China's Cyber Laws and Regulations

MARGIN RESEARCH

The research described in this report was sponsored by the Defense Advanced Research Projects Agency (DARPA) under Contract No. HR00112190088. The views expressed are those of the authors, and do not reflect any views or opinions of the United States Government.

www.margin.re

Contents

Foreword and Acknowledgements

At present, the most significant foreign cyber threats come from China, Russia, North Korea, and Iran. To help meet this challenge, the team at Margin Research has engaged in an integrated program looking at both the development of potentially malicious software as well as the way these states recruit skilled personnel, organize their cyber operations, and the legal regime within which they operate. Today China stands out as the most significant threat in the cyber arena, with a longstanding interest in information and its power and the usefulness of dominating it. In line with this tradition, the PRC has greatly expanded its cyber capabilities in intelligence collection, espionage, deception, and cyber warfare.

This rapidly growing threat has received increasing notice and discussion in the open literature, although data supporting China's malicious cyber operations are limited. A prior report by the Margin Research team presents an analysis based on open-source data generated by Chinese operations using code artifacts inserted into software such as the Linux Kernel. The result has been an exploration of China's malicious cyber ecosystem, rather than simply observing the aftermath of hostile cyber activities.

The present report extends the analysis to the Chinese legal and regulatory regime that both enables and controls the cyber ecosystem. Based on a review of the original materials, the team has explored several specific laws with regard to the control of data; regulation of activities that manage Internet and media operations; and the ability of the PRC and its security services to control individuals both within China and outside the country as well.

This study effort was made possible with support from the Defense Advanced Research Projects Agency (DARPA). The study team has benefited greatly from discussions with personnel from U.S. Government agencies and offices, as well as former officials and other experts. In addition to the Margin Research team, supporting the work have been several research assistants, currently graduate and law students at Harvard University and New York University (NYU) School of Law. The views expressed do not reflect the views of any organization or the U.S. Government.

February 1, 2023

Executive Summary

China's President Xi Jinping has made a point of emphasizing the importance of law in China and the promotion of the rule of law at the base of Chinese Communist Party governance and power. Like any law, Chinese law expresses national policy. In China, management and control of cyberspace and law go hand in hand, and cyber law proceeds from the big picture to data security, protection of personal information, and management of network product security vulnerabilities.

China's legal regime governing cyberspace includes three principal data laws, as well as dozens of administrative guidelines, including the recent Provisions on the Management of Network Product Security Vulnerabilities. Taken together, they reveal a sophisticated and dynamic regulatory system that the Chinese Communist Party will continue to strengthen as it pursues technological supremacy.

Over the last five years, China has produced and revised legislation and administrative regulations governing information communication technologies (ICTs), personal information, data, and cybersecurity. Officials have pushed these regulatory developments as an extension of China's concentration on technological development and as part of an effort to bring the country's cyber regulatory regime more in line with international standards, particularly those in Europe. These laws, guidelines, and ordinances govern the ways in which individuals and entities within the PRC may process data, interact with information networks, and engage with developing technologies.

Although some may point to China's authoritarian nature as a reason to be skeptical of the utility of Chinese law in understanding how the State will manage cyberspace, the Party, particularly under the leadership of Xi Jinping, has made a concerted effort to promote the rule of law and expand law-based government administration. Understanding the legal system in China provides insight into how the Party creates, legitimates, and manages power, and in particular shows how State power is experienced by the majority of Chinese citizens through the law and legal institutions.

Cybersecurity Law

China's Cybersecurity Law (CL), effective June 1, 2017, sits at the center of China's cyber regulatory regime, governing data management and network security and authorizing State organs to both establish and enforce network security requirements. The Cybersecurity Law imposes network security and data protection requirements on network operators – the owners, managers, and providers of networks – and can apply quite broadly under its stated definition of a network. Operators of critical information infrastructure must adhere to even more stringent demands.

This law further defines networks, network operators, network data, cybersecurity, and related subjects such as "Critical Information Infrastructure" (CII). Like other laws in the cyber domain, it requires operators to take steps, including through inspections, to fulfill their duties with respect to management and security. At the same time, the law makes clear that, on the one hand, Chinese citizens have rights and expectations with regard to the management, maintenance, and security of the network.

On the other hand, those responsible for network operations owe a duty to provide technical support and assistance to public officials responsible for national security and law and order. Therefore, privacy rights and the protection of personal information on the network do not shield one from government surveillance. Quite the contrary, the legal regime provides a basis for widespread surveillance and intrusion on personal privacy.

Data Security Law

Effective September 1, 2021, China's Data Security Law (DSL) was implemented to govern the collection, transfer, use, and storage of data. The DSL applies to all data handling activities that take place within the mainland territory of the PRC as well as certain listed activities outside the country. Depending on the particular classification of data and its relevance to key State interests, such as national security, State and government authorities, network operators, and data handlers must follow requirements dictating how and when data can be collected, how it can be stored, protected, and managed, and when and to whom it can be transferred.

In particular, this law imposes specific obligations on those who collect, transfer, and store data and penalties for failure to comply, establishing a comprehensive data definition and regulatory system. Government approval is required prior to any transmission of data to foreign law enforcement officials or agencies or indeed any person or entity abroad without a security assessment, although the law is not detailed about what constitutes a satisfactory security assessment. Detailed information about security assessment requirements is provided by administrative guidelines, such as the Cybersecurity Review Measures.

Personal Information Protection Law

Often compared to the European Union's GDPR, China's Personal Information Protection Law (PIPL), effective November 1, 2021, provides a comprehensive legal framework governing how domestic and foreign companies may collect, process, and transfer personal data. It requires that personal information handlers establish a "clear and reasonable" purpose in order to process personal information and sometimes imposes separate consent requirements as well. The law also lists the responsibilities of data processors when handling personal information, including the principles to which they must adhere, the security measures that must be followed, and the measures organizations must take in the event of a data breach.

The PIPL creates rights for individuals whose personal information may be processed, including rights of amendment and deletion. It imposes obligations on private and government entities, sets limitations on retention and storage location, and prohibits transfers under certain conditions. Additional regulations and guidelines have been clarified and expanded by subsequent publications from regulatory bodies such as the Cyberspace Administration of China.

