in the course of carrying out their law enforcement duties, this provision does not specify the corresponding legal liability, which has to be supplemented by detailed implementing regulations in the future.

2.4. *Critical information infrastructure protection*

Critical Information infrastructure plays a key role in society and attacks on or destructions of critical information infrastructure could be a lethal blow to a country's political and social life. On July 11, 2017, China's State Internet Information Office promulgated a draft Critical Information Infrastructure Safety Protection Regulations to solicit public views on combating breaches of critical information infrastructure in China by overseas organizations or individuals. Ensuring the safety of critical information infrastructure through legislation has become a social consensus. The EU Network and Information Systems Security Directive employs the concept of Operators of Essential Services to distinguish from Digital Service Providers and sets different obligations for them. Singapore's draft Network Security Act also provides a definition of critical information infrastructure and specifies the authority charged with certifying critical information infrastructure. The Cybersecurity Law specifically provides for critical information infrastructure protection. The main provisions include:

2.4.1. *Definition and scope of critical information infrastructures*

Article 31 of the Cybersecurity Law states that information infrastructure in public communications, information services, energy, transportation, water conservancy, finance, public services, e-government and other critical industries and fields, or

[43] General Data Protection Regulation, Art. 83, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

other information infrastructure that is key to national security and public interests, receives priority protection under the law. In nature, critical information infrastructure is different from network operators and has more stringent requirements in terms of security, network products and services procurement, data storage, and data transfers. In China, the Office of the Central Leading Group for Cyberspace Affairs established the Guidance for National Network Safety Inspection Operation in June 2016. According to this guidance, critical information infrastructure refers to "operating information systems or industrial control systems that provide network information services to the public or support energy, communications, finance, transportation, utilities and other important industries. These systems affect the normal operation of important industries and, once breached, will cause serious losses. As a result, the scope of critical information infrastructure in this guidance is quite broad. It includes not only governmental websites, but also popular online platforms providing instant messaging, e-commerce, search engine, email, map, and other services. This means that a large number of influential commercial network services that are used by average people are likely to be considered critical information infrastructure.

Regarding methods of certification, China's draft Critical Information Infrastructure Security Protection Regulations require relevant authorities to develop guidelines on certifying critical information infrastructure identity and carry out the certification. In Singapore, under the draft Internet Security Act, the certification and decertification of critical information infrastructure are carried out by the Commissioner of Cybersecurity. Other network security authorities are not authorized to conduct the certification. The Singapore law also empowers members of the Network Security Council to obtain information about computers or computer systems. When the Network Security Council has reasons to suspect that a computer or a computer system is critical information infrastructure, it has the right to require the owner of the computer or computer system to submit information on the specific functions, service objects, technical parameters and other aspects of the computer or computer system.[44] By contrast, China takes a more rational approach by having regulators and industry authorities share the certification authority. Singapore's practice of giving the certification and decertification authority to one government agency may jeopardize the objectivity of the decisions. In addition, Singapore's law may also lack reasonable restrictions on the access of cybersecurity commissioners to the relevant information, especially business secrets and other business information.

2.4.2. *Legal obligations of critical information infrastructure operators*

The mandatory obligations of network operators that are considered critical information infrastructure under the Cybersecurity Law have received much attention. Once identified as part of critical information infrastructure, a network operator will be charged with more onerous network security obligations than average network operators. These obligations mainly include: (a) stable and reliable business operation, planning, adoption, and use of security measures;[45] (b) establishing security management agencies and security management personnel to educate, train and evaluate employees, backing up critical systems and databases in case of emergencies, developing contingency plans and conducting drills;[46] (c) security review of network products or services procurement: network products and services involving national security should be reviewed for security by government authorities;[47] (d) confidentiality requirements for network products and services procurement: signing security confidentiality agreements with providers, and making clear security and confidentiality obligations and responsibilities;[48] (e) storage of domestic data: personal information and important data collected and generated by operators of critical information infrastructure should be stored within the territory;[49] (f) security assessment for transfer of data overseas: data exports with legitimate business reasons should undergo security assessment;[50] and (g) security assessment: conducting a security assessment at least once a year and reporting assessment results and suggestions for improvements.[51]

