Country Focus Report: China Internet-Related Policy Initiatives and Laws

Veni Markovski & Alexey Trepykhalin
31 January 2022
GE-010 (updated)

ICANN

TABLE OF CONTENTS

Introduction

This paper covers Internet-related policy initiatives and laws/regulations put forward by China between 16 December 2015 and 5 November 2021; ensuring that the ICANN community has the necessary information to develop a better understanding of the deliberations taking place at the U.N., ITU, and other U.N. agencies.

This is part of a periodic series of country-specific reports that provide an overview of activities relevant to the Internet ecosystem and ICANN's mission. Monitoring such initiatives is a fundamental responsibility of the Government and Intergovernmental Organizations Engagement (GE) team of the ICANN organization (ICANN org), in keeping the broader ICANN community informed about issues of importance for the global, single, interoperable Internet and its unique identifier systems.[1]

As in previous GE papers, this report is based on primary source texts related to Internet policies and technologies, such as the Domain Name System (DNS), Internet Protocol (IP) addresses, and protocol parameters, among others. Additionally, this paper relies on relevant texts, statements, and legal/regulatory provisions about positions of China on the same issues at the United Nations (U.N.), International Telecommunications Union (ITU) and domestically.

China's Foreign Policy Statements and Initiatives

On 16 December 2015, in a speech at the Opening Ceremony of the Second World Internet Conference in Wuzhen[2], the President of the People's Republic of China, Xi Jinping, said: "...the international community must enhance dialogue and cooperation on the basis of mutual respect and trust, promote transformation of the global Internet governance system, and work together to foster a peaceful, secure, open and cooperative cyberspace and put in place a multilateral, democratic and transparent global Internet governance system."[3]

To achieve this, President Xi stated that "respect for cyber sovereignty" for individual countries, with participation in "international cyberspace governance on an equal footing" is needed as one of four guiding principles.[4] President Xi also added that "International cyberspace governance should feature a multilateral approach with multi-party participation. It should be based on consultation among all parties, leveraging the role of various players, including governments, international organizations, Internet companies, technology communities, non-government institutions and individual citizens. There should be no unilateralism. Decisions should not be made with one party calling the shots or only a few parties discussing among themselves. All countries should step up communication and exchange, improve dialogue and consultation

[1] "ICANN Operating and Financial Plans," p. 47, ICANN organization, December 2020, https://www.icann.org/en/system/files/files/draft-op-financial-plan-fy21-25-opplan-fy21-20dec19-en.pdf.
[2] The World Internet Conference is held in the town of Wuzhen, Zhejiang province, annually by the Cyberspace Administration of China and Zhejiang Provincial People's Government http://www.wuzhenwic.org/2020-10/15/c_547699.htm.
[3] Remarks by H.E. Xi Jinping, President of the People's Republic of China, at the Opening Ceremony of the Second World Internet Conference, Wuzhen, 16 December 2015 https://www.fmprc.gov.cn/eng/wjdt_665385/zyjh_665391/201512/t20151224_678467.html.
[4] Remarks by H.E. Xi Jinping.

mechanism on cyberspace, and study and formulate global Internet governance rules, so that the global Internet governance system becomes more fair and reasonable and reflects in a more balanced way the aspiration and interests of the majority of countries."[5]

On 7 March 2016, during the ICANN Governmental Advisory Committee (GAC) session, China's representative underscored that the "four principles and the five proposals" put forward by President Xi at the 2016 Second World Internet Conference in Wuzhen "provide us a (indiscernible) account of the thinking and the positions of China for the governance of the Internet."[6]

On 27 April 2016, China released its National Cybersecurity Strategy,[7] explaining the importance for the country in "strengthening international cooperation in cyberspace." To this end, the strategy details that this cooperation should "promote the reform of the global Internet governance system" and "the internationalization of the management of Internet addresses, domain name servers and other such basic resources". The strategy also expressed support for "the United Nations to play a leading role, promote the formulation of international norms for cyberspace that are universally recognized by all sides, and an international treaty on anti-terrorism in cyberspace, complete judicial assistance mechanisms to attack cybercrime, deepen international cooperation's in areas such as policies and laws, technological innovation, standards and norms, emergency response, critical information infrastructure protection, etc." It also called to "establish a multilateral, democratic and transparent international Internet governance system."

On 2 March 2017, China published the International Strategy of Cooperation on Cyberspace.[8] It states that "China will push for institutional reform of the UN Internet Governance Forum to enable it to play a greater role in Internet governance, strengthen its decision-making capacity, secure steady funding, and introduce open and transparent procedures in its member election and report submission." The International Strategy of Cooperation on Cyberspace also states that China "will participate in international discussions on fair distribution and management of critical Internet resources," and that it "will vigorously promote the reform of ICANN to make it a truly independent international institution, increase its representations and ensure greater openness and transparency in its decision-making and operation."[9]

On 20 April 2018, at the National Cybersecurity and Informatization Work Conference in Beijing, President Xi said that "moving forward, reform of the global Internet governance system is the general trend and a common aspiration." He added that "International cyberspace governance should persist in multilateral participation and multi-stakeholder participation, giving rein to the roles of all types of actors, including governments, international organizations, Internet enterprises, the technical community, civil organizations, and individual citizens. We must both

[5] Remarks by H.E. Xi Jinping
[6] MARRAKECH – GAC High Level Governmental Meeting Monday, March 07, 2016, ICANN55 | Marrakech, Morocco, page 86 https://gac.icann.org/transcripts/public/transcript-icann55-gac-hl-governmental-meeting-2016-03-07.pdf..
[7] China Copyright and Media, National Cyberspace Security Strategy, updated on 27 December 2016, https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/.
[8] International Strategy of Cooperation on Cyberspace, China Daily, 2 March 201, https://www.chinadaily.com.cn/kindle/2017-03/02/content_28409210.htm.
[9] International Strategy of Cooperation on Cyberspace, China Daily, 2 March 2017.

promote cyberspace governance within the United Nations framework, and do a better job of giving rein to the positive role of all kinds of non-state actors."[10]

On 9 July 2019, in its submissions to the Open-ended Working Group (OEWG) on Developments in the Field of Information and Telecommunications in the Context of International Security, China noted: "States should work together to create a multilateral, democratic and transparent global Internet governance system. The organization charged with management of critical resources such as Root Servers should be truly independent from any state's control to ensure the broad participation and joint decision-making of all states".[11]

In April 2020, China submitted the following contribution to the U.N. OEWG pre-draft report, in which it stated: "Given the limited amount of time we have, attention should also be drawn to avoid introducing concepts that have not gained global consensus yet ("public core" for instance) into the report," and also: "During the previous two sessions, parties including China have put forward dozens of constructive proposals on issues such as cyber sovereignty, supply chain security, protection of critical infrastructure, refraining from unilateral sanction and fight against cyber terrorism. It is hoped that these proposals could be incorporated in the report."[12]

On 8 September 2020, the Chinese Foreign Ministry published a Global Initiative on Data Security, in which it addresses the need for states to better cooperate in the field of data security, cybercrime, etc. The document suggests that "governments, international organizations, ICT[13] companies, technology communities, civil organizations, individuals and all other actors to make concerted efforts to promote data security under the principle of extensive consultation, joint contribution and shared benefits." The document calls for states to, among other things, "handle data security in a comprehensive, objective and evidence-based manner, and maintain an open, secure and stable supply chain of global ICT products and services."[14]

In March 2021, the Annual "Two Sessions" legislative conference passed the 14th Five-Year Plan and the 2035 Vision, in which Chapter 18 (Creating Good Digital Ecosystem) Section 4 (Promote the construction of a community with a shared future in cyberspace) states: "Advance international exchanges and cooperation in cyberspace, and promote the formulation of international digital and cyberspace rules within the United Nations as the main channel and the

---

[10] New America, Translation: Xi Jinping's April 20 Speech at the National Cybersecurity and Informatization Work Conference, 30 April 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-xi-jinpings-april-20-speech-national-cybersecurity-and-informatization-work-conference/ .

[11] China's Submissions to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, 7 July 2019. https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/09/china-submissions-oewg-en.pdf.

[12] China's Contribution to the Initial Pre-Draft of OEWG Report, 16 April 2020 (dated as from the properties of the PDF), https://front.un-arm.org/wp-content/uploads/2020/04/china-contribution-to-oewg-pre-draft-report-final.pdf .

[13] ICT – information and communications technologies, UNTERM – The United Nations Terminology Database, https://unterm.un.org/unterm/display/record/imo/na?OriginalId=551772be82184a22adaeb86841e335e6.

[14] Global Initiative on Data Security, China Foreign Ministry website, 8 September 2020, https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjfywj_665252/202009/t20200908_599773.html and China launches a global data security initiative to oppose the politicization of data security issues, Reuters, 7 September 2020, https://www.reuters.com/article/wangyi-global-digital-security-0908-idCNKBS25Z0AJ.

UN Charter as the basic principles. Promote the establishment of a multilateral, democratic, and transparent global Internet governance system, and establish a more fair and reasonable network infrastructure and resource governance mechanism."[15]

On 10 March 2021, during the OEWG deliberations at the U.N., China stated: "States should participate in the management and distribution of international Internet resources on equal footings."[16]

On 29 June 2021, China and the Russian Federation issued a joint statement agreeing to extend the existing bilateral "Treaty of Good Neighbourliness and Friendly Cooperation." In the joint statement, they agreed to "reaffirm their commitment to strengthen international information security both at bilateral and multilateral levels" and underscored "their unity on issues related to Internet governance, which include ensuring that all States have equal rights to participate in global-network governance, increasing their role in this process and preserving the sovereign right of States to regulate the national segment of the Internet. Russia and China emphasize the need to enhance the role of the International Telecommunication Union and strengthen the representation of the two countries in its governing bodies."[17]

On 1 November 2021, the Russian Federation made a presentation of its draft text[18] of a proposed U.N. Cybercrime Convention and announced that the text was co-sponsored by China.[19,20]

On 5 November 2021, China introduced its proposals for the U.N. Ad Hoc Committee (AHC) first session.[21]Among other things, it states: "Member States are requested to criminalize the intrusion and destruction of ICTs facilities, systems, data or critical information infrastructure. This may include illegal access to computer information systems, illegal interference with computer information systems, illegal acquisition of computer data, illegal interference with computer data, infringement of critical information infrastructure, etc."

---

[15] Guancha, The "14th Five-Year Plan" and the outline of long-term goals for 2035 (full text), 13 March 2021, https://www.guancha.cn/politics/2021_03_13_583945_5.shtml.

[16] Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Third substantive session, 8–12 March 2021, OEWG Chair's Summary, Conference room paper, 10 March 2021, A/AC.290/2021/CRP.3*, https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf.

[17] The Embassy of the Russian Federation to the United Kingdom of Northern Ireland and Great Britain, Joint Statement of the Russian Federation and the People's Republic of China on the Twentieth Anniversary of the Treaty of Good Neighbourliness and Friendly Cooperation between the Russian Federation and the People's Republic of China, 28 June 2021, https://www.rusemb.org.uk/fnapr/7007 .

[18] United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, 27 July 2021, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_E.pdf .