The PIPL appears to establish a comprehensive, detailed, and deep regime for the collection, storage, dissemination, and protection of personal information. In this respect, it seems to share goals with the EU and other western regimes regulating the same categories of data. Unlike the situation in the EU, however, the PIPL, gives the State broad authority to collect and use personal information as it decides is necessary for national security and in the public interest.

While signage is required to notify people of collection of data in public places, the government may use such information for public security purposes if the individual's consent is not obtained. Chinese State organs are required to comply with regulations regarding the collection, handling, and storage of such data.

Provisions on the Management of Network Product Security Vulnerabilities

Issued by the Cyberspace Administration of China, the Provisions on the Management of Network Product Security Vulnerabilities (Provisions) regulate the "discovery, reporting, patching, and publication of software security vulnerabilities." Covering network operators, hardware and software developers, and any relevant companies or individuals, the Provisions prohibit the use, sale, and disclosure of vulnerabilities.

Under these guidelines, those who discover or encounter vulnerabilities must cooperate with State and government authorities. Further they are required to report their discovery to the Ministry of Industry and Information Technology (MIIT) within two days and are forbidden from disclosing this information to anyone else without government permission, although they may reveal the vulnerability to the provider of the product or service where it was discovered.

The Provisions emphasize that knowledge of vulnerabilities is State property, thus tightening the State's hold over knowledge of their existence and apply to all providers of hardware and software located in the PRC. Any person or organization involved in the "discovery, collection, and publication" of network vulnerability information also are covered and must comply.

Within the government, the CAC has overall planning and coordination responsibility with respect to implementing the Provisions while the MIIT oversees telecommunications and Internet. The Ministry of Public Security (MPS) is responsible for combatting illegal activities that exploit vulnerabilities.

In particular the Provisions prohibit: exploitation or use of vulnerabilities to engage in activities that endanger network security; collecting, selling, or publishing information about network product security vulnerabilities; publication of information about vulnerabilities prior to the patching of the problem by the provider without prior permission of the MIIT and MPS.

Users must not provide information about vulnerabilities in systems in use or exaggerate the hazards and risks of vulnerabilities to extort advantages from vendors. In short, those who discover vulnerabilities operate under serious legal restrictions. They are encouraged to contact providers, who then are required to inform the MIIT within two days of discovery.

Frequently Asked Questions

China's evolving legal and regulatory regime for cyberspace contains a substantial number of prohibitions and reporting requirements, especially with respect to hacking, denial of service, phishing, malware, and cybercrime tools, and related information. Further, the law on Guarding State Secrets creates a wide net for activities bearing on State security and national interests. One result is a likely prohibition on notifying foreign companies about foreign government exploitation of vulnerabilities of Chinese network products.

Even though this regime has been quite specific, there are a number of questions that remain, including:

- Is hacking a crime?
- Is there a legal basis for obtaining vulnerabilities or offensive cyber capabilities from outside the country?
- If China finds a vulnerability being used against its own government, can they legally keep it a secret and use it against other people (e.g., their own citizens or other governments)?
- What is the legal basis for disclosing vulnerabilities to the government before some other entity?
- If a citizen of a foreign government sells an exploit that's used against China (which the citizen is unaware of), have they technically committed a crime in China? Do they risk being arrested if they ever visit China after?
- Can Chinese intelligence or private industry warn American companies (e.g., Apple) about in-the-wild exploits being used by the American government they've discovered?

1. Introduction to China's Cyber Laws and Regulations

Information communication technologies, personal information and other data, and cybersecurity in China are governed by an ever-expanding system of legal and administrative regulations. Three laws - the Cybersecurity Law (CL), the Data Security Law (DSL), and the Personal Information Privacy Law - provide a foundational legal regime upon which state and government institutions have built a series of provisions, guidelines, and measures to manage data and cyberspace. Together, these regulations have established the parameters under which individuals and organizations within the PRC may process data, interact with information networks, and engage with developing technologies.

Some may point to China's authoritarian nature as a reason to be skeptical of the utility of Chinese law in understanding how the State will manage cyberspace. After all, law in China is subject to the leadership of the Party, and Xi Jinping's increasingly dictatorial assertion of power undermines any pretense of judicial independence from Party interference.

But to dismiss China's legal system out of hand ignores the power of law within the PRC. The Party has made a concerted effort to promote the rule of law and make "'law-based governance' (依法治国) a cornerstone of the party's governance strategy," all while maintaining the judicial systems' responsiveness to the "will of the Party." In his recent report to the 20th National Congress, Xi Jinping emphasized the need for promoting structural reform to ensure that administrative law enforcement is "strict, procedure-based, impartial, and civil."

The Party has also pushed to expand law-based government administration, empowering State legal institutions to augment legislation and create concrete regulatory guidelines that govern "complex matters on a day-to-day basis." The legal system in China thus provides insight into how the Party creates, legitimates, and manages power, and in particular shows how State power is experienced by the majority of Chinese citizens through the law and legal institutions. Notably, consumers in China have themselves pushed for more stringent regulatory control over data handling.

This guide provides an overview of the key parameters of China's three main data laws, as well as the recent Provisions on the Management of Network Product Security Vulnerabilities. It also attempts to answer key questions about the disclosure and use of vulnerabilities within China. While this is merely a glimpse into China's expansive legal regime for cyberspace, it reveals a sophisticated and dynamic regulatory system that the Party will certainly continue to strengthen as it continues to pursue technological supremacy.

2. Cybersecurity Law

中华人民共和国网络安全法

What is the purpose of the law?

Effective June 1, 2017, the Cybersecurity Law (CL) began as a means to bring China's legal regime "in line with global best practices for cybersecurity." Introducing a number of requirements governing data management and network security in China and authorizing government authorities to conduct security checks of networks, the CL provided a blueprint for the PRC's broader cyber governance regime, sitting at the center of the country's ICT regulatory scheme.

China's stated purpose in passing the legislation was 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" (Art 1).

Key Definitions

N**etwork** is "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" (Art. 76).

Network operators refers to "network owners, managers, and network service providers" (Art. 76).

Network data refers to "all kinds of electronic data collected, stored, transmitted, processed, and produced through networks" (Art. 76).