2.4.3. *Local storage of data and data export security assessment*

While local storage of data may be necessary for purposes of national security and social stability, cross-border transfer of data is an inevitable requirement of international economic cooperation. Promoting the free flow of data on a global scale for the development of the digital economy has become a development strategy for many countries and regions. However, in order to reinforce national sovereignty and cyberspace security, countries in the world have enacted laws to restrict the foreign storage and trans-border transmission of specific data. Regarding the issue of data storage and cross-border transmission, the United States had long been advocating and promoting the free flow of data around the world. However, the EU has taken a very different approach. Both the 1995 Data Protection Directive and the 2016 GDPR have made strict restrictions on the transmission of personal data from EU companies to overseas partners. One of these restrictions is that the receiving country in a cross-border data transfer transaction must be certified to have adequate protection for personal information. It requires that full protection of personal data be guaranteed by the receiving country before the implementation of a cross-border data transmission. Since 2015 the European Court of Justice (ECJ) declared invalid the Safe Harbor Agreement between Europe and the United States in 2000, the two sides have reached a new Privacy Shield Agreement on cross-border transmission of data.

The Cybersecurity Law, for the first time, imposed a local data storage requirement in the form of law. Article 37 of the law provides that the personal information and im-

[44] Singapore's draft Cybersecurity Bill, Part 3, critical information infrastructure https://www.csa.gov.sg/~/media/csa/cybersecurity_bill/draft_cybersecurity_bill_2017.ashx?la=en.

[45] Cybersecurity Law, *supra* note xxx, art. 33.
[46] *Id*. art 34.
[47] *Id*. art 35.
[48] *Id*. art 36.
[49] *Id*. art 37.
[50] Id.
[51] *Id*. art 38.

portant data collected and generated by operators of critical information infrastructure shall be stored within the territory. If the data need to be transmitted abroad because of business needs, a security assessment shall be carried out in accordance with the methods formulated by the State network and information authorities. This requirement provides basic rules for data storage and cross-border transmission.

In addition, Article 37 of the Cybersecurity Law stipulates that other laws or regulations may also apply to the transmission of data across borders. Specifically, the data required to be stored locally in accordance with other laws or regulations include: population and health data (Section 10 of the Provisional Measures on Population Health Information Management), credit information (Section 24 of the Rules on Credit Industry Administration), personal financial information (Article 6 of the People's Bank of China Notice on the Protection of Personal Financial Information), map data (Section 34 of the Rules on Map Management), online publication data (Article 8 of the Regulations on the Administration of Online Publishing Services); data related to online car-hailing business (Article 27th of the Provisional Measures on Online Car-hailing Operation Service Management).

3. Tensions and controversies

3.1. *Internet openness and cyberspace sovereignty*

Internet openness and cyberspace sovereignty have been considered contradictory with each other. When the Internet was created, the majority view was that the government would be driven away from the new space and traditional boundaries would be broken given the decentralized nature of the Internet. They perceive cyberspace as a global public space and insist that the Internet should not be controlled by any single country.[52] This poses a serious challenge to the legal and political concept of sovereignty. Ever since John P. Barlow published the Declaration of the Independence of Cyberspace in 1996, Internet openness has become a buzz word in the world.

Nevertheless, problems begin to soar as more and more individuals and countries enter the cyberspace. People are increasingly calling for global governance of the Internet since they come to realize that Internet openness should be under the rule of law or the premises of the Internet could be destroyed by uncontrolled openness. Furthermore, it is argued that although a state is incapable of implementing national sovereignty towards cyberspace itself, it could exercise sovereignty over basic network infrastructure and all related activities within its territory.[53] Another view is that although there is no boundary on the Internet, entities such as basic network infrastructure, netizens, and internet companies could all be assigned a nationality. Moreover, they are regarded as essential strategic resources of a particular country, justifying the country's jurisdiction. From this perspective, cyberspace sovereignty would be a necessary principle.[54]

Between cyberspace sovereignty and Internet openness, the Chinese government appears to be inching towards the former. The Chinese government believes that despite the dramatic changes the Internet has brought about, the Internet still needs to be regulated due to the prevalence of illegal activities in cyberspace. Therefore, the Cybersecurity Law clearly stipulates the principle of cyberspace sovereignty, which has set the basis for the Chinese government to regulate the entire Internet.[55] Responding to some criticisms from the international community, some Chinese scholars argue that one needs to look no further than the U.S. control over domain systems to realize that the sovereign states have never ceased to control the cyberspace.[56]

3.2. *Market competition and security review*

During the drafting period of the Cybersecurity Law, some foreign organizations were strongly opposed to security review of Internet products or services. They argued that the security review would increase operation costs and limit foreign companies' market access, which would lead to unfair competitive advantages given to Chinese companies and violations of the market openness commitment made by the Chinese government.