[19] New UN Convention against cybercrime about to start, fm4.orf.at, https://fm4.orf.at/stories/3019118/ .

[20] Konstantinos Komaitis, Twitter account, 1 November 2021 and 19 January 2022, https://twitter.com/i/web/status/1455217317504327683.

[21] China's Suggestions on the Scope, Objectives and Structure (Elements) of the United Nations Convention on Countering the Use of ICTs for Criminal Purposes: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/Chinas_Suggestions_on_the_Scope_Objectives_and_Structure_AHC_ENG.pdf.

Domestic Statements, Legislation, and Regulations

On 1 July 2015, the National Security Law was passed. It states (art. 59): "The State establishes national security review and oversight management systems and mechanisms, conducting national security review of foreign commercial investment, special items and technologies, internet information technology products and services, projects involving national security matters, as well as other major matters and activities, that impact or might impact national security."[22] Article 25 of the law states: "The State establishes a national network and information security safeguard system, [...] increasing network management, maintaining cyberspace sovereignty, security and development interests."

On 1 June 2017, the Cyber Security Law (CSL) took effect. It stipulates that the State is responsible for "promoting a peaceful, secure, open, and cooperative cyberspace, and establishing a multilateral, democratic, and transparent Internet governance system." The law also provides a provision to store Internet data domestically in the "China mainland." Article 31 of the law defines the scope of the critical information infrastructure to include a "cybersecurity multi-level protection system for public communication and information services, power, traffic, water resources, finance, public service, e-government, and other critical information infrastructure." Article 37 of the law says that, "where due to business requirements it is truly necessary to provide it [personal information, important data] outside the mainland, they [critical information infrastructure operators] shall follow the measures jointly formulated by the State cybersecurity and informatization departments and the relevant departments of the State Council to conduct a security assessment; where laws and administrative regulations provide otherwise, follow those provisions."[23] (The relevant provisions are provided in Appendix 1 to this paper.)

On 24 August 2017, the Chinese Ministry of Industry and Information Technology (MIIT) published the revised Measures on the Administration of Internet Domain Names. [24] (The relevant provisions are provided in Appendix 2 to this paper.)

On 29 January 2018, the MIIT announced, on the basis of Article 5 of its new measures as mentioned above, the adjusted Chinese Internet Domain Name System.[25] (The relevant provisions are provided in Appendix 3 to this paper.)

On 13 June 2019, the Measures on Security Assessment of the Cross-border Transfer of Personal Information proposed in Article 2: "Network operators who provide personal information collected in the course of operations within the mainland territory of the People's Republic of China (hereinafter referred to as personal information outbound transfer), shall

[22]China Law Translate, National Security Law of the People's Republic of China, 1 July 2015, https://www.chinalawtranslate.com/en/2015nsl/.
[23] New America, Translation: Cybersecurity Law of the People's Republic of China (Effective 1 June 2017), 29 June 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.
[24] Ministry of Industry and Information Technology, Internet Domain Name Management Measures, 24 August 2017 https://www.chinalawtranslate.com/en/internet-domain-name-management-measures/.
[25] The URL to the Chinese source is not working as of 19 August 2021, in English: https://www.chinalawtranslate.com/en/chinese-internet-domain-name-system/.

conduct security assessments in accordance with these Measures. If it is determined by the security assessment that the outbound transfer of personal information may affect national security or harm the public interest, or that the security of personal information is difficult to effectively protect, such information shall not leave the country. Where the state has other provisions on the outbound transfer of personal information, those provisions apply." [26]

On 10 June 2021, the 29th meeting of the Standing Committee of the 13th National People's Congress adopted the Data Security Law (DSL).[27] (See relevant texts from the law in Appendix 4 to this paper.)

On 30 July 2021, the new Regulations on the Security Protection of Critical Information Infrastructure were released (after adoption by China's State Council on 27 April 2021). The Regulations define the scope of the Critical Information Infrastructure, provide provisions for the "industries and sectors" to detail the scope further, and define reporting requirements for these agencies to the central cyber authorities in case of an "especially grave cybersecurity incident," such as the "relatively large-scale" leakage of personal information.[28] The Regulations took effect 1 September 2021. (The relevant articles of the Regulations are in Appendix 6 to this paper.)

On 20 August 2021, the National People's Congress Standing Committee of the People's Republic of China passed the Personal Information Protection Law (PIPL). The law went into effect 1 November 2021. The law "is formulated [...] to protect personal information rights and interests, standardize personal information handling activities, and promote the rational use of personal information." The personal information "of natural persons receives legal protection; no organization or individual may infringe natural persons' personal information rights and interests." This law "applies to organizations and individuals handling personal information activities of natural persons within the borders of the People's Republic of China." "Where one of the following circumstances is present in handling activities outside the borders of the People's Republic of China of personal information of natural persons within the borders of the People's Republic of China, this Law applies as well" in cases (1) "Where the purpose is to provide products or services to natural persons inside the borders;" (2) "Where analyzing or assessing activities of natural persons inside the borders;" (3) "Other circumstances provided in laws or administrative regulations." The law also defines personal information and what is included in its handling: "Personal information is all kinds of information recorded by electronic

[26] New America, Translation: New Draft Rules on Cross-Border Transfer of Personal Information Out of China, 13 June 2019, "Personal Information Outbound Transfer Security Assessment Measures (Draft for Comment)," 13 June 2019, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-new-draft-rules-cross-border-transfer-personal-information-out-china/.

[27] Inside Privacy, Covington Unofficial Translation: Measures on Security Assessment of the Cross-border Transfer of Personal Information (Draft for comments), 13 June 2019, https://www.insideprivacy.com/wp-content/uploads/sites/51/2019/06/Measures-for-Security-Assessment-of-the-Cross-Border-Transfer-of-Personal-Information_bilingual.pdf, and New America, Translation: New Draft Rules on Cross-Border Transfer of Personal Information Out of China 'Personal Information Outbound Transfer Security Assessment Measures (Draft for Comment)," June 2019 https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-new-draft-rules-cross-border-transfer-personal-information-out-china/.

[28] Order of the State Council of the People's Republic of China No. 745, 30 July 2021, http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm?trs=1, as translated by DigiChina: https://digichina.stanford.edu/news/translation-critical-information-infrastructure-security-protection-regulations-effective-sept.

or other means related to identified or identifiable natural persons, not including information after anonymization handling. Personal information handling includes personal information collection, storage, use, processing, transmission, provision, publishing, deletion, etc.".[29] (Full text of the law is in Appendix 5 to this paper).

Conclusion

China is actively participating in all relevant cyber-related discussions at the U.N. The international and national contributions by China have the potential to touch on ICANN's mission. ICANN org, through its Government Engagement team, will continue to provide information to the ICANN community when such statements or proposals are relevant to the technical governance of the Internet or to ICANN's mission.

[29] Personal Information Protection Law of the People's Republic of China, (Passed at the 30th meeting of the Standing Committee of the 13th National People's Congress on August 20, 2021), http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

Appendix 1
Cybersecurity Law of the People's Republic of China[30]
Passed 6 November 2016. Effective 1 June 2017.

1. Table of Contents

Chapter I: General Provisions
Article 1: This Law is formulated in order to: ensure cybersecurity; safeguard cyberspace sovereignty and national security, and social and public interests; protect the lawful rights and interests of citizens, legal persons, and other organizations; and promote the healthy development of the informatization of the economy and society.
Article 2: This Law is applicable to the construction, operation, maintenance, and use of networks, as well as to cybersecurity supervision and management within the mainland territory of the People's Republic of China.
Article 3: The State persists in equally stressing cybersecurity and informatization development, and abides by the principles of active use, scientific development, management in accordance with law, and ensuring security. The State advances the construction of network infrastructure and interconnectivity, encourages the innovation and application of network technology, supports the cultivation of qualified cybersecurity personnel, establishes a complete system to safeguard cybersecurity, and raises capacity to protect cybersecurity.
Article 4: The State formulates and continuously improves cybersecurity strategy, clarifies the fundamental requirements and primary goals of ensuring cybersecurity, and puts forward cybersecurity policies, work tasks, and procedures for key sectors.
Article 5: The State takes measures for monitoring, preventing, and handling cybersecurity risks and threats arising both within and without the mainland territory of the People's Republic 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.
Article 6: The State advocates sincere, honest, healthy, and civilized online conduct; it promotes the dissemination of core socialist values, adopts measures to raise the entire society's awareness and level of cybersecurity, and formulates a good environment for the entire society to jointly participate in advancing cybersecurity.

[30] NewAmerica, Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017), 29 June 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/

Article 7: The State actively carries out international exchanges and cooperation in the areas of cyberspace governance, research and development of network technologies, formulation of standards, attacking cybercrime and illegality, and other such areas; it promotes constructing a peaceful, secure, open, and cooperative cyberspace, and establishing a multilateral, democratic, and transparent Internet governance system.
Article 8: State cybersecurity and informatization departments are responsible for comprehensively planning and coordinating cybersecurity efforts and related supervision and management efforts. The State Council departments for telecommunications, public security, and other relevant organs, are responsible for cybersecurity protection, supervision, and management efforts within the scope of their responsibilities, in accordance with the provisions of this Law and relevant laws and administrative regulations.
Cybersecurity protection, supervision, and management duties for relevant departments in people's governments at the county level or above will be determined by relevant national regulations.
Article 9: Network operators carrying out business and service activities must follow laws and administrative regulations, respect social morality, abide by commercial ethics, be honest and credible, perform obligations to protect cybersecurity, accept supervision from the government and public, and bear social responsibility.
Article 10: 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 with the mandatory requirements of national standards; adopting technical measures and other necessary measures to safeguard cybersecurity and operational stability; effectively responding to cybersecurity incidents; preventing cybercrimes and unlawful activity; and preserving the integrity, secrecy, and usability of online data.
Article 11: Relevant Internet industry organizations, according to their Articles of Association, shall strengthen industry self-discipline, formulate cybersecurity norms of behavior, guide their members in strengthening cybersecurity protection according to the law, raise the level of cybersecurity protection, and stimulate the healthy development of the industry.
Article 12: The State protects the rights of citizens, legal persons, and other organizations to use networks in accordance with the law; it promotes widespread network access, raises the level of network services, provides secure and convenient network services to society, and guarantees the lawful, orderly, and free circulation of network information.
Any person and organization using networks shall abide by the Constitution and laws, observe public order, and respect social morality; they must not endanger cybersecurity, and must not use the Internet to engage in activities endangering national security, national honor, and national interests; they must not incite subversion of national sovereignty, overturn the socialist system, incite separatism, break national unity, advocate terrorism or extremism, advocate ethnic hatred and ethnic discrimination, disseminate violent, obscene, or sexual information, create or disseminate false information to disrupt the economic or social order, or information that infringes on the reputation, privacy, intellectual property or other lawful rights and interests of others, and other such acts.
Article 13: The State encourages research and development of network products and services conducive to the healthy upbringing of minors; the State will lawfully punish the use of networks to engage in activities that endanger the psychological and physical well-being of minors; and the State will provide a safe and healthy network environment for minors.
Article 14: All individuals and organizations have the right to report conduct endangering cybersecurity to cybersecurity and informatization, telecommunications, public security, and other departments. Departments receiving reports shall promptly process them in accordance with law; where matters do not fall within the responsibilities of that department, they shall promptly transfer them to the department empowered to handle them.