Cybersecurity is defined as "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" (Art. 76).

Who and what does the Cybersecurity Law cover?

The Cybersecurity Law is generally applicable to network operators, defined as the owners, managers, and providers of networks. Given the law's expansive understanding of what constitutes a network, effectively any business that manages their own email or other data network can fall under the scope of the law. Other businesses involved in critical sectors - e.g., communications, information services, energy, transportation, etc. - are also subject to the law.

What are the security protection duties of network operators?

Network operators must (Art. 21):

- Create an internal security management system and operating rules, and appoint personnel to manage cybersecurity protection measures
- Adopt technical measures to prevent data breaches and other network intrusions
- Adopt technical measures to monitor and record network status and cybersecurity incidents
- Adopt measures such as data classification, backup of important data, and encryption
- Adhere to other obligations provided by law or administrative regulations.

Network providers must also ensure that products or services comply with any mandatory requirements. They must submit to government conducted security checks, conduct security maintenance of products, develop an emergency response plan for cybersecurity incidents, and immediately adopt remedial measures upon the discovery of a security flaw or vulnerability (Arts. 22 & 24). Critical network equipment and specialized cybersecurity products must comply with specific requirements and security certifications formulated by state departments (Art. 23).

Art. 28 requires network providers to provide technical support and assistance to public and national security authorities that are "safeguarding national security and investigating criminal activities."

Network operators that fail to perform their cybersecurity protection duties may be subject to fines or corrective action, may have operations suspended, or may have any relevant permits or licenses revoked. Directly responsible management personnel may face personal liability. (Arts 59-75).

What is Critical Information Infrastructure?

Critical Information Infrastructure (CII) refers to key public communication and information services where "a loss of function" or data breach "might seriously endanger national security, national welfare, the people's livelihood, or the public interest" (Art 31). Examples of CII include power services, water resources, finance, and e-government infrastructure. CII are subject to specific security implementation plans developed by State Council departments (Art. 32) and must adhere to the following duties (Art. 34):

- Establish specialized security management bodies and appoint personnel to manage security
- Periodically conduct cybersecurity education, technical training, and skill evaluations for employees
- Conduct disaster recovery backups of important systems and databases
- Create emergency response plans for cybersecurity instances and periodically conduct drills

- Adhere to other obligations provided by law or administrative regulations.

CII operators must conduct, at minimum, yearly inspections of their network security measures and assess any risks that might exist (Art. 38). Critical information infrastructure may also be subject to random spot checks by State departments, may be required to conduct emergency cyber incident response drills, promote cybersecurity information sharing among State departments, operators, and other organizations, and provide technical support for emergency situations involving cybersecurity (Art. 39).

What are the data protection duties of network operators?

Network operators must maintain the confidentiality and security of any user information they collect (Arts. 40 & 42). They must publish rules for the collection and use of personal information and obtain the consent of individuals before gathering their personal data (Art. 41). Operators are forbidden to disclose, tamper with, or destroy any personal information they gather.

Individuals have the right to demand network operations delete or correct their personal information (Art. 43). Network operators must establish and publicize systems for making complaints or reports about data or network security (Art. 49).

What are the requirements for data storage?

Operators of critical information infrastructure that gather or produce important data during operations within Mainland China must store that data within China (Art. 37). A CII operator found storing or providing data to those outside the mainland territory can face corrective measures and fines, have illegal gains confiscated, receive a suspension, and have business licenses or permits revoked (Art. 66).

Has anything changed since the law was first implemented?

Not yet, but the CAC proposed a series of amendments in September 2022, primarily focused on increasing fines and introducing new penalties for violations. The revisions would also remove language on personal information protection, which is now covered by the Personal Information Protection Law (PIPL).

3. Data Security Law

中华人民共和国数据安全法

What is the purpose of the law?

The Data Security Law (DSL), effective September 1, 2021, was implemented to "standardize data handling activities, ensure data security, [and] promote data development and use" in China (Art. 1). It imposes several requirements for the collection, transfer, and storage of data and provides a legal basis for imposing liability on those who fail to meet these requirements (Art. 2).

Key Definitions

The DSL defines:

Data as "any information record in electronic or other form" (Art. 3).

Data handling refers to "the collection, storage, use, processing, transmission, provision, disclosure, etc., of data" (Art. 3).

Data security is defined as "ensuring data is in a state of effective protection and lawful use through adopting necessary measures, and [] possessing the capacity to ensure a persistent state of security" (Art. 3).

Core data (核心数据) refers to data concerning "national security, the lifelines of the national economy, important aspects of people's livelihoods, [or] major public interests" (Art. 21).

What does the Data Security Law cover?

The DSL applies to all data handling activities that take place within the mainland territory of the PRC, as well as those activities outside of China that "harm the national security, the public interest, or the lawful rights and interests of citizens or organizations of the PRC" (Art. 2).

The law classifies data per its relevance to national security, privacy, and major public interests and regulates the use, storage, and transfer of data according to its classification level. Data concerning Chinese national and economic security, the welfare of citizens, or major public interests constitute **core data (核心数据)** and are subject to the highest level of protection and regulation (Art. 21). A step below core data is **important data (重要数据)**, a concept which first emerged in the Cybersecurity Law and is undefined by both the CL and the DSL. Later guidelines have referred to important data as information that "may affect national security, economic security, social stability or public health, safety and interest" if disclosed.

Who does the Data Security Law cover?

The DSL creates obligations for the State and government authorities at the national, provincial, and local levels. It also covers Critical Information Infrastructure Operators, data collectors, data handlers, and intermediary services engaged in data transactions.

What is required by the Data Security Law for the State?

The DSL creates several obligations for the State. It requires the State to establish data security governance systems, increase data security protection capacities, protect the rights and interests of individuals and organizations, encourage the use and free-flow of data, and "promote the development of the digital economy" (Arts. 4 & 7). The State is obligated to create a national "big data strategy," advance the construction of data infrastructure, and support the application of data in all industries and fields (Art. 14).

These obligations trickle down to the provincial and local level governments, which are similarly tasked with incorporating digital economy development in economic and social development plans. Article 12 also compels the State to promote the free flow of data across borders and participate in international exchanges involving the development of international rules and standards for data security.