The fact is that as a latecomer to the Internet industry, the core computer hardware and software programs used by both Chinese citizens and enterprises rely heavily on foreign manufacturers. Take the computer operating systems for an example. Due to the lack of R&D efforts by domestic manufacturers, the operating systems adopted by Chinese computer users are dominated by Microsoft Windows and Apple Mac OS. In this context, there is no doubt that the Chinese government is concerned with the hidden safety risks of the network products and services purchased from abroad. Such concerns are not groundless. The disclosures made by Edward Snowden reveal that there are backdoors inserted in foreign security software, which are used as spying tools for foreign intelligence agencies.[57] In 2007, the backdoor inserted in the simplified Chinese operating system of Microsoft Windows was detected by the Norton security software, and it was identified as being specifically written for mainland China.[58] In 2017, the ransomware

[52] The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, available at:https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf.

[53] *See* Tallinn Manual 2.0 on the International Law Applicable to Cyberspace Operations (Michael N. Schmitt eds., 2n ed., 2010), http://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf.

[54] Xie Xinzhou, 打造普惠共享的国际网络空间 [Building an International Cyberspace Conducive to Mutual Benefits], 《人民日报》(People's Daily) (Mar. 17, 2016).

[55] Fang Binxing et al., 网络空间主权研究 [Research on Cyberspace Sovereignty], 《中国工程科学》 [China Engineering Sciences], No. 6, 2016.

[56] *See* Zhang Xinbao & Xu Ke,网络空间主权的治理模式及其制度构建 [The Governance Models of Cyberspace Sovereignty and Its Institutional Implementation], 《中国社会科学》[China Social Sciences], 2016(8), 139-158.

[57] 政府采购对部分软件说不 [Government Procurement To Say No to Certain Software], 法制网 [Legal Net] (Aug. 13, 2014) http://www.legaldaily.com.cn/IT/content/2014-08/13/content_5717899_2.htm.

[58] Jiang Qiping, 蹊跷的微软"后门"事件:诺顿误杀的是秘密程序? [Mysterious Microsoft Backdoor: Secret Program Killed by Norton?],

WannaCry exploited the 445 port vulnerability of Microsoft's Windows system and attacked the network systems of hundreds of Chinese universities, government agencies and gas stations.[59]

The Cybersecurity Law actually sets different obligations for internet operators and operators of critical information infrastructure, and only the Internet products or services purchased by critical information infrastructure operators shall be under strict national security review. The review system, according to the Office of the Central Leading Group for Cyberspace Affairs, "aims to safeguard state cyberspace sovereignty, national security, public interests and rights of citizens, legal persons and other organizations, instead of restricting the access of overseas companies, technology and products to China's market or restricting the free legal and orderly flow of data."[60] It is clearly stated in the Decision of the CCCPC on Several Major Issues Concerning Comprehensively Deepening Reforms at the third plenary session of the 18th CPC Central Committee that the relationship between the government and the market should be to let market play a decisive role in allocating resources, and let the government come in where the market falls short. Neither individuals nor the market can provide cyber protection alone, and cybersecurity regulations are considered an essential part of national security and even global cyber security. Therefore, security review for Internet products and services could be justified as being necessary to defend national security. In actual implementation, however, Internet operators covered by the review are not clearly defined and circumstances where key information infrastructure operators might "jeopardize national security" when buying Internet products and services are not clearly stipulated. This has influenced the implementation of the law, causing uncertainty and puzzlement among both domestic and foreign enterprises.

3.3. *Free flow and local storage of data*

It is argued that although free flow of data can facilitate the growth of digital economy, cross-border transmission of data might endanger the national security and law enforcements of a country as well as the privacy or other personal rights of its citizens. This is why many countries and regions set up restrictions on cross-border flow of data. For example, In the U.K., for example, the Company Act of 2006 states that if accounting records are kept at a place outside the U.K., accounts and returns must be sent to, kept at, a place in the U.K., and must at all times be open to such inspection. Through a decree amending the Code of Electronic Communications, France has included a territorial restriction requiring that the systems for interception of electronic communications must be established in France. In October 2015, Germany adopted a new data retention law, which provides that telecommunication providers must retain data such as phone numbers, the time and place of communication, and the IP addresses for either 4 or 10 weeks, and the data shall be stored in servers located within Germany. Finally, the GDPR launched in 2016 by the EU strengthens the principle of data localization, stating that personal data can only be transferred to countries outside the EU when an adequate level of protection is guaranteed.