Relevant departments shall preserve the confidentiality of the informants' information and protect the lawful rights and interests of informants.

Chapter II: The Support and Promotion of Cybersecurity

Article 15: The State establishes and improves a system of cybersecurity standards. State Council standardization administrative departments and other relevant State Council departments, on the basis of their individual responsibilities, shall organize the formulation and timely revision of relevant national and industry standards for cybersecurity management, as well as for the security of network products, services, and operations.

The State supports enterprises, research institutions, schools of higher learning, and network-related industry organizations to participate in the formulation of national and industry standards for cybersecurity.

Article 16: The State Council and people's governments of provinces, autonomous regions, and directly-governed municipalities shall: do comprehensive planning; expand investment; support key cybersecurity technology industries and programs; support cybersecurity technology research and development, application, and popularization; promote secure and trustworthy network products and services; protect intellectual property rights for network technologies; and support research and development institutions, schools of higher learning, etc., to participate in State cybersecurity technology innovation programs.

Article 17: The State advances the establishment of socialized service systems for cybersecurity, encouraging relevant enterprises and institutions to carry out cybersecurity certifications, testing, risk assessment, and other such security services.

Article 18: The State encourages the development of network data security protection and utilization technologies, advancing the opening of public data resources, and promoting technical innovation and economic and social development.

The State supports innovative methods of cybersecurity management, utilizing new network technologies to enhance the level of cybersecurity protection.

Article 19: All levels of people's governments and their relevant departments shall organize and carry out regular cybersecurity publicity and education, and guide and stimulate relevant units in properly carrying out cybersecurity publicity and education work.

The mass media shall conduct targeted cybersecurity publicity and education aimed at the public.

Article 20: The State supports enterprises and education or training institutions, such as schools of higher learning and vocational schools, in carrying out cybersecurity-related education and training, and it employs multiple methods to cultivate qualified personnel in cybersecurity and promote the interaction of cybersecurity professionals.

Chapter III: Network Operations Security

Section 1: Ordinary Provisions

Article 21: The State implements a cybersecurity multi-level protection system [MLPS]. Network operators shall perform the following security protection duties according to the requirements of the cybersecurity multi-level protection system to ensure the network is free from interference, damage, or unauthorized access, and to prevent network data leaks, theft, or falsification:

(1) Formulate internal security management systems and operating rules, determine persons who are responsible for cybersecurity, and implement cybersecurity protection responsibility;

(2) Adopt technical measures to prevent computer viruses, cyber attacks, network intrusions, and other actions endangering cybersecurity;

(3) Adopt technical measures for monitoring and recording network operational statuses and cybersecurity incidents, and follow provisions to store network logs for at least six months;

(4) Adopt measures such as data classification, backup of important data, and encryption;
(5) Other obligations provided by law or administrative regulations.

Article 22: Network products and services shall comply with the relevant national and mandatory requirements. Providers of network products and services must not install malicious programs; when discovering that their products and services have security flaws or vulnerabilities, they shall immediately adopt remedial measures, and follow provisions to promptly inform users and report to the competent departments.

Providers of network products and services shall provide security maintenance for their products and services, and they must not terminate the provision of security maintenance during the time limits or period agreed on with clients.

If a network product or service has the function of collecting user information, its provider shall clearly indicate this and obtain consent from the user; and if this involves a user's personal information, the provider shall also comply with the provisions of this law and relevant laws and administrative regulations on the protection of personal information.

Article 23: Critical network equipment and specialized cybersecurity products shall follow national standards and mandatory requirements, and be security certified by a qualified establishment or meet the requirements of a security inspection, before being sold or provided.

The state cybersecurity and informatization departments, together with the relevant departments of the State Council, will formulate and release a catalog of critical network equipment and specialized cybersecurity products, and promote reciprocal recognition of security certifications and security inspection results to avoid duplicative certifications and inspections.

Article 24: Network operators handling network access and domain name registration services for users, handling stationary or mobile phone network access, or providing users with information publication or instant messaging services, shall require users to provide real identity information when signing agreements with users or confirming the provision of services. Where users do not provide real identity information, network operators must not provide them with relevant services.

The State implements a network identity credibility strategy and supports research and development of secure and convenient electronic identity authentication technologies, promoting reciprocal acceptance among different electronic identity authentication methods.

Article 25: Network operators shall formulate emergency response plans for cybersecurity incidents and promptly address system vulnerabilities, computer viruses, cyber attacks, network intrusions, and other such cybersecurity risks. When cybersecurity incidents occur, network operators should immediately initiate an emergency response plan, adopt corresponding remedial measures, and report to the relevant competent departments in accordance with relevant provisions.

Article 26: Those carrying out cybersecurity certification, testing, risk assessment, or other such activities—or publicly publishing cybersecurity information such as system vulnerabilities, computer viruses, network attacks, or network incursions—shall comply with relevant national provisions.

Article 27: Individuals and organizations must not engage in illegal intrusion into the networks of other parties, disrupt the normal functioning of the networks of other parties, or steal network data or engage in other activities endangering cybersecurity; they must not provide programs, or tools specially used in network intrusions, that disrupt normal network functions and protection measures, steal network data, or engage in other acts endangering cybersecurity; and where they clearly are aware that others will engage in actions that endanger cybersecurity, they must not provide help such as technical support, advertisement and promotion, or payment of expenses.

Article 28: Network operators shall provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law.
Article 29: The State supports cooperation between network operators in areas such as the gathering, analysis, reporting, and emergency handling of cybersecurity information, increasing the security safeguarding capacity of network operators.
Relevant industrial organizations are to establish and complete mechanisms for standardization and coordination of cybersecurity for their industry, strengthen their analysis and assessment of cybersecurity, and periodically conduct risk warnings, support, and coordination for members in responding to cybersecurity risks.
Article 30: Information obtained by cybersecurity and informatization departments and relevant departments performing cybersecurity protection duties can only be used as necessary for the protection of cybersecurity, and must not be used in other ways.

Section 2: Operations Security for Critical Information Infrastructure
Article 31: The State implements key protection on the basis of the cybersecurity multi-level protection system for public communication and information services, power, traffic, water resources, finance, public service, e-government, and other critical information infrastructure which—if destroyed, suffering a loss of function, or experiencing leakage of data—might seriously endanger national security, national welfare, the people's livelihood, or the public interest. The State Council will formulate the specific scope and security protection measures for critical information infrastructure.
The State encourages operators of networks outside the [designated] critical information infrastructure systems to voluntarily participate in the critical information infrastructure protection system.
Article 32: In accordance with the duties and division of labor provided by the State Council, departments responsible for security protection work for critical information infrastructure are to separately compile and organize security implementation plans for their industry's or sector's critical information infrastructure, and to guide and supervise security protection efforts for critical information infrastructure operations.
Article 33: Those constructing critical information infrastructure shall ensure that it has the capability to support business stability and sustained operations, and ensure the synchronous planning, synchronous establishment, and synchronous application of security technical measures.
Article 34: In addition to the provisions of Article 21 of this Law, critical information infrastructure operators shall also perform the following security protection duties:
(1) Set up specialized security management bodies and persons responsible for security management, and conduct security background checks on those responsible persons and personnel in critical positions;
(2) Periodically conduct cybersecurity education, technical training, and skills evaluations for employees;
(3) Conduct disaster recovery backups of important systems and databases;
(4) Formulate emergency response plans for cybersecurity incidents, and periodically organize drills;
(5) Other duties provided by law or administrative regulations.
Article 35: Critical information infrastructure operators purchasing network products and services that might impact national security shall undergo a national security review organized by the State cybersecurity and informatization departments and relevant departments of the State Council.

Article 36: Critical information infrastructure operators purchasing network products and services shall follow relevant provisions and sign a security and confidentiality agreement with the provider, clarifying duties and responsibilities for security and confidentiality.
Article 37: Critical information infrastructure operators that gather or produce personal information or important data during operations within the mainland territory of the People's Republic of China, shall store it within mainland China. Where due to business requirements it is truly necessary to provide it outside the mainland, they shall follow the measures jointly formulated by the State cybersecurity and informatization departments and the relevant departments of the State Council to conduct a security assessment; where laws and administrative regulations provide otherwise, follow those provisions.
Article 38: At least once a year, critical information infrastructure operators shall conduct an inspection and assessment of their networks' security and risks that might exist, either on their own or through retaining a cybersecurity services organization; CII operators should submit a cybersecurity report on the circumstances of the inspection and assessment as well as improvement measures, to be sent to the relevant department responsible for critical information infrastructure security protection efforts.
Article 39: State cybersecurity and informatization departments shall coordinate relevant departments in employing the following measures for critical information infrastructure security protection:

(1) Conduct spot testing of critical information infrastructure security risks, put forward improvement measures, and when necessary they can retain a cybersecurity services organization to conduct testing and assessment of cybersecurity risks;

(2) Periodically organize critical information infrastructure operators to conduct emergency cybersecurity response drills, increasing the level, coordination, and capacity of responses to cybersecurity incidents.

(3) Promote cybersecurity information sharing among relevant departments, critical information infrastructure operators, and also relevant research institutions and cybersecurity services organizations.

(4) Provide technical support and assistance for cybersecurity emergency management and recovery, etc.

Chapter IV: Network Information Security

Article 40: Network operators shall strictly maintain the confidentiality of user information they collect, and establish and complete user information protection systems.
Article 41: Network operators collecting and using personal information shall abide by the principles of legality, propriety, and necessity; they shall publish rules for collection and use, explicitly stating the purposes, means, and scope for collecting or using information, and obtain the consent of the persons whose data is gathered.
Network operators must not gather personal information unrelated to the services they provide; must not violate the provisions of laws, administrative regulations or agreements between the parties to gather or use personal information; and shall follow the provisions of laws, administrative regulations, and agreements with users to process personal information they have stored.
Article 42: Network operators must not disclose, tamper with, or destroy personal information they gather; and, absent the consent of the person whose information was collected, must not provide personal information to others. However, this is the case with the exception that information can be provided if after processing there is no way to identify a specific individual, and the identity cannot be recovered.
Network operators shall adopt technical measures and other necessary measures to ensure the security of personal information they gather and to prevent personal information from leaking,

being destroyed, or lost. When the leak, destruction, or loss of personal information occurs, or might have occurred, remedial measures shall be immediately taken, and provisions followed to promptly inform users and to make a report to the competent departments in accordance with regulations.

Article 43: Where individuals discover that network operators have violated the provisions of laws, administrative regulations, or agreements between the parties to gather or use their personal information, they have the right to demand the network operators delete their personal information; where discovering that personal information gathered or stored by network operators has errors, they have the right to demand the network operators make corrections. Network operators shall employ measures for deletions and corrections.

Article 44: Individuals or organizations must not steal or use other illegal methods to acquire personal information, and must not unlawfully sell or unlawfully provide others with personal information.

Article 45: Departments lawfully having cybersecurity supervision and management duties, and their staffs, must keep strictly confidential personal information, private information, and commercial secrets that they learn of in performing their duties, and they must not leak, sell, or unlawfully provide it to others.