The State must develop procedures for encouraging individuals, organizations, and other government and industry entities to engage in data security protection, including developing services for data security testing, assessment, and certification (Arts. 9 & 18). Similarly, the law also provides for the development of a "categorized and graded protection system for data," with stricter security requirements depending on the data's relevance to national security or the public interest (Art. 21).

For example, "the government IT standards-setting authority" distinguishes between five levels of data with increasing risk: open data (公开), internal data (内部), sensitive data (敏感), important data (重要) and core data (核心).) Local and sectoral authorities must create a specific catalog of important data that falls within the purview of their authority.

The DSL requires the State to create a centralized mechanism for managing data security risk assessments (Art. 22), as well as a data security emergency response mechanism (Art. 23), and a data security review system (Art. 24).

The State must implement export controls for data (Art. 25). The DSL also allows the PRC to adopt reciprocal measures in response to states that impose restrictive measures against the PRC involving data or data development and use technology (Art. 26).

The "central leading institution for national security" is tasked with policy-making, coordinating national data security work, developing and implementing a national data security strategy, and creating a mechanism to coordinate any work on national data security (Art. 5).

Local departments and authorities, including law enforcement, are responsible for data security in their respective areas of work. Departments involved in critical industries, such as telecommunications and transportation, are given "data security regulatory duties within the scope

of their respective duties" (Art. 6). When public authorities obtain data for national security or other investigatory purposes, they must undergo strict approval procedures to be provided by future guidelines (Art. 35).

What are the requirements for State and government authorities that handle data?

Any State authority that collects or uses data to "perform their legally-prescribed duties" must operate within the scope of such duties and adhere to any conditions or procedures provided by the law or other administrative regulations (Art. 38). They must also preserve the confidentiality of personal private data, personal information, commercial secrets, and confidential commercial information.

State authorities are required to establish data security management systems, implement data security protection responsibilities, and ensure the security of government data (Art. 39). When outsourcing data management or security responsibilities to outside entities, State authorities must undergo approval procedures and supervise the outside parties' activities (Art. 40). These outside parties are in turn subject to specific legal and administrative obligations and cannot retain, use, or disclose government data without authorization.

The DSL also establishes operating principles for government data, including building a "uniform and standard" data platform for facilitating the interoperability of government data (Art. 42).

What is required for data handlers?

Individuals and entities handling data in China must establish a data security management system, conduct data security education and training, and must adopt technical and other measures to ensure data security (Art. 27).

Organizations handling important data must designate an officer or management body responsible for data security and submit periodic risk assessments to relevant government departments (Arts. 27 & 30). These assessments must include "the type and amount of important data being handled, the circumstances of the data handling activities, [and] the data security risks faced and measures to address them" among other information (Art. 30). More specific details about the content of security assessments are provided by administrative guidelines, such as the Cybersecurity Review Measures, the Internet Information Service Algorithmic Recommendation Management Provisions, and the Outbound Data Transfer Security Assessment Measures.

When a security risk is discovered or a data breach occurs, a data handler must take immediate remedial measures (Art. 29). Data handlers must also notify users of any data breaches "promptly" and must report any incidents to the relevant government department.

Organizations, as well as directly responsible personnel, that fail to adhere to these obligations may face severe fines (Art. 45). These fines may be compounded by failure to make corrections, the scope of the consequences of the violation, or the classification of the data. Data handlers may also be required to suspend operations, have business permits or licenses, or even face criminal liability depending on the nature of the violation.

Data handlers that do not collect data themselves but are engaged in intermediary services involving data transactions (e.g., commercial data transfers) must ask data providers to explain their data sources, verify the identities of both parties to the data transaction, and retain verification and transaction (Art. 33). Intermediary service providers that fail to adhere to these obligations face similar penalties to those described above, including fines, suspension of business operations, revocation of permits, and the confiscation of unlawful gains (Art. 47). The DSL also creates a basis for civil liability for harms caused by violations of the law, and those who contravene any obligations may also face criminal liability where such transgressions constitute a crime (Art. 52).

Can data be shared abroad?

Whether data may be transferred outside of China is determined by the data's classification and the recipient of the transfer. The DSL prohibits domestic organizations and individuals from providing any data stored in China to any foreign justice or law enforcement institutions without the prior approval of PRC authorities (Art. 36). Penalties for providing data without approval include fines, forced suspension of operations, and the revocation of business licenses (Art. 48)

Important data collected or produced by critical information infrastructure operators (CIIO) must be stored in China and cannot be sent abroad without first completing a security assessment. The DSL provides for the development of other outbound security measures by the Cyberspace Administration of China (CAC) and other State Council departments (Art. 31). Data handlers that violate these provisions may face corrective actions, warning, and fines between 100,000 and 1,000,000 yuan, be required to suspend operations, and have business permits or licenses revoked (Art. 46).

The CAC's Outbound Data Transfer Security Assessment Measures came into effect on September 1st, 2022. The Measures delineate the security assessment requirements data processors must complete in order to obtain approval for (Art. 4):

- The outbound transfer of important data by a data processor
- The outbound transfer of personal information by a critical information infrastructure operator or a personal information process that has processed the information of more than 1 million individuals
- The outbound transfer of personal information by a personal information handler that has made outbound transfers of the personal information of more than 100,000 individuals or the sensitive personal information of more than 10,000 individuals in a year
- Other circumstances required by the CAC.

The CAC released its first data export security assessment on January 18, 2022, approving the exchange of data (presumably including personal and medical information) between Beijing and Amsterdam based hospitals collaborating on a joint research project. Although the CAC has stated they have only approved two outbound data transfer security assessments at this time, more are certain to follow in short order.

4. Personal Information Protection Law

中华人民共和国个人信息保护法

What is the purpose of the law?

The Personal Information Protection Law (PIPL) is a comprehensive legal framework governing how companies both within and outside China may collect, process, and transfer personal data. The law provides "broad principles, objectives, mandates, and responsibilities" for the use of personal information, which will be (and have been) clarified by subsequent guidelines and regulations from regulatory bodies such as the Cyberspace Administration of China.