To advocates of free flow of data, however, data localization restrictions may function as trade protection since it can be utilized by a country to boost its local economy by propping up its domestic companies.[61] It is also argued that forced data localization may even stifle free speech and political dissent given that the information locally retained can be accessed easily by government authorities.[62] For its part, the U.S. supports eliminating as many barriers to data flows as possible while considering data localization laws as another barrier to trade.[63] At present, the U.S. is seeking new data localization laws within a renegotiated and modernized NAFTA.[64] For the EU, the rules on personal information protection introduced by the GDPR are not perfect. In June 2018, with the passage of the Regulation on the Free Flow of Non-personal Data, EU member states and parliament reached an agreement on a new principle that abolishes data localization restrictions.[65] The regulation covers only non-personal data, however. This includes any data not relating to an identified or identifiable person, such as anonymised data and machine to machine data. Combined with the GDRP, the new rule aims to facilitate the free flow of data in Europe, an important step towards creating Europe's digital single market.

In the case of China, Article 37 of the Cybersecurity Law requires personal information and important data collected by operators of critical information infrastructure to be stored within China's border. This data localization rule allows China to restrict market access for cloud computing if the required data localization requirements are not met. The Chinese government believes that allowing foreign companies to collect information from China without restrictions will put its citizens' privacy, national security and long-term economic de-

人民网 [People's Net] (Jun. 12, 2007), http://it.people.com.cn/GB/42893/5851803.html.

[59] 全球遭遇 Wannacry (永恒之蓝) 勒索蠕虫攻击国内高校及政企内网成重灾区 [Ransomware Wannacry Hits Chinese Universities, Government Agencies, and Enterprises],中国网 [China Net] (May 13, 2017), http://science.china.com.cn/2017-05/13/content_9480800.htm.

[60] 国家网信办相关负责人就《网络安全法》答记者问 [National Network and Information Office Gives Press Interview on the Cybersecurity Law], 人民网 [People's Net] (May 31, 2017), http://politics.people.com.cn/n1/2017/0531/c1001-29309728.html.

[61] Bret Cohen, Britanie Hall, & Charlie Wood, Data Localization Laws and Their Impact on Privacy, Data Security, and the Global Economy. ANTITRUST, Vol. 30, No. 1, 2017.

[62] *See, e.g.*, Jillian C. York, *What's Going on in Central Asia?*, Elec. Frontier Found (Nov. 29, 2012), https://www.eff.org/deeplinks/2012/11/whatsgoing-on-in-central-asia; Kaveh Waddell, *Kazakhstan's New Encryption Law Could Be a Preview of US Policy*, ATLANTIC (Dec. 8, 2015), https://www.theatlantic.com/technology/archive/2015/12/kazakhstans-new-encryptionlaw-could-be-a-preview-of-us-policy/419250/.

[63] William Alan Reinsch, *A Data Localization Free-for-All?* March 9, 2018, https://www.csis.org/blogs/future-digital-trade-policy-and-role-us-and-uk/data-localization-free-all.

[64] Erica Alini, *NAFTA, Trump and the Cloud: What the Negotiations Mean for Your Personal Data, GLOBAL NEWS,* August 2017, https://globalnews.ca/news/3660107/nafta-trump-the-cloud-data-privacy-canada/.

[65] European Commission, *Digital Single Market: EU Negotiates Reach a Political Agreement on Free Flow of Non-personal Data*. June 19, 2018. http://europa.eu/rapid/press-release_IP-18-4227_en.htm.

velopment at risk. Also, it is argued that China among many countries enacts the data location rule not only as a means to reduce its comparative disadvantage in Internet data hosting, but also as a means to reduce its comparative disadvantage in Internet signals intelligence.[66] In spite of this, during the legislative process of this rule, 46 foreign corporate groups led by the American Chamber of Commerce went to great lengths to oppose the rule's enactment out of fear that their business related to the data locally stored in China would be largely jeopardized by the law. The protest was not successful as China finalized the rule.

