


China's Cybersecurity Law



Companies operating in China should take swift actions now to assess their specific obligations under the CSL and other related regulations and adopt a comprehensive approach to mitigate the compliance risks.

China's Cybersecurity Law

China's new Cybersecurity Law (CSL) was passed November 7, 2016, and came into force June 1, 2017. As the nation's first comprehensive privacy and security regulation for cyberspace, the CSL imposes paradigm-shifting requirements such as data localization. Together with a dozen other related legislations, guidelines, and industrial standards already released or being drafted, the CSL will present an unprecedented challenge for international businesses with operations in China.

The path to CSL compliance is not straightforward. The Chinese legislative and enforcement style creates confusion and misunderstandings, and sometimes false hopes, for Western companies. Despite this environment of uncertainty and change, the Chinese authority has already begun initiating enforcement actions for CSL violations. The same is expected when the data localization provision goes into effect on December 31, 2018.

The over-reaching scope of the CSL

The CSL applies to "Network Operators" and operators of "Critical Information Infrastructure" (CII). The term "Network Operators," defined to include "owners, operators, and service providers of networks", may actually capture any companies providing services or operating business through a computer network, such as company intranets absent from further clarifications from the authority.

Operators of CII are subject to more stringent requirements. However, the scope of CII is equally broad, including companies in critical sectors such as radio, television, energy, transport, water conservancy, finance and public service, or other critical information infrastructure that "will result in serious damage to state security, the national economy and the people's livelihood and public interest if it is destroyed, loses function or encounters data leakage."

Data localization requirement

"Personal information" and "important data" collected or generated by CII operators in China must be stored in China. Although the CSL provides that the data localization requirement only applies to CII operators, subsequent draft implementation rules and guidance provide that Network Operators are also subject to