Article 46: All individuals and organizations shall be responsible for their use of websites and must not establish websites or communications groups for use in perpetrating fraud, imparting criminal methods, the creation or sale of prohibited or controlled items, or other unlawful activities, and websites must not be exploited to publish information related to perpetrating fraud, the creation or sale of prohibited or controlled items, or other unlawful activities.

Article 47: Network operators shall strengthen management of information published by users and, upon discovering information that the law or administrative regulations prohibits the publication or transmission of, they shall immediately stop transmission of that information, employ handling measures such as deleting the information, prevent the information from spreading, save relevant records, and report to the relevant competent departments.

Article 48: Electronic information sent, or application software provided by any individual or organization, must not install malicious programs, and must not contain information that laws and administrative regulations prohibit the publication or transmission of.

Electronic information distribution service providers, and application software download service providers, shall perform security management duties; where they know that their users have engaged in conduct provided for in the preceding paragraph, they shall: employ measures such as stopping provision of services and removal of information or malicious programs; store relevant records; and report to the relevant competent departments.

Article 49: Network operators shall establish network information security complaint and reporting systems, publicly disclose information such as the methods for making complaints or reports, and promptly accept and handle complaints and reports relevant to network information security.

Network operators shall cooperate with cybersecurity and informatization departments and relevant departments in conducting implementation of supervision and inspections in accordance with the law.

Article 50: State cybersecurity and informatization departments and relevant departments will perform network information security supervision and management responsibilities in accordance with law; and where they discover the publication or transmission of information which is prohibited by laws or administrative regulations, shall request that network operators stop transmission, employ disposition measures such as deletion, and store relevant records; for information described above that comes from outside the mainland People's Republic of China, they shall notify the relevant organization to adopt technical measures and other necessary measures to block transmission.

Chapter V: Monitoring, Early Warning, and Emergency Response

Article 51: The State will establish a cybersecurity monitoring, early warning, and information communication system. The State cybersecurity and informatization departments shall do overall coordination of relevant departments to strengthen collection, analysis, and reporting efforts for cybersecurity information, and follow regulations for the unified release of cybersecurity monitoring and early warning information.

Article 52: Departments responsible for critical information infrastructure security protection efforts shall establish and complete cybersecurity monitoring, early warning, and information reporting systems for their respective industry or sector, and report cybersecurity monitoring and early warning information in accordance with regulations.

Article 53: State cybersecurity and informatization departments will coordinate with relevant departments to establish and complete mechanisms for cybersecurity risk assessment and emergency response efforts, formulate cybersecurity incident emergency response plans, and periodically organize drills.

Departments responsible for critical information infrastructure security protection efforts shall formulate cybersecurity incident emergency response plans for their respective industry or sector, and periodically organize drills.

Cybersecurity incident emergency response plans shall rank cybersecurity incidents on the basis of factors such as the degree of damage after the incident occurs and the scope of impact, and provide corresponding emergency response handling measures.

Article 54: When the risk of cybersecurity incidents increases, the relevant departments of people's governments at the provincial level and above shall follow the scope of authority and procedures provided, and employ the following measures on the basis of the characteristics of the cybersecurity risk and the damage it might cause:

(1) Require that relevant departments, institutions, and personnel promptly gather and report relevant information, and strengthen monitoring of the occurrence of cybersecurity risks;

(2) Organize relevant departments, institutions, and specialist personnel to conduct analysis and assessment of information on the cybersecurity risk, and predict the likelihood of incident occurrence, the scope of impact, and the level of damage;

(3) Issue cybersecurity risk warnings to the public, and publish measures for avoiding or reducing damage.

Article 55: When a cybersecurity incident occurs, the cybersecurity incident emergency response plan shall be immediately initiated, an evaluation and assessment of the cybersecurity incident shall be conducted, network operators shall be requested to adopt technical and other necessary measures, potential security risks shall be removed, the threat shall be prevented from expanding, and warnings relevant to the public shall be promptly published.

Article 56: Where, while performing cybersecurity supervision and management duties, relevant departments of people's governments at the provincial level or above discover that networks have a relatively large security risk or the occurrence of a security incident, they may call in the legal representative or responsible party for the operator of that network to conduct interviews in accordance with the scope of authority and procedures provided. Network operators shall follow requirements to employ procedures, make corrections, and eliminate hidden dangers.

Article 57: Where sudden emergencies or production security accidents occur as a result of cybersecurity incidents, they shall be handled in accordance with the provisions the "Emergency Response Law of the People's Republic of China," the "Production Safety Law of the People's Republic of China," and other relevant laws and administrative regulations.

Article 58: To fulfill the need to protect national security and the social public order, and to respond to the requirements of major security incidents within the society, it is possible, as

stipulated or approved by the State Council, to take temporary measures regarding network communications in a specially designated region, such as limiting such communications.

Chapter VI: Legal Responsibility

Article 59: Where network operators do not perform cybersecurity protection duties provided for in Articles 21 and 25 of this Law, the competent departments will order corrections and give warnings; where corrections are refused or it leads to harm to cybersecurity or other such consequences, a fine of between RMB 10,000 and 100,000 shall be levied; and the directly responsible management personnel shall be fined between RMB 5,000 and 50,000.

Where critical information infrastructure operators do not perform cybersecurity protection duties as provided for in Articles 33, 34, 36, and 38 of this Law, the competent departments will order corrections and give warnings; where corrections are refused or it leads to harm to cybersecurity or other such consequences, a fine of between RMB 100,000 and 1,000,000 shall be levied; and the directly responsible management personnel shall be fined between RMB 10,000 and 100,000.

Article 60: Where Article 22 Paragraphs 1 or 2 or Article 48 Paragraph 1 of this Law are violated by any of the following conduct, the relevant competent departments shall order corrections and give warnings; where corrections are refused or it causes harm to cybersecurity or other consequences, a fine of between RMB 50,000 and 500,000 shall be levied; and the persons who are directly in charge shall be fined between RMB 10,000 and 100,000:

(1) Installing malicious programs;

(2) Failure to immediately take remedial measures for security flaws or vulnerabilities that exist in products or services, or not informing users and reporting to the competent departments in accordance with regulations;

(3) Unauthorized ending of the provision of security maintenance for their products or services.

Article 61: Network operators violating Article 24 Paragraph 1 of this Law in failing to require users to provide real identity information or providing relevant services to users who do not provide real identity information, are ordered to make corrections by the relevant competent department; where corrections are refused or the circumstances are serious, a fine of between RMB 50,000 and 500,000 shall be levied, and the relevant competent department may order a temporary suspension of operations, a suspension of business for corrections, closing down of websites, cancellation of relevant operations permits, or cancellation of business licenses; persons who are directly in charge and other directly responsible personnel shall be fined between RMB 10,000 and 100,000.

Article 62: Where Article 26 of this Law is violated in carrying out cybersecurity certifications, testing, or risk assessments, or publishing cybersecurity information such as system vulnerabilities, computer viruses, cyber attacks, or network incursions, corrections are to be ordered and a warning given; where corrections are refused or the circumstances are serious, a fine of between RMB 10,000 and 100,000 shall be imposed, and the relevant competent department may order a temporary suspension of operations, a suspension of business for corrections, closing down of websites, cancellation of relevant operations permits, or cancellation of business licenses; persons who are directly in charge and other directly responsible personnel shall be fined between RMB 5,000 and 50,000.

Article 63: Where Article 27 of this Law is violated in engaging in activities harming cybersecurity, or by providing specialized software or tools used in engaging in activities harming cybersecurity, or by providing others engaging in activities harming cybersecurity with assistance such as technical support, advertising and promotions, or payment of expenses, and where this does not constitute a crime, public security organizations shall confiscate unlawful gains and impose up to 5 days detention, and may levy a fine of between RMB 50,000 and

500,000; and where circumstances are serious, shall impose between 5 and 15 days detention, and may levy a fine of between 100,000 and 1,000,000 RMB.
Where units have engaged in the conduct of the preceding paragraph, public security organizations shall confiscate unlawful gains and levy a fine of between RMB 100,000 and 1,000,000, and the directly responsible persons in charge and other directly responsible personnel shall be fined in accordance with the preceding paragraph.
Where Article 27 of this Law is violated, persons who receive public security administrative sanctions must not engage in cybersecurity management or key network operations positions for 5 years; those receiving criminal punishments will be subject to a lifetime ban on engaging in work in cybersecurity management and key network operations positions.
Article 64: Network operators, and network product or service providers violating Article 22 Paragraph 3 or Articles 41-43 of this Law by infringing on personal information that is protected in accordance with law, shall be ordered to make corrections by the relevant competent department and may, either independently or concurrently, be given warnings, be subject to confiscation of unlawful gains, and/or be fined between 1 to 10 times the amount of unlawful gains; where there are no unlawful gains, the fine shall be up to RMB 1,000,000, and a fine of between RMB 10,000 and 100,000 shall be given to persons who are directly in charge and other directly responsible personnel; where the circumstances are serious, the relevant competent department may order a temporary suspension of operations, a suspension of business for corrections, closing down of websites, cancellation of relevant operations permits, or cancellation of business licenses.
Where Article 44 of this Law is violated in stealing or using other illegal means to obtain, illegally sell, or illegally provide others with personal information, and this does not constitute a crime, public security organizations shall confiscate unlawful gains and levy a fine of between 1 and 10 times the amount of unlawful gains, and where there are no unlawful gains, levy a fine of up to RMB 1,000,000.
Article 65: Where critical information infrastructure operators violate Article 35 of this Law by using network products or services that have not had security inspections or did not pass security inspections, the relevant competent department shall order the usage to stop and levy a fine in the amount of 1 to 10 times the purchase price; the persons who are directly in charge and other directly responsible personnel shall be fined between RMB 10,000 and 100,000.
Article 66: Where critical information infrastructure operators violate Article 37 of this Law by storing network data outside the mainland territory, or provide network data to those outside of the mainland territory, the relevant competent department: shall order corrective measures, provide warning, confiscate unlawful gains, and levy fines between RMB 50,000 and 500,000; and may order a temporary suspension of operations, a suspension of business for corrective measures, closing down of websites, revocation of relevant operations permits, or cancellation of business licenses. Persons who are directly in charge and other directly responsible personnel shall be fined between RMB 10,000 and 100,000.
Article 67: Where Article 46 of this Law is violated by establishing a website or communications group used for the commission of illegal or criminal activities, or the network is used to publish information related to the commission of illegal or criminal activities, but a crime has not been committed, public security organizations shall impose up to 5 days detention and may levy a fine of between RMB 10,000 and 15,000; and where circumstances are serious, they may impose between 5 and 15 days detention, and may give a fine of between 50,000 and 500,000 RMB. They may also close websites and communications groups used for illegal or criminal activities.
Where units have engaged in conduct covered by the preceding paragraph, a fine of between RMB 100,000 and 500,000 shall be levied by public security organizations, and the principal

responsible managers and other directly responsible personnel shall be fined in accordance with the preceding paragraph.