Key Definitions

Personal information is defined as any kind of information related to "identified or identifiable natural persons" that is "recorded by electronic or other means" (Art. 4). This definition, however, excludes information that has been anonymized.

Sensitive personal information refers to "personal information that, once leaked or illegally used" may cause harm to individuals or their property. This includes "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" (Art. 28).

Personal information processing (or handling) includes the "collection, storage, use, processing, transmission, provision, disclosure and deletion" of personal information (Art. 3).

Personal information handler "refers to organizations and individuals that, in personal information handling activities, autonomously decide handling purposes and handling methods" (Art. 73).

Anonymized data cannot be used to distinguish specific persons and cannot be restored to identifiable information after processing (Arts 4. & 73).

What or who does the law cover?

The PIPL applies to all activities that involve processing "the personal information of natural persons within the borders" of the PRC (Art. 3). Any entity that collects, stores, uses, transfers, or otherwise handles the personal information of people within China is therefore subject to the law, regardless of whether or not the organization is located or conducts operations outside the country.

When an entity processes the personal information of people within China but conducts its data processing activities outside of the state, the PIPL still applies when (1) the processing purpose

is to provide goods of services to people within China; (2) the organization analyzes or assesses the behavior of people within China, or (3) the activity satisfies other conditions established by law or administrative regulation (Art. 3).

The PIPL explicitly applies to the private information of employees and Human Resources, meaning that employers cannot send employment or HR related data outside of China without first anonymizing the data or obtaining the consent of the employee in question (Art. 13).

When can an entity process personal data?

Personal information handlers must have a "clear and reasonable purpose" for data processing, and any data handling must be related to that purpose (Art. 6). They also must establish one of the following legal bases in order to process personal information (Art. 13):

- Consent of individual data subjects
- Where necessary to conclude or fulfill a contract in which the individual is an interest party
- Where necessary to conduct Human Resources management, adhering to other labor laws and existing contracts
- Where necessary to fulfill legal responsibilities or obligations
- Where necessary to respond to sudden public health emergencies or under emergency conditions to protect the lives, health, and property of people
- Within a reasonable scope for news reporting, supervising public opinion, or other such activities for the public information
- When handling personal information disclosed by the relevant persons themselves or otherwise lawfully disclosed
- Other conditions in laws and administrative regulations

Consent is *not* required if an entity can establish one of the other listed bases for processing. However, separate consent is required when:

- Transmitting personal information to a third party, including another data processor (Art. 23)
- Processing sensitive personal information (Art. 29)
- Processing the personal information of minors under the age of 14 (Art. 31)
- Conducting cross-border transfers of personal information (Art. 39)

Sensitive personal information may only be handled for a specific purpose and need, and handlers must adhere to strict protection measures (Art. 28). Personal information handlers should cease to process or proactively delete personal information when the data processing's purpose has been achieved, has proven impossible to achieve, or is no longer necessary; the handler no longer operates; the retention period has expired; the individual rescinds consent; or the data was handled in violation of another law, regulation, or agreement (Art. 47).

When an entity processes personal information on the basis of consent, what is required?

Before handling personal information, data handlers must explicitly notify individuals, in "clear and easily understood language," of the following (Art. 17):

- The name and contact method of the personal information handler
- The purpose of personal information handling and the handling methods, the categories of handled personal information, and the retention period
- Methods and procedures for individuals to exercise their rights
- Other items required by law or administrative regulations

Individuals must provide a "voluntary and explicit statement" of their consent, and in some cases, may be required to provide separate or written consent (Art. 14). If there is any change to the purpose, method, or categories of personal information being processed, the data handler must obtain the data subject's consent again, unless a law or regulation provides that notification is not necessary or there are emergency circumstances as per Article 18.

Data subjects retain the right to revoke consent, and data processors must provide a "convenient way to withdraw consent" (Art. 15).

What are organizations' responsibilities when processing personal information?

Organizations must have a "clear and reasonable purpose" for data processing, and any data handling must be related to that purpose. Data handlers are also obligated to exercise data minimization by limiting the processing of personal information to only what is necessary for the data processing purposes (Art. 6) and limiting data storage to the shortest period necessary to fulfill the purpose of the data processing (Art. 19). Data processors cannot handle personal information in misleading, swindling, or coercive ways (Art. 5).

Data handlers are required to adhere to the principles of openness and transparency and are expected to disclose the purpose, method, and scope of data processing, as well as any rules for handling personal information (Art. 7). They must ensure the quality and accuracy of any data under their control and adopt adequate security measures to protect personal information (Arts. 8 & 9).

If handlers process data jointly with another processor or entrust another entity to handle personal information under their purview, all engaged entities must create an agreement detailing how the personal information is to be managed, what the responsibilities of the respective parties are, and what security measures will be adopted to protect the data (Art. 21).

Data processors must notify individuals when transferring personal information due to a merger, separation, dissolution, or bankruptcy (Art. 22). They must notify and obtain separate consent when giving personal information under their control to another data handler (Art. 23) or when processing sensitive personal information (Art. 29). Data handlers are also forbidden from engaging in "unreasonable differential treatment of individuals" when using personal information to conduct automated decision making (Art. 24).

Individuals and organizations are prohibited from illegally collecting, using, processing, transmitting, selling, buying, providing, or disclosing personal information without consent and are entirely restricted from personal data processing that threatens national security or the public interest (Arts. 10 & 25).

Under Article 51, personal information handlers are required to:

- Formulate internal management structures and operating rules
- Implement categorized management of personal information
- Adopt technical security measures
- Determine operational limits for personal information handling
- Regularly conduct security education and training for employees
- Develop and implement security incident response plans
- Adhere to other measures provided by law or administrative regulations

Data handlers must also regularly audit their data processing activities for compliance (Art. 54).

Foreign personal information processors must establish a dedicated entity or appoint a representative within China's borders to be responsible for personal information handling activities (Art. 53).

What should organizations do in the event of a data breach?

If there is a data breach, data handlers must take immediate steps to remedy the situation and notify the relevant authorities and affected individuals. This notification should include (Art. 57):

- The categories of information implicated
- The causes of and possible harm caused by the breach
- The measure the handler has taken to mitigate harm
- What measures individuals can adopt to mitigate harm
- How to contact the personal information handler

Individual notification is not required if data processors adopt measures that are able to "effectively avoid harm" created by the breach.