However, the data localization rule prescribed by the Cyberspace Law does raise several reasonable concerns. Firstly, does this law apply to operators of non-critical information infrastructure? Secondly, the law does not define what constitutes important data. Thirdly, the specific content of security assessment and evaluation procedures is uncertain. In April 2017, China's State Internet Information Office issued the draft Measure on the Security Assessment for Personal Information and Important Data to Be Transmitted Aboard to implement the Cybersecurity Law.[67] The draft measure appears to extend the localization requirement to "network operators" which are far more broadly defined under the law to include network service providers and owners or operators of any systems that gather, store, transmit, exchange, or otherwise process information. While the concept of "personal data" is specifically prescribed in the Cybersecurity Law, the term of "important data" remains undefined in the draft Measure. In addition, due to the aforementioned ambiguity, how to carry out the security assessment of cross-data transmission remains unclear in the draft Measure. Given the significant degree of uncertainty as to the scope and effect of the data localization restriction, the impact of the rule on domestic and foreign businesses is difficult to assess at this stage.

3.4. *Freedom of speech and internet censorship*

Chinese citizens are arguably enjoying more freedom of speech as they have a chance to leverage numerous new media tools to acquire information and express opinion on topics of interest. Meanwhile, the Chinese government is becoming much more responsive to the public opinion, especially those voiced in cyberspace, for the purpose of improving governance and maintaining legitimacy. While the Internet has facilitated the dissemination of information, it has also enabled the spread of information containing pornography, violence, terrorism, and threats to national security and has caused tremendous harms to public safety and national security. Therefore, the Cybersecurity Law sets up a real-name online registration system and a system for reviewing online contents.

The real-name online registration system stipulated in Article 24 of the Cybersecurity Law aims at preventing the spread of irresponsible and illegal contents. The problem is that it may become an obstacle to the free expression of public opinions. For instance, in November 2010, Wang Peng, a Gansu province youth who criticized local officials using his real name on the Internet, was detained in a much publicized criminal case.[68] Although he was acquitted later, this incident became one of the reasons why many people opposed and feared the real-name system. The real-name registration system factually started in Korea in 2008 after actress Choi Jinsil committed suicide reportedly due to malicious comments about her on Internet bulletin boards. The system was then enacted for the purpose of minimizing the amount of negative information to make individuals responsible for their online behaviors. In 2012, however, the Constitutional Court of Korea ruled that the real-name system stipulated by relevant laws is unconstitutional, citing its violation of freedom of speech in cyberspace.[69] Whether and what the Chinese government can learn from the Korean experience so far remain unclear.

As far as the online remarks review system goes, Article 47 of the Cybersecurity Law provides that Internet operators should suspend services immediately upon noticing violations of laws, prevent further spread of the information, save record and report to authority. Article 48 forbids any individual or organization from posting information banned by laws or administrative regulations. These security review systems, however, inevitably give rise to concerns that the government might use them to conduct speech censorship and suppression. There are costs associated with suppression of speech. If citizens could not freely express their opinions, lawmakers and policymakers will not be able to accurately assess the needs of the citizenry. Also, suppression of speech may lead to political and social tensions that may find outlets in more socially disruptive ways. But apparently, the Chinese government believes that the costs of censorship are outweighed by the threats to national security and China's approach to cybersecurity is heavily tilted towards the latter.

4. Conclusion

The Cybersecurity Law aims to strengthen cyberspace governance through a number of initiatives, including Internet operator security protection, personal information protection, special protection of critical information infrastructure, local storage of data, security evaluation for data export and government regulation of cybersecurity. This Article discusses the major concepts and principles of the Cybersecurity Law. It also discusses the tensions and controversies inherent in the law.

[66] John Selby, *Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?* INT'L JOURNAL OF LAW AND INFORMATION TECHNOLOGY, Vol. 25, No. 3, 2017, https://doi.org/10.1093/ijlit/eax010.

[67] China's State Internet Information Office, 《个人信息和重要数据出境安全评估办法(征求意见稿)》 [The draft Measure on the Security Assessment for Personal Information and Important Data to Be Transmitted Aboard], http://www.cac.gov.cn/2017-04/11/c_1120785691.htm.

[68] Xu Yunping & Zhou Zhizhong, 举报公考作弊竟遭 "跨省刑拘" [Reporting Civil Servant Exam Cheating Was Actually Subject to "Inter-Provincial Detention"], People.com. December 3, 2010 http://legal.people.com.cn/GB/13384966.html.

[69] *Online Real-name System Unconstitutional*, KOREA TIMES, August 23, 2012. http://www.koreatimes.co.kr/www/news/nation/2012/08/117_118115.html.

All in all, the Cybersecurity Law exhibits distinctive Chinese characteristics. It is premised on the concept of cyberspace sovereignty and emphasizes security over free flow of data and freedom of speech. It provides a basic legal framework for cyberspace governance in China, to be supplemented by implementing regulations in years to come.