Article 68: Where network operators violate Article 47 of this Law by failing to stop the transmission of information for which transmission and publication are prohibited by laws or administrative regulations, failing to employ disposition measures such as deletion or failing to preserve relevant records, the relevant competent department shall order correction, provide warning, and confiscate unlawful gains; where correction is refused or circumstances are serious, fines between RMB 100,000 and 500,000 shall be imposed, and a temporary suspension of operations, a suspension of business to conduct correction, closing down of websites, cancellation of relevant operations permits, or cancellation of business licenses may be ordered; and persons who are directly in charge and other directly responsible personnel are fined between RMB 10,000 and 100,000.

Where electronic information service providers and application software download service providers do not perform their security management duties provided for in Paragraph 2 of Article 48 of this Law, punishment shall be in accordance with the provisions of the preceding paragraph.

Article 69: Network operators violating the provisions of this Law, who exhibit any of the following conduct, will be ordered to make corrections by the relevant competent departments; where corrections are refused or the circumstances are serious, a fine of between RMB 50,000 and 500,000 shall be imposed, and directly responsible management personnel and other directly responsible personnel are to be fined between RMB 10,000 and 100,000:

(1) Not following the requirements of relevant departments to adopt disposition measures such as stopping dissemination or deleting information for which laws or administrative regulations prohibit publication or dissemination;

(2) Refusal or obstruction of the competent departments in their lawful supervision and inspection;

(3) Refusing to provide technical support and assistance to public security organs and state security organs.

Article 70: Publication or transmission of information prohibited by Article 12 Paragraph 2 of this Law or other laws or administrative regulations shall be punished in accordance with the provisions of the relevant laws and administrative regulations.

Article 71: When there is conduct violating the provisions of this Law, it shall be recorded in credit files and made public in accordance with relevant laws and administrative regulations.

Article 72: Where state organization government affairs network operators do not perform cybersecurity protection duties as provided by this Law, the organization at the level above or relevant organizations will order corrections; sanctions will be levied on the directly responsible managers and other directly responsible personnel.

Article 73: Where cybersecurity and informatization and other relevant departments violate the provisions of Article 30 of this Law by using personal information acquired while performing cybersecurity protection duties for other purposes, the directly responsible persons in charge and other directly responsible personnel shall be given sanctions.

Where cybersecurity and informatization departments and other relevant departments' personnel neglect their duties, abuse their authority, show favoritism, and it does not constitute a crime, sanctions will be imposed in accordance with law.

Article 74: Where violations of the provisions of this Law cause harm to others, civil liability is borne in accordance with law.

Where provisions of this Law are violated, constituting a violation of public order management, public order administrative sanctions will be imposed in accordance with law; where a crime is constituted, criminal responsibility will be pursued in accordance with law.

Article 75: Where foreign institutions, organizations, or individuals engage in attacks, intrusions, interference, damage, or other activities the endanger the critical information infrastructure of the People's Republic of China, and cause serious consequences, legal responsibility is to be pursued in accordance with the law; public security departments under the State Council and relevant departments may also decide to freeze institutional, organization, or individual assets or take other necessary punitive measures.

Chapter VII: Supplementary Provisions

Article 76: The language below has the following meanings in this law:

(1) "Network" [网络, also "cyber"] refers to a system comprised of computers or other information terminals and related equipment that follows certain rules and procedures for information gathering, storage, transmission, exchange, and processing.

(2) "Cybersecurity" [网络安全, also "network security"] refers to taking the necessary measures to prevent cyber attacks, intrusions, interference, destruction, and unlawful use, as well as unexpected accidents, to place networks in a state of stable and reliable operation, as well as ensuring the capacity for network data to be complete, confidential, and usable.

(3) "Network operators" [网络运营者] refers to network owners, managers, and network service providers.

(4) "Network data" [网络数据] refers to all kinds of electronic data collected, stored, transmitted, processed, and produced through networks.

(5) "Personal information" [个人信息] refers to all kinds of information, recorded electronically or through other means, that taken alone or together with other information, is sufficient to identify a natural person's identity, including but not limited to natural persons' full names, birth dates, national identification numbers, personal biometric information, addresses, telephone numbers, and so forth.

Article 77: Protection of the operational security of networks that store or process information touching on national secrets shall follow this Law and shall also uphold the provisions of laws and administrative regulations pertaining to secrecy protection.

Article 78: The security protection rules for military networks are formulated by the Central Military Commission.

Article 79: This Law shall enter into effect June 1, 2017.

Appendix 2
Chinese Ministry of Industry and Information Technology Internet Domain Name Management Measures[31] (Excerpts).

Article 3 of the measures appointed by the Ministry of Industry and Information Technology to carry out "supervision and management over domain name services nationwide, its main tasks are: (1) formulating Internet domain name management rules and policies; (2) formulating an internet domain name system, and plan for developing domain name resources; (3) managing domestic domain name root server-running bodies and domain name registration and management bodies; (4) being responsible for the network and information security management of the domain name system; (5) protecting users' personal information and lawful rights and interests according to the law; (6) being responsible for international coordination concerning domain names; (7) managing domestic domain name resolution services; (8) managing other activities concerning domain name services."
Article 10 of the measures provided that "those applying to establish a domain name root server or domain name root-server-running body, shall meet the following conditions: (1) the domain name root server is to be set up within the borders, and shall conform to corresponding Internet development plans and the requirements of the safe and stable operation of the domain name system."
Article 11: Those applying to establish a domain name registration and management body shall meet the following conditions:
(1) the top-level domain name management system is to be set up within the borders, and the top-level domain names they hold are to conform to relevant laws and regulations as well as the requirements of the safe and stable operation of the domain name system;
(2) [they shall] be legal persons lawfully established within the borders, the said legal person and their main investors, main operational and management personnel are to have good credit records;
(3) having perfect professional development plans and technological plans, as well as premises, finance and specialist personnel suited to engaging in top-level domain name operations and management, as well as information management systems conforming to telecommunications management body requirements;
(4) having complete network and information security management measures, including management personnel, network and information security management structures, emergency response processing plans and corresponding technological and management measures;
(5) having the capability to engage in real identity information verification and users' personal information protection, the capability to provide long-term services as well as complete service withdrawal processing mechanisms;
(6) having complete domain name registration service management structures and supervision mechanisms for domain name registration service bodies;
(7) other requirements provided for by laws and administrative regulations.
Article 12: Those applying to establish a domain name registration service body, shall meet the following conditions:
(1) the domain name registration service system, registration database and resolution systems

[31] Ministry of Industry and Information Technology, Internet Domain Name Management Measures, 24 August 2017 https://www.chinalawtranslate.com/en/internet-domain-name-management-measures/ (unofficial translation)

are to be set up within the borders;
(2) [they shall] be legal persons lawfully established within the borders, the said legal person and their main investors, main operational and management personnel are to have good credit records;
(3) having premises, finance and specialist personnel suited to engaging in domain name registration services, as well as information management systems conform to telecommunications management body requirements;
(4) having the capability to engage in real identity information verification and users' personal information protection, the capability to provide long-term services and complete service withdrawal mechanism;
(5) having complete domain name registration service management structures and supervision mechanisms for domain name registration agency bodies;
(6) having complete network and information security protection measures, including management personnel, network and information security management structures, emergency response processing plans and corresponding technological and management measures.
(7) other requirements provided for by laws and administrative regulations.
Article 13: Those applying to establish a domain name root server and root server-running body, or domain name registration management body shall submit application materials to the Ministry of Industry and Information Technology. Those applying to establish a domain name registration service body shall submit application materials to the local provincial, autonomous region or municipal telecommunications management department.
The application materials shall include:
(1) the basic circumstances of the applying work unit
(2) certification materials for the effective management of domain name services, including certification materials for relevant systems and premises, as well as service capabilities, management structures as well as agreements concluded with other bodies;
(3) network and information security protection structures and measures;
(4) materials certifying the reputation of the applying work unit;
(5) a letter of commitment, signed by the legally-designated representative, to do business sincerely and according to the law."
Article 37: "In the provision of domain name resolution services, resolution information may not be distorted without authorization. Domain name resolution must not be maliciously redirected towards other persons' IP addresses by any organization or individual".
Article 41 of the measures states that **"**When necessary due to national security or to deal with emergency incidents, domain name root server-running bodies, domain name registration management bodies and domain name registration service bodies shall obey the unified command and coordination of telecommunications management bodies, and respect the management requirements of telecommunications management bodies".
Article 46: "Telecommunications management bodies shall establish credit record structures for domain name root server-running bodies, domain name registration management bodies and domain name registration service bodies, and shall enter their violations of these Measures, as well as the administrative punishment they receive, into the credit file".

Appendix 3
Chinese Internet Domain Name System[32] (Excerpts)

I. All levels of Internet domain name in our nation may be comprised of letters (A-Z, a-z, with capital and lowercase letters being equivalent), numbers (0-9), dashed (-), or Chinese characters; and all domains are to use dot (.) as connectors, and all levels of Chinese language domain names are to use either dots or Chinese period (。) as connectors.

II. In addition to the ".CN" and ".中国" top-level domains, our nation's Internet domain name system establishes multiple English and Chinese language top-level domains, of these, the top-level domains "政务" [.gov] and ".公益" [.org - literally public interest] are to be specialized Chinese language top-level domains for the nation's Party and Government groups and organs and all level levels of other government affairs department, and for non-profit institutions. Our nation's' Internet domain system diagram can be found at http://中国互联网域名体系.中国 ""http://中国互联网域名体系.政务"or "http://中国互联网域名体系.信息".

III. Under the national top-level domain ".CN", two types of second-level domains are established, 'category domains' and 'administrative region domains'. Nine 'category domains' are established, namely: ".政务" used for Party and government groups and organs at all levels of party and other government affairs departments; ".公益" used for non-profit organizations; ".GOV" used for government bodies; ".ORG" used for non for-profit organizations; ".AC" used for scientific research institutions; ".COM" used for industrial, commercial, financial, and other enterprises; ".EDU" used for educational bodies; ".MIL" used for national defense institutions; and ".NET" used for institutions providing Internet services.
Thirty-four "administrative region domains are established, to be used for each of the nation's provinces, autonomous regions, directly-governed municipalities, and special administrative region organizations [...].

IV. Applications may be made to directly register second-level domain names under the ".CN" and ".中国" national top-level domains.

[32] China Law Translate, Chinese Internet Domain Name System, 5 March 2018 https://www.chinalawtranslate.com/en/chinese-internet-domain-name-system/ (unofficial translation)

Appendix 4
Data Security Law of the People's Republic of China (DSL)[33] (Excerpts)

Article 3: "Data" as used in this Law refers to any record of information in electronic or other forms.
- Data handling includes the collection, storage, use, processing, transmission, provision, disclosure, etc., of data.
- Data security refers to employing necessary measures to ensure that data is effectively protected and legally used, as well as having the capacity to ensure a sustained state of security.

Article 7: The State is to protect the rights and interests of individuals and organizations with regards to data; encourage the lawful, reasonable, and effective use of data; ensure the lawful and orderly free flow of data; and promote the development of a digital economy with data as a key factor.

Article 11: The State is to actively carry out international exchanges and cooperation in the sectors of data security governance and data development and use, participate in the formulation of international rules and standards related to data security, and promote the safe and free flow of data across borders.