What rights are granted to individuals?

Under the PIPL, individuals have the right to:

- Know and decide relating to their personal information (Art. 44)
- Limit or refuse the processing of their personal information unless otherwise stipulated by law (Art. 44)
- Consult or copy their personal information from personal information handlers (Art. 45)

- The portability of their personal information when requested (Art. 45)
- Amend, supplement, or delete their personal information (Arts. 46 & 47)
- Request that data processors explain their rules for processing personal information (Art. 48)

If the data subject is deceased, their next of kin may exercise the rights listed above (Art. 49).

When is a personal impact protection assessment required?

A personal information handler should conduct a personal information impact assessment when the entity is (Art. 55):

- Handling sensitive personal information
- Using personal information in automated decision making
- Entrusting personal information data processing or providing personal information to other personal information handlers
- Transferring personal information aboard
- Engaging in other personal information handling activities with a major influence on individuals

The personal information impact assessment should include (Art. 56):

- Whether the purpose and method of the data handling are lawful, legitimate, and necessary
- How the data handling will affect individuals' rights and interests
- The security risks of the data processing
- Whether protective measures are legal, effective, and suitable to the degree of risk

These assessment reports and records should be retained for at least 3 years (Art. 56).

What are the consequences for non-compliance?

Individuals or entities that violate the PIPL may be required to correct violations, have illegal gains confiscated, suspend or terminate services, and have operating or business licenses revoked, among other remedies. The head of a company or "directly responsible" individuals may be held individually liable and fined or prohibited from working in certain positions (Art. 66).

Violating entities can be fined up to 50 million yuan (approximately $7.7 million) or 5% of their annual revenue. Individuals can face fines between 100,000 and 1 million Yuan or be prohibited from engaging in certain business activities or positions. Their violations may be incorporated into their social credit file or publicized (Art. 67). If they engage in data processing activities that harm citizens' rights and interests or threaten national security and public interest, organizations and individuals may also be placed on a government blacklist, limiting their access to personal information (Art. 42).

The PIPL gives a private right of action to individuals who have suffered harm due to the improper processing of their personal data (Art. 69). Organizations may be required to provide compensation if they cannot demonstrate a lack of fault. They may face even harsher punishments, including criminal liability, if their actions violate public security regulations (Art. 71).

Individuals may file a lawsuit when processors disregard an individual's request to exercise their rights as listed in Chapter IV (Art. 50). They can also file a complaint with enforcement authorities (Art. 65). Article 70 also authorizes designated organizations to file a public interest class action lawsuit when a processor "infringes the rights and interests of many individuals."

Where can data be stored?

Entities that operate critical information infrastructure or which handle an amount of personal information exceeding requirements established by the CAC are required to store data within the mainland territory of the PRC (Art. 40). The latter must also appoint a personal information protection officer in charge of supervising handling activities and enforcing security measures (Art. 52).

Can personal information be transferred across borders?

Art. 12 of the PIPL encourages state officials to participate in the formulation of international rules or norms for protecting personal information and promote "mutual recognition of personal information protection rules."

In order to engage in cross-border data transfers, data processors must have a legitimate purpose for the transfer, establish the necessity of the transfer, and notify and gain the consent of any data subjects prior to the transfer. State organs are also forbidden from providing information abroad unless truly necessary, in which case they must undertake a security assessment (Art. 36).

To satisfy the notification requirement, data handlers must provide the affected individuals with (Art. 39):

- The name and contact details of the overseas recipient;
- The purposes and methods of the data processing;
- The categories of handled personal information:
- The procedures by which individuals can exercise their rights under the PIPL with the overseas recipient of the data Data processors must also meet one of the conditions laid out in Article 38;
- Passing a security assessment conducted by the Cybersecurity Administration of China (CAC);
- Obtaining personal information protection certification from a specialized agency adhering to CAC requirements
- Contracting with the foreign party receiving the data to allocate rights and responsibilities in accordance with the CAC's standard contract

- Complying with other conditions provided by law, administrative regulations, or the CAC

As with the Data Security Law, personal information handlers are forbidden from providing personal data stored within China to any foreign judicial or law enforcement agencies (Art. 41). The Outbound Data Transfer Security Assessment Measures provide more detailed information about the prerequisites for transferring personal information abroad.

Are there special obligations for certain personal information handlers?

Per Article 58, data processors that provide important Internet platform services, have a large number of users, or have "complex" business models should:

- Establish an internal structure system to ensure compliance and protect personal information
- Form an independent body to supervise any internal protection processes
- Abide by the principles of openness, fairness, and justice
- Provide platform rules and clarify standards for handling personal information
- Cease services to providers on the platform that violate the law or other administrative regulations governing the use of personal information
- Regularly publish social responsibility reports
- Accept society's supervision

Which authorities are responsible for enforcing the Personal Information Protection Law?

The CAC is responsible for planning and coordinating personal information protection, as well as any related supervisory or administrative work (Art. 60). Other ministries and departments of the State Council are responsible for the protection, supervision, and management of personal information that falls within the scope of their duties and responsibilities. Local government departments at the county level or above are required to adhere to other duties and responsibilities for personal information protection imposed by State regulations.

What are the obligations of State organs under the PIPL?

The CAC is responsible for coordinating all work involving the protection of personal information, including creating rules and standards for protection; supporting the research, development, and adoption of technologies and services; facilitating the construct of public service systems for personal data protection; supporting the development of security certification programs; and formulating mechanisms to process complaints and reports (Art. 62).

Agencies tasked with personal information protection duties may create propaganda or education to inform data handlers, as well as guide and supervise their activities; field complaints and reports related to personal information protection; establish evaluation procedures for data violations; and investigate unlawful activities (Art. 61).

To fulfill their own responsibilities and duties to protect personal information, State and government departments may interview concerned parties, investigate circumstances related to data processing activities, consult a concerned party's records, conduct on-site inspections or investigations, and inspect equipment or other articles relevant to personal information handling activities (Art. 63).

Does the PIPL restrict government or State use of personal information?