Article 14: The State is to implement a big data strategy, advancing the establishment of data infrastructure, and encouraging and supporting innovative applications of data in each industry and field.

Article 17: The State is to advance the establishment of a system of standards for data development and exploitation technologies and data security. Within the scope of their respective duties, the State Council departments in charge of standardization and other relevant State Council departments are to organize the formulation and appropriate revision of standards related to technology and products for the development and use of data and to data security. The state is to support enterprises and social groups, educational or research bodies, and so forth, participating in drafting standards.

Article 21: Data related to national security, the lifeblood of the national economy, important people's livelihood, major public interests and others belong to the national core data, shall apply to a more stringent management system.

Article 25: The state is to implement export controls in accordance with the law for data that are controlled items, related to preserving national security and performing international obligations.

Article 26: Where any nation or region employs discriminatory, restrictive, or other similar measures against the PRC in areas such as investment or trade in data and technology for the exploitation and development of data, the PRC may employ equal measures against that nation or region based on the actual circumstances.

Article 27: The carrying out of data handling activities through information networks, i.e., the Internet, shall fulfill the duties to protect data security on the basis of the multi-level protection system for cybersecurity.

Article 31: The provisions of the Cybersecurity Law of the PRC apply to the security management for exporting of data from the [mainland] territory that was collected or produced by critical information infrastructure operators inside the [mainland] territory of the PRC; security

[33] Data Security Law of the People's Republic of China, 11 June 2021, as translated here: https://www.secrss.com/articles/31844 (Unofficial translation, the original publication is here: http://www.cac.gov.cn/2021-06/11/c_1624994566919140.htm)

management measures for the export of important data from the mainland territory that was collected or produced by other data handlers within the [mainland] territory of the PRC are to be drafted by the State internet information department in conjunction with the relevant departments of the State Council.

Article 32: Any organization or individual collecting data shall employ lawful and appropriate methods and must not steal or obtain data through other, illegal methods. Where laws and administrative regulations have provisions on the purpose or scope of data collection and use, data is to be collected or used within the purpose and scope provided for in those laws and administrative regulations.

Article 33: When institutions engaged in data transaction intermediary services provide services, they shall require the party providing data to explain the sources of the data, verify the identities of both parties to the transaction, and store a record of the review and transaction.

Article 36: The competent PRC State organs shall, under the provisions of laws and treaties or agreements concluded or participated in by the PRC, or under the principle of equality and mutual benefits, handle the request of providing data by foreign judicial or law enforcement agency. Without the approval of the competent PRC State organs, organizations or individuals within the [mainland] territory of the PRC shall not provide data within the [mainland] PRC to foreign judicial or law enforcement agency.

Article 38: State organs' performance of legally-prescribed duties that require the collection and use of data shall be within the scope of the legally-prescribed duties and proceed in accordance with the requirements and procedures of laws and administrative regulations; in the performance of duties to know personal privacy, personal information, trade secrets, confidential business information and other data shall be kept confidential in accordance with the law, and shall not be disclosed or illegally provided to others.

Article 40: State organs entrusting others to establish or maintain electronic government affairs systems or to store or process government affairs data, shall go through strict approval procedures and shall oversee the performance of corresponding data security protection obligations by the entrusted parties. The entrusted party shall perform data security protection obligations in accordance with the provisions of laws and regulations and contractual agreements, and shall not retain, use, disclose or provide government affairs data to others without authorization.

Article 44: Where relevant regulatory departments performing data security oversight and management duties discover that data handling activities have larger security risks, they may give the relevant organizations and individuals a talking and require to employ procedures, make corrections, and eliminate hidden dangers in accordance with the authority and procedures provided.

Article 49: Where State organs do not perform obligations to protect data security as provided for in this Law, the directly responsible managers and other directly responsible personnel are to be given sanctions in accordance with law.

Article 52: Where violations of the provisions of this law cause harm to others, civil liability is borne in accordance with law.

Appendix 5
Personal Information Protection Law of the People's Republic of China[34]

(Passed at the 30th meeting of the Standing Committee of the 13th National People's Congress on August 20, 2021)

Chapter I: General Provisions

Article 1: This Law is formulated, on the basis of the Constitution, in order to protect personal information rights and interests, standardize personal information handling activities, and promote the rational use of personal information.

Article 2: The personal information of natural persons receives legal protection; no organization or individual may infringe upon natural persons' personal information rights and interests.

Article 3: This Law applies to the activities of handling the personal information of natural persons within the borders of the People's Republic of China.

Where one of the following circumstances is present in handling activities outside the borders of the People's Republic of China of personal information of natural persons within the borders of the People's Republic of China, this Law applies as well:

1. Where the purpose is to provide products or services to natural persons inside the borders;
2. Where analyzing or assessing activities of natural persons inside the borders;
3. Other circumstances provided in laws or administrative regulations.

Article 4: Personal information is all kinds of information, recorded by electronic or other means, related to identified or identifiable natural persons, not including information after anonymization handling.

Personal information handling includes personal information collection, storage, use, processing, transmission, provision, disclosure, deletion, etc.

Article 5: The principles of legality, propriety, necessity, and sincerity shall be observed for personal information handling. It is prohibited to handle personal information in misleading, swindling, coercive, or other such ways.

[34] Personal Information Protection Law of the People's Republic of China, (Passed at the 30th meeting of the Standing Committee of the 13th National People's Congress on August 20, 2021), http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml, as translated by DigiChina here: https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-effective-nov-1-2021

Article 6: Personal information handling shall have a clear and reasonable purpose, and shall be directly related to the handling purpose, using a method with the smallest influence on individual rights and interests.
The collection of personal information shall be limited to the smallest scope for realizing the handling purpose, and excessive personal information collection is prohibited.
Article 7: The principles of openness and transparency shall be observed in the handling of personal information, disclosing the rules for handling personal information and clearly indicating the purpose, method, and scope of handling.
Article 8: The handling of personal information shall ensure the quality of personal information, and avoid adverse effects on individual rights and interests from inaccurate or incomplete personal information.
Article 9: Personal information handlers shall bear responsibility for their personal information handling activities, and adopt the necessary measures to safeguard the security of the personal information they handle.
Article 10: No organization or individual may illegally collect, use, process, or transmit other persons' personal information, or illegally sell, buy, provide, or disclose other persons' personal information, or engage in personal information handling activities harming national security or the public interest.
Article 11: The State establishes a personal information protection structure, to prevent and punish acts harming personal information rights and interests, strengthen personal information protection propaganda and education, and promote the creation of a good environment for personal information protection, with joint participation from government, enterprise, relevant social organizations, and the general public.
Article 12: The State vigorously participates in the formulation of international rules [or norms] for personal information protection, stimulates international exchange and cooperation in the area of personal information protection, and promotes mutual recognition of personal information protection rules [or norms], standards, etc., with other countries, regions, and international organizations.

Chapter II: Personal Information Handling Rules

Section 1: Ordinary Provisions

Article 13: Personal information handlers may only handle personal information where they conform to one of the following circumstances:

1. Obtaining individuals' consent;
2. Where necessary to conclude or fulfill a contract in which the individual is an interested party, or where necessary to conduct human resources management according to lawfully formulated labor rules and structures and lawfully concluded collective contracts;
3. Where necessary to fulfill statutory duties and responsibilities or statutory obligations;
4. Where necessary to respond to sudden public health incidents or protect natural persons' lives and health, or the security of their property, under emergency conditions;
5. Handling personal information within a reasonable scope to implement news reporting, public opinion supervision, and other such activities for the public interest;
6. When handling personal information disclosed by persons themselves or otherwise already lawfully disclosed, within a reasonable scope in accordance with the provisions of this Law.
7. Other circumstances provided in laws and administrative regulations.

In accordance with other relevant provisions of this Law, when handling personal information, individual consent shall be obtained. However, obtaining individual consent is not required under conditions in items 2 through 7 above.

Article 14: Where personal information is handled based on individual consent, said consent shall be given by individuals under the precondition of full knowledge, and in a voluntary and explicit statement. Where laws or administrative regulations provide that separate consent or written consent shall be obtained to handle personal information, those provisions are to be followed.

Where a change occurs in the purpose of personal information handling, the handling method, or the categories of handled personal information, the individual's consent shall be obtained again.

Article 15: Where personal information is handled based on individual consent, individuals have the right to rescind their consent. Personal information handlers shall provide a convenient way to withdraw consent.

If an individual rescinds consent, it does not affect the effectiveness of personal information handling activities undertaken on the basis of individual consent before consent was rescinded.

Article 16: Personal information handlers may not refuse to provide products or services on the basis that an individual does not consent to the handling of their personal information or rescinds their consent, except where handling personal information is necessary for the provision of products or services.

Article 17: Personal information handlers shall, before handling personal information, explicitly notify individuals truthfully, accurately, and fully of the following items using clear and easily understood language:

1. The name or personal name and contact method of the personal information handler;
2. The purpose of personal information handling and the handling methods, the categories of handled personal information, and the retention period;
3. Methods and procedures for individuals to exercise the rights provided in this Law;
4. Other items that laws or administrative regulations provide shall be notified.

Where a change occurs in the matters provided in the previous paragraph, individuals shall be notified about the change.

Where personal information handlers notify the matters as provided in Paragraph 1 through the method of formulating personal information handling rules, the handling rules shall be made public [disclosed] and convenient to read and store.

Article 18: Personal information handlers handling personal information are permitted not to notify individuals about the items provided in Paragraph 1 of the previous Article under circumstances where laws or administrative regulations provide that confidentiality shall be preserved or notification is not necessary.

Under emergency circumstances, where it is impossible to notify individuals in a timely manner in order to protect natural persons' lives, health, and the security of their property, personal information handlers shall notify them after the conclusion of the emergency circumstances.

Article 19: Except where laws or administrative regulations provide otherwise, personal information retention periods shall be the shortest period necessary to realize the purpose of the personal information handling.

Article 20: Where two or more personal information handlers jointly decide on a personal information handling purpose and handling method, they shall agree on the rights and obligations of each. However, said agreement does not influence an individual's rights to demand any one personal information handler perform under this Law's provisions.

Where personal information handlers jointly handling personal information harm personal information rights and interests, resulting in damages, they bear joint liability according to the law.

Article 21: Where personal information handlers entrust the handling of personal information, they shall conclude an agreement with the entrusted person on the purpose for entrusted handling, the time limit, the handling method, categories of personal information, protection

measures, as well as the rights and duties of both sides, etc., and conduct supervision of the personal information handling activities of the entrusted person.
Entrusted persons shall handle personal information according to the agreement; they may not handle personal information for handling purposes or in handling methods, etc., in excess of the agreement. If the entrusting contract does not take effect, is void, has been cancelled, or has been terminated, the entrusted person shall return the personal information to the personal information handler or delete it, and may not retain it.
Without the consent of the personal information handler, an entrusted person may not further entrust personal information handling to other persons.
Article 22: Personal information handlers shall, where it is necessary to transfer personal information due to mergers, separations, dissolution, declaration of bankruptcy, and other such reasons, notify individuals about the receiving party's name or personal name and contact method. The receiving party shall continue to fulfill the personal information handler's duties. Where the receiving side changes the original handling purpose or handling method, they shall notify the individual again as provided in this Law.
Article 23: Where personal information handlers provide other personal information handlers with the personal information they handle, they shall notify individuals about the name or personal name of the recipient, their contact method, the handling purpose, handling method, and personal information categories, and obtain separate consent from the individual.
Recipients shall handle personal information within the above mentioned scope of handling purposes, handling methods, personal information categories, etc. Where recipients change the original handling purpose or handling methods, they shall again obtain the individual's consent.
Article 24: When personal information handlers use personal information to conduct automated decision-making, the transparency of the decision-making and the fairness and justice of the handling result shall be guaranteed, and they may not engage in unreasonable differential treatment of individuals in trading conditions such as trade price, etc.
Those conducting information push delivery or commercial sales to individuals through automated decision-making methods shall simultaneously provide the option to not target an individual's characteristics, or provide the individual with a convenient method to refuse.
When the use of automated decision-making produces decisions with a major influence on the rights and interests of the individual, they have the right to require personal information handlers to explain the matter, and they have the right to refuse that personal information handlers make decisions solely through automated decision-making methods.
Article 25: Personal information handlers may not disclose the personal information they handle; except where they obtain separate consent.
Article 26: The installation of image collection or personal identity recognition equipment in public venues shall occur as required to safeguard public security and observe relevant State regulations, and clear indicating signs shall be installed. Collected personal images and personal distinguishing identity characteristic information can only be used for the purpose of safeguarding public security; it may not be used for other purposes, except where individuals' separate consent is obtained.
Article 27: Personal information handlers may, within a reasonable scope, handle personal information that has already been disclosed by the person themselves or otherwise lawfully disclosed, except where the person clearly refuses. Personal information handlers handling already disclosed personal information, where there is a major influence on individual rights and interests, shall obtain personal consent in accordance with the provisions of this Law.

Section II: Rules for Handling Sensitive Personal Information

Article 28: Sensitive personal information means personal information that, once leaked or illegally used, may easily cause harm to the dignity of natural persons grave harm to personal or property security, including information on biometric characteristics, religious beliefs, specially-designated status, medical health, financial accounts, individual location tracking, etc., as well as the personal information of minors under the age of 14.
Only where there is a specific purpose and a need to fulfill, and under circumstances of strict protection measures, may personal information handlers handle sensitive personal information.
Article 29: To handle sensitive personal information, the individual's separate consent shall be obtained. Where laws or administrative regulations provide that written consent shall be obtained for handling sensitive personal information, those provisions are to be followed.
Article 30: Personal information handlers handling sensitive personal information, in addition to the items set out in Article 17, Paragraph 1, of this Law, shall also notify individuals of the necessity and influence on the individual's rights and interests of handling the sensitive personal information, except where this Law provides that it is permitted not to notify the individuals.
Article 31: Where personal information handlers handle the personal information of minors under the age of 14, they shall obtain the consent of the parent or other guardian of the minor. Where personal information handlers handle the personal information of minors under the age of 14, they shall formulate specialized personal information handling rules.
Article 32: Where laws or administrative regulations provide that relevant administrative licenses shall be obtained or other restrictions apply to the handling of sensitive personal information, those provisions are to be followed.

Section III: Specific Provisions on State Organs Handling Personal Information

Article 33: This Law applies to State organs' activities of handling personal information; where this Section contains specific provisions, the provisions of this Section apply.
Article 34: State organs handling personal information to fulfill their statutory duties and responsibilities shall conduct them according to the powers and procedures provided in laws or administrative regulations; they may not exceed the scope or extent necessary to fulfill their statutory duties and responsibilities.
Article 35: State organs handling personal information for the purpose of fulfilling statutory duties and responsibilities shall fulfill notification duties, except where circumstances as provided in Article 18, Paragraph I, of this Law exist, or where notification will impede State organs' fulfillment of their statutory duties and responsibilities.
Article 36: Personal information handled by State organs shall be stored within the mainland territory of the People's Republic of China. If it is truly necessary to provide it abroad, a security assessment shall be undertaken. Relevant authorities may be requested to support and assist with security assessment.
Article 37: The provisions of this Law regarding personal information handling by State organs apply to the handling of personal information in order to fulfill statutory duties by organizations authorized by laws and regulations to manage public affairs functions.

Chapter III: Rules on the Cross-Border Provision of Personal Information

Article 38: Where personal information handlers truly need to provide personal information outside the borders of the People's Republic of China for business or other such requirements, they shall meet one of the following conditions:

1. Passing a security assessment organized by the State cybersecurity and informatization department according to Article 40 of this Law;
2. Undergoing personal information protection certification conducted by a specialized body according to provisions by the State cybersecurity and informatization department;

3. Concluding a contract with the foreign receiving side in accordance with a standard contract formulated by the State cyberspace and informatization department, agreeing upon the rights and responsibilities of both sides;
4. Other conditions provided in laws or administrative regulations or by the State cybersecurity and informatization department.

Where treaties or international agreements that the People's Republic of China has concluded or acceded to contain relevant provisions such as conditions on providing personal data outside the borders of the People's Republic of China, those provisions may be carried out.
Personal information handlers shall adopt necessary measures to ensure that foreign receiving parties' personal information handling activities reach the standard of personal information protection provided in this Law.
Article 39: Where personal information handlers provide personal information outside of the borders of the People's Republic of China, they shall notify the individual about the foreign receiving side's name or personal name, contact method, handling purpose, handling methods, and personal information categories, as well as ways or procedures for individuals to exercise the rights provided in this Law with the foreign receiving side, and other such matters, and obtain individuals' separate consent.
Article 40: Critical information infrastructure operators and personal information handlers handling personal information reaching quantities provided by the State cybersecurity and informatization department shall store personal information collected and produced within the borders of the People's Republic of China domestically. Where they need to provide it abroad, they shall pass a security assessment organized by the State cybersecurity and informatization department; where laws or administrative regulations and State cybersecurity and informatization department provisions permit that security assessment not be conducted, those provisions are to be followed.
Article 41: Competent authorities of the People's Republic of China, according to relevant laws and treaties or international agreements that the People's Republic of China has concluded or acceded to, or according to the principle of equality and mutual benefit, are to handle foreign judicial or law enforcement authorities' requests regarding the provision of personal information stored domestically. Without the approval of the competent authorities of the People's Republic of China, personal information handlers may not provide personal information stored within the mainland territory of the People's Republic of China to foreign judicial or law enforcement agencies.
Article 42: Where foreign organizations or individuals engage in personal information handling acts violating personal information rights and interests of citizens of the People's Republic of China, or harming the national security or public interest of the People's Republic of China, the State cybersecurity and informatization department may put them on a list limiting or prohibiting personal information provision, issue a warning, and adopt measures such as limiting or prohibiting the provision of personal information to them, etc.
Article 43: Where any country or region adopts discriminatory prohibitions, limitations or other similar measures against the People's Republic of China in the area of personal information protection, the People's Republic of China may adopt reciprocal measures against said country or region on the basis of actual circumstances.

Chapter IV: Individuals' Rights in Personal Information Handling Activities

Article 44: Individuals have the right to know and the right to decide relating to their personal information, and have the right to limit or refuse the handling of their personal information by others, unless laws or administrative regulations stipulate otherwise.

Article 45: Individuals have the right to consult and copy their personal information from personal information handlers, except in circumstances provided in Article 18, Paragraph 1, or Article 35 of this Law.
Where individuals request to consult or copy their personal information, personal information handlers shall provide it in a timely manner.
Where individuals request that their personal information be transferred to a personal information handler they designate, meeting conditions of the State cybersecurity and informatization department, personal information handlers shall provide a channel to transfer it.
Article 46: Where individuals discover their personal information is incorrect or incomplete, they have the right to request personal information handlers correct or complete their personal information. Where individuals request to correct or complete their personal information, personal information handlers shall verify the personal information and correct or complete it in a timely manner.
Where individuals request to correct or supplement their personal information, personal information handlers shall verify the personal information and correct or supplement it in a timely manner.
Article 47: Personal information handlers shall proactively delete personal information where one of the following circumstances occurs; if the personal information handler has not deleted it, individuals have the right to request deletion:

1. The handling purpose has been achieved, is impossible to achieve, or [the personal information] is no longer necessary to achieve the handling purpose;
2. Personal information handlers cease the provision of products or services, or the retention period has expired;
3. The individual rescinds consent;
4. Personal information handlers handled personal information in violation of laws, administrative regulations, or agreements;
5. Other circumstances provided by laws or administrative regulations.

Where the retention period provided by laws or administrative regulations has not expired, or personal information deletion is technically hard to realize, personal information handlers shall cease personal information handling except for storage and taking necessary security protective measures.
Article 48: Individuals have the right to request personal information handlers explain personal information handling rules.
Article 49: When a natural person is deceased, their next of kin may, for the sake of their own lawful, legitimate interests, exercise the rights provided in this Chapter to consult, copy, correct, delete, etc., the personal information of the deceased, except where the deceased has arranged otherwise before their death.
Article 50: Personal information handlers shall establish convenient mechanisms to accept and handle applications from individuals to exercise their rights. Where they reject individuals' requests to exercise their rights, they shall explain the reason.
Where personal information handlers reject individuals' requests to exercise their rights, individuals may file a lawsuit with a People's Court according to the law.

Chapter V: Personal Information Handlers' Duties

Article 51: Personal information handlers shall, on the basis of the personal information handling purpose, handling methods, personal information categories, as well as the influence on individuals' rights and interests, possibly existing security risks, etc., adopt the following measures to ensure personal information handling conforms to the provisions of laws and administrative regulations, and prevent unauthorized access as well as personal information leaks, distortion, or loss:

2. Formulating internal management structures and operating rules;
3. Implementing categorized management of personal information;
4. Adopting corresponding technical security measures such as encryption, de-identification, etc.;
5. Reasonably determining operational limits for personal information handling, and regularly conducting security education and training for employees;
6. Formulating and organizing the implementation of personal information security incident response plans;
7. Other measures provided in laws or administrative regulations.

Article 52: Personal information handlers that handle personal information reaching quantities provided by the State cybersecurity and informatization department shall appoint personal information protection officers, to be responsible for supervising personal information handling activities as well as adopted protection measures, etc.

Personal information handlers shall disclose the methods of contacting personal information protection officers, and report the personal names of the officers and contact methods to the departments fulfilling personal information protection duties and responsibilities.

Article 53: Personal information handlers outside the borders of the People's Republic of China, as provided in Article 3, Paragraph 2, of this Law, shall establish a dedicated entity or appoint a representative within the borders of the People's Republic of China to be responsible for matters related to the personal information they handle, and are to report the name of the relevant entity or the personal name of the representative and contact method, etc., to the departments fulfilling personal information protection duties and responsibilities.

Article 54: Personal information handlers shall regularly engage in audits of their personal information handling and compliance with laws and administrative regulations.

Article 55: When one of the following circumstances is present, personal information handlers shall conduct a personal information protection impact assessment in advance, and record the handling situation:

1. Handling sensitive personal information;
2. Using personal information to conduct automated decision-making;
3. Entrusting personal information handling, providing personal information to other personal information handlers, or disclosing personal information;
4. Providing personal information abroad;
5. Other personal information handling activities with a major influence on individuals.