The PIPL gives the State broad authority to collect and use personal information as necessary for matters of national security and the public interest. Article 26, for example, declares that the State will install image collection or personal identity recognition equipment in public venues in order to "safeguard public security and observe relevant State regulations." The law, however, does provide some limitations, such as requiring clear indicating signs when equipment is installed and restricting the use of collected information to public security purposes without other consent.

State organs must adhere to several requirements when handling personal information, including limiting the scope of data handling to the "extent necessary to fulfill their statutory duties and responsibilities" (Art. 34), fulfilling notification duties unless otherwise exempted (Art. 35), and storing data within the mainland territory of the PRC (Art. 36).

5. Provisions on the Management of Network Product Security Vulnerabilities

关于印发网络产品安全漏洞管理规定的通知

What is the purpose of these provisions?

Issued by the Cyberspace Administration of China, the Provisions on the Management of Network Product Security Vulnerabilities regulate the "discovery, reporting, patching, and publication of security vulnerabilities" in software (Art. 1). The provisions purportedly defend against security risks by compelling those that discover vulnerabilities to cooperate with State and government authorities. Critically, these provisions emphasize vulnerabilities' use as a government resource, tightening the State's hold over knowledge of their existence.

Who do the provisions cover?

The provisions apply to the providers of network products (e.g., hardware and software) and network operators located within Mainland China (Art. 2). Organizations and individuals that are involved in the "discovery, collection, and publication" of network vulnerabilities are also required to comply with the Provisions.

Which authorities are responsible for managing network security vulnerabilities?

The State Internet Information Office (i.e., the CAC), Ministry of Industry and Information Technology (MIIT), and Ministry of Public Security are together responsible for coordinating and managing network security vulnerabilities. The CAC is responsible for overall planning and coordination, the MIIT oversees vulnerabilities in telecommunications and Internet industries, and the MPS is tasked with combating the use of vulnerabilities to engage in illegal activities (Art. 3).

Can Chinese citizens use vulnerabilities they discover?

Art. 4 prohibits organizations and individuals from exploiting or using vulnerabilities in "activities that endanger network security." They must also not provide any support to other actors they know to be engaged in the exploitation of security vulnerabilities.

Can Chinese nationals sell vulnerabilities to other countries?

Organizations and individuals in China are forbidden from "illegally collect[ing], sell[ing], or publish[ing] information on network product security vulnerabilities" (Art. 4).

Can Chinese citizens tell anyone about any vulnerabilities they discover?

Organizations and individuals may not publish information about vulnerabilities before the network product provider provides a patch or during periods when the State hosts "major activities" (Art. 9). If a person or entity feels that it is necessary to publicly disclose a vulnerability

prior to this, they must obtain permission to publish from the MIIT and MPS. Individuals cannot provide detailed information about vulnerabilities if the network, system, or equipment is in use, nor can they "deliberately exaggerate the hazards and risks" of a vulnerability to extort vendors.

The Provisions also forbid using information about a vulnerability for fraud, or publishing or providing procedures or tools that can be used to exploit vulnerabilities "to engage in activities that endanger network security" (Art. 9). Organizations are required to "strengthen internal management and employ measures" so that information about undisclosed vulnerabilities will not leak (Art. 11).

Art. 9 also prohibits individuals and organizations from sharing information about an undisclosed vulnerability to "overseas organizations or individuals" other than the manufacturer of the product where the vulnerability was discovered.

What should Chinese citizens and organizations do if they discover a vulnerability?

Organizations and individuals who discover network vulnerabilities are "encouraged" to report the vulnerability to the provider of the network product where the vulnerability was discovered (Art. 5). For their part, network product providers, network operators, and vulnerability collection platforms must provide channels for receiving information on vulnerabilities (Art. 5). They are also obligated to promptly test and evaluate the impact of the security vulnerability, patch any security vulnerabilities in their network, and inform any impacted users if necessary (Art. 7). If the security vulnerability exists in an upstream product, they must immediately notify the provider of the product in question.

Most importantly, network product providers must report any "information on the relevant vulnerabilities" to the MIIT **within two days** of discovery.

6. Frequently Asked Questions

Is hacking a crime?

The unauthorized access of a computer information system is a crime under Art. 285 of the Criminal Law. A person who violates this provision will face different penalties depending on what kind of computer information system they intruded upon. The Public Security Administration Punishments Law also allows a person to be detained when they invade a computer system in such a way that causes harm to the system (Art. 29). Art. 27 of the Cybersecurity Law prohibits individuals and organizations from illegally intruding into other parties' networks, disrupting the normal function of the network, or stealing network data.

Denial of service attacks could violate Art. 286 of the Criminal Law (sabotaging a computer information system), Art. 29 of the Public Security Administration Punishments Law ("deleting, changing, increasing or interfering with the functions of a computer information system, which makes it impossible for the system to operate normally"), and Art. 27 of the Cybersecurity Law.

Similarly, a person engaging in phishing, infecting IT systems with malware, distributing or possessing tools to commit cybercrime, participating in identity theft, conducting unsolicited penetration testing, or playing a role in any other activity that "adversely affects or threatens the security… of any IT system" could face penalties under the Criminal Law, the Public Security Administration Punishments Law, and the Cybersecurity Law, in addition to several other rules and regulations.

Note that according to China's Criminal Law, a crime is committed within the territory of China when "the criminal act or its consequences take place within the territory of China." Thus, the law could apply to Chinese citizens who commit prohibited crimes outside China's territory or to foreigners who commit crimes outside of China against the State or Chinese citizens.

Is there a legal basis for obtaining vulnerabilities or offensive cyber capabilities from outside the country?

Art. 7 of the National Intelligence Law obligates Chinese citizens and organizations to "support, assist, and cooperate with national intelligence efforts," which may include the discovery, disclosure, or exploit of vulnerabilities. Intelligence agencies may also request that organizations and citizens assist them in their intelligence efforts (Art. 14). Art. 10 of the same law permits "national intelligence work institutions… to use the necessary means, tactics, and channels to carry out intelligence efforts, domestically and abroad."

Similarly, the Counter-espionage Law, currently under revision, imposes a duty on PRC citizens to "preserve national security, honor and interests." Per Art. 20, citizens and organizations cannot refuse to facilitate and provide assistance to government and State counter-espionage efforts.