Article 56: The content of the personal information protection impact assessment shall include:

1. Whether or not the personal information handling purpose, handling method, etc., are lawful, legitimate, and necessary;
2. The influence on individuals' rights and interests, and the security risks;
3. Whether protective measures undertaken are legal, effective, and suitable to the degree of risk.

Personal information protection impact assessment reports and handling status records shall be preserved for at least three years.

Article 57: Where a personal information leak, distortion, or loss occurs or might have occurred, personal information handlers shall immediately adopt remedial measures, and notify the departments fulfilling personal information protection duties and responsibilities and the individuals. The notification shall include the following items:

1. The information categories, causes, and possible harm caused by the leak, distortion, or loss that occurred or might have occurred;
2. The remedial measures taken by the personal information handler and measures individuals can adopt to mitigate harm;
3. Contact method of the personal information handler.

Where personal information handlers adopt measures that are able to effectively avoid harm created by information leaks, distortion, or loss, personal information handlers are permitted to not notify individuals; however, where departments fulfilling personal information protection duties and responsibilities believe harm may have been created, they may require personal information handlers to notify individuals.

Article 58: Personal information handlers providing important Internet platform services, that have a large number of users, and whose business models are complex shall fulfill the following obligations:

1. Establish and complete personal information protection compliance systems and structures according to State regulations, and establish an independent body composed mainly of outside members to supervise personal information protection circumstances;
2. Abide by the principles of openness, fairness, and justice; formulate platform rules; and clarify the standards for intra-platform product or service providers' handling of personal information and their personal information protection duties;
3. Stop providing services to product or service providers on the platform that seriously violate laws or administrative regulations in handling personal information;
4. Regularly release personal information protection social responsibility reports, and accept society's supervision.

Article 59: Entrusted persons accepting entrusted handling of personal information shall, according to the provisions of this Law and relevant laws and administrative regulations, take necessary measures to safeguard the security of the personal information they handle, and assist personal information handlers in fulfilling the obligations provided in this Law.

8. **Chapter VI: Departments Fulfilling Personal Information Protection Duties and Responsibilities**

Article 60: The State cybersecurity and informatization department is responsible for comprehensive planning and coordination of personal information protection work and related supervision and management work. Relevant State Council departments are responsible for personal information protection, supervision, and management work within their respective scope of duties and responsibilities, according to the provisions of this Law and relevant laws and administrative regulations.

County-level and higher people's governments' relevant departments' personal information protection, supervision, and management duties and responsibilities are determined according to relevant State provisions.

Departments provided in the previous two Paragraphs are all referred to as departments fulfilling personal information protection duties and responsibilities.

Article 61: Departments fulfilling personal information protection duties and responsibilities fulfill the following personal information protection duties and responsibilities:

1. Conducting personal information protection propaganda and education, and guiding and supervising personal information handlers' conduct of personal information protection work;
2. Accepting and handling personal information protection-related complaints and reports;
3. Organizing evaluation of the personal information protection situation such as procedures used, and publishing the evaluation results.
4. Investigating and dealing with unlawful personal information handling activities;
5. Other duties and responsibilities provided in laws or administrative regulations.

Article 62: The State cybersecurity and informatization department coordinates overall the following personal information protection work by the relevant departments:

1. Formulate concrete personal information protection rules and standards;

2. Formulate specialized personal information protection rules and standards for small-scale personal information handlers and new technologies and new applications for handling sensitive personal information, facial recognition, artificial intelligence, etc.;
3. Support the research, development, and broad adoption of secure and convenient electronic identity authentication technology, and promote the construction of public online identity authentication services;
4. Advance the construction of service systems to socialize personal information protection, and support relevant organizations to launch personal information protection evaluation and certification services;
5. Perfect personal information protection complaint and reporting work mechanisms.

Article 63: When departments fulfilling personal information protection duties and responsibilities fulfill personal information protection duties and responsibilities, they may adopt the following measures:

1. Interviewing relevant concerned parties, and investigating circumstances related to personal information handling activities;
2. Consulting and reproducing a concerned party's contracts, records, and receipts as well as other relevant material related to personal information handling activities;
3. Conducting on-site inspections, and conducting investigations of suspected unlawful personal information handling activities;
4. Inspecting equipment and articles relevant to personal information handling activities; and when there is evidence the equipment or articles are used to engage in illegal personal information handling activities, after reporting to their department's main person responsible in writing and receiving approval, they may seal or confiscate them.

Where departments fulfilling personal information protection duties and responsibilities fulfill their duties and responsibilities according to the law, concerned parties shall provide assistance and cooperation, and they may not obstruct or impede them.

Article 64: Where departments fulfilling personal information protection duties and responsibilities discover relatively large risks exist in personal information handling activities or personal information security incidents occur, they may conduct a talk with the personal information handler's legal representative or main person responsible according to regulatory powers and procedures, or require personal information handlers to entrust specialized institutions to conduct compliance audits of their personal information handling activities. Personal information handlers shall adopt measures according to requirements to correct the matter and eliminate the vulnerability.

Where departments fulfilling personal information protection duties and responsibilities discover in the course of their duties discover unlawful handling of personal information that is suspected of constituting a crime, they shall promptly transfer the matter to public security authorities for processing according to the law.

Article 65: Any organization or individual has the right to file a complaint or report about unlawful personal information handling activities with departments fulfilling personal information protection duties and responsibilities. Departments receiving complaints or reports shall process them promptly and according to the law, and notify the complaining or reporting person of the handling outcome.

Departments fulfilling personal information protection duties and responsibilities shall publish contact methods to accept complaints and reports.

Chapter VII: Legal Liability

Article 66: Where personal information is handled in violation of this Law or personal information is handled without fulfilling personal information protection duties in accordance with the provisions of this Law, the departments fulfilling personal information protection duties and

responsibilities are to order correction, confiscate unlawful income, and order the provisional suspension or termination of service provision of the application programs unlawfully handling personal information; where correction is refused, a fine of not more than 1 million Yuan is to be additionally imposed; the directly responsible person in charge and other directly responsible personnel are to be fined between 10,000 and 100,000 Yuan.
Where the circumstances of the unlawful acts mentioned in the preceding Paragraph are grave, the provincial- or higher-level departments fulfilling personal information protection duties and responsibilities are to order correction, confiscate unlawful income, and impose a fine of not more than 50 million Yuan, or 5% of annual revenue. They may also order the suspension of related business activities or cessation of business for rectification, and report to the relevant competent department for cancellation of corresponding administrative licenses or cancellation of business licenses. The directly responsible person in charge and other directly responsible personnel are to be fined between 100,000 and 1 million Yuan, and it may also be decided to prohibit them from holding positions of director, supervisor, high-level manager, or personal information protection officer for a certain period.
Article 67: Where unlawful acts as provided in this Law occur, they will be entered into credit files as provided by relevant laws and administrative regulations, and be publicized.
Article 68: Where State organs fail to fulfill personal information protection duties as provided in this Law, their superior organs or the departments fulfilling personal information protection duties and responsibilities shall order correction; the directly responsible person in charge and other directly responsible persons are to be sanctioned according to the law.
Where the personnel of departments fulfilling personal information protection duties commit dereliction of duties, abuse their power, or engage in favoritism, but not yet constituting a crime, they shall be sanctioned according to the law.
Article 69: Where the handling of personal information infringes upon personal information rights and interests and results in harm, and personal information handlers cannot prove they are not at fault, they shall bear compensation and other take responsibility for the infringement. In the above clause, the responsibility to compensate for infringement shall be determined according to the resulting loss to the individual or the personal information handler's resulting benefits. Where the loss to the individual and the personal information handler's benefits are difficult to determine, determine compensation according to practical conditions.
Article 70: Where personal information handlers handle personal information in violation of the provisions of this Law, infringing on the rights and benefits of many individuals, the People's Procuratorates, statutorily designated consumer organizations, and organizations designated by the State cybersecurity and informatization department may file a lawsuit with a People's Court according to the law.
Article 71: Where a violation of the provisions of this Law constitutes a violation of public security management, public security management punishment shall be imposed according to the law; where it constitutes a crime, criminal liability is to be investigated according to the law.

Chapter VIII: Supplemental Provisions

Article 72: This Law does not apply to natural persons handling personal information for personal or family affairs.
Where the law contains provisions on personal information handling by people's governments at all levels and their relevant departments and organizations implementing statistical and archival management activities, those provisions apply.
Article 73: The following terms used in this Law are defined as follows:

1. "Personal information handler" refers to organizations and individuals that, in personal information handling activities, autonomously decide handling purposes and handling methods.

2. “Automated decision-making” refers to the activity of using computer programs to automatically analyze or assess personal behaviors, habits, interests, or hobbies, or financial, health, credit, or other status, and make decisions [based thereupon].
3. “De-identification” refers to the process of personal information undergoing handling to ensure it is impossible to identify specific natural persons without the support of additional information.
4. “Anonymization” refers to the process of personal information undergoing handling to make it impossible to distinguish specific natural persons and impossible to restore.

Article 74: This Law shall enter into force on November 1, 2021.

Appendix 6
Critical Information Infrastructure Security Protection Regulations.[35] (Excerpts)

Article 2. Critical information infrastructure as mentioned in these regulations, refers to important network infrastructure, information systems, etc., in important industries and sectors such as public telecommunications and information services, energy, transportation, water, finance, public services, e-government, national defense science, technology, and industry, etc., as well as where their destruction, loss of functionality, or data leakage may gravely harm national security, the national economy and people's livelihood, or the public interest.
Article 8: The competent departments and supervision and management departments of important industries and sectors mentioned in Article 2 of these Regulations are the departments responsible for critical information infrastructure security protection work (hereafter abbreviated as "protection work departments").
Article 9: Protection work departments are to formulate critical information infrastructure identification rules in integration with the real situation in their industries and sectors, and report them to the State Council public security department for filing.
When formulating identification rules, the following factors shall be mainly considered:

1. The degree of importance of the network infrastructure, information system, etc., for the critical and core activities within the industry or sector;
2. The degree of harm that might result from the network infrastructure, information system, etc., if it is destroyed, loses functionality, or has its data leaked;
3. The associated influence on other industries and sectors.

Article 18: When major cybersecurity incidents occur or major cybersecurity threats are discovered in critical information infrastructure, operators shall report the matter to the protection work department and the public security authorities according to relevant regulations. When it occurs that critical information infrastructure completely ceases to function or its main functions are impeded, national basic information or other important data is leaked, personal information is leaked at a relatively large scale, relatively large economic damage is brought about, unlawful information is disseminated on a relatively large scale, or other such especially grave cybersecurity incidents occur, or especially grave cybersecurity threats are discovered, the protection work department shall, after receiving the report, promptly report the matter to the national cybersecurity and informatization department and the State Council public security department.

[35] Order of the State Council of the People's Republic of China No. 745, 30 July 2021, http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm?trs=1, as translated by DigiChina: https://digichina.stanford.edu/news/translation-critical-information-infrastructure-security-protection-regulations-effective-sept