The Data Security Law requires organizations and individuals to cooperate with requests by public security and national security authorities to obtain "data as necessary to safeguard national security or investigate crimes in accordance with law" (Art. 35). The Personal Information Protection Law requires concerned parties to provide assistance and cooperate with government departments "fulfilling personal information protection duties" and forbids such parties from obstructing or impeding these departments in any way (Art. 63).

Art. 7(2) of the Provisions on the Management of Network Product Security Vulnerabilities require organizations operating within China to report any known software vulnerabilities to the Ministry of Industry and Information Technology within two days of discovery.

While these laws do not create an explicit legal basis for *obtaining* vulnerabilities or offensive cyber capabilities from outside the country, they do create legal obligations for Chinese citizens and organizations to comply with government requests for data, which can include sharing vulnerabilities or other offensive cyber capabilities that individuals or entities discover.

If China finds a vulnerability being used against its own government, can they legally keep it a secret and use it against other people (e.g., their own citizens or other governments)?

The Law of the People's Republic of China on Guarding State Secrets defines state secrets as "matters that have a vital bearing on State security and national interests and, as specified by legal procedure, are entrusted to a limited number of people for a given period of time." These matters are not limited to those related to the military, national security, law enforcement, and foreign affairs, but can also include matters involving "the national economy, social development, science and technology" and anything else Chinese authorities classify as a state secret.

A network vulnerability being used against the Chinese government would almost certainly "have a vital bearing on State security and national interests," and authorities would likely be able to qualify designating it a state secret. The question of whether or not China could then use that vulnerability against other people is less clear, but the Cybersecurity Law, Data Security Law, and Personal Information Protection Law, in addition to other regulations, all provide the State with broad leeway to exercise authority in matters of national security and the public interest.

There is some evidence to suggest that the Ministry of State Security (MSS) delays publishing software vulnerabilities in the National Vulnerability Database (CNNVD) in order to review "high-threat CVEs…for their operational utility." In one instance examined by Recorded Future's report, the CNNVD delayed publishing a vulnerability until 57 days after it was disclosed. This vulnerability had been used by, among others, a suspected Chinese threat group to target telecommunication industry analysts and financial firms in Russian and Central Asia. The publication of another vulnerability was delayed for 236 days after disclosure; these backdoors have been connected to Chinese government surveillance of cell phones and internet use.

What is the legal basis for disclosing vulnerabilities to the government before some other entity?

Article 7 of the Provisions on the Management of Network Product Security Vulnerabilities requires individuals and organizations to report information about vulnerabilities to the MIIT

within two days. The Provisions also prohibit disclosing vulnerabilities to parties beside the network provider of the product where the vulnerability was discovered without government approval.

Other laws impose similar reporting requirements on Chinese citizens. The Counter-espionage Law, for example, requires citizens and organizations that discover espionage to promptly report the activity to State security organs (Art. 21).

If a citizen of a foreign government sells an exploit that's used against China (which the citizen is unaware of), have they technically committed a crime in China? Do they risk being arrested if they ever visit China after?

Article 27 of the Counter-espionage Law imposes criminal liability on any extraterritorial institutions, organizations, or individuals that "carry out, or instigate or fund others in carrying out espionage activities." (For a definition of "espionage conduct," see Art. 38). Likewise, when domestic institutions, organizations, or individuals that are linked to foreign entities conduct espionage activities, they may also be subject to criminal penalties. Foreign personnel that violate the Counter-espionage Law may be required to leave the country or be deported (Art. 34). The law does permit some leniency for violators who turn themselves in and/or make meritorious services. Those who were coerced or induced to participate in espionage activities may avoid prosecution by "promptly and truthfully" reporting the circumstances to a state or public security organ.

A person selling an exploit unknowingly used against China could face imprisonment under China's Criminal Law, insofar that selling the exploit could constitute providing "special programs or tools specially used for intruding into or illegally controlling computer information systems" (Art. 285). The sale of vulnerabilities could also arguably constitute intentionally "spread[ing] programs such as the computer viruses, thus affecting the normal operation of the computer system," violating Art. 286 of the law.

Can Chinese intelligence or private industry warn American companies (e.g., Apple) about in-the-wild exploits being used by the United States government they've discovered?

Likely not, unless the exploit has already been publicly disclosed or they have the permission of State authorities. The Provisions on the Management of Network Product Security Vulnerabilities require almost immediate disclosure to public authorities and forbid premature disclosure of exploits. Moreover, Art. 9 prohibits anyone from sharing information about an undisclosed vulnerability to "overseas organizations or individuals." If, however, the vulnerability was discovered within the American company's product, then the provisions allow for disclosure only to the product's manufacturer.

7. Other Regulations

Cybersecurity Review Measures (网络安全审查办法) (Effective 15 February 2022)

Critical Information Infrastructure Security Protection Regulations (关键信息基础设施安全保护条例) (Effective 1 September 2021)

Cryptography Law of the People's Republic of China (中华人民共和国密码法) (Effective 1 January 2020)

Guidelines for Internet Platform Categorization and Grading (Draft for Comment) (--互联网平台分类分级指南)

Internet Information Service Algorithmic Recommendation Management Provisions (互联网信息服务算法推荐管理规定) (Effective 1 March 2022)

Internet Information Service Deep Synthesis Management Provisions (Draft for Comment) (互联网信息服务深度合成管理规定)

Law of the People's Republic of China on Countering Telecommunications and Online Fraud (中华人民共和国反电信网络诈骗法) (Effective 1 December 2022)

Mobile Internet Application Program Information Service Management Regulations (Draft for Comment) (移动互联网应用程序信息服务管理规定)

Provisions on the Management of Mobile Internet Applications' Information Services (移动互联网应用程序信息服务管理规定) (Effective 1 August 2022)

Provisions on Procedures for Administrative Law Enforcement by Cyberspace Departments (Draft for Comment) (国家互联网信息办公室关于《网信部门行政执法程序规定（征求意见稿）》公开征求意见的通知)

Outbound Data Transfer Security Assessment Measures (国家互联网信息办公室令) (Effective 1 September 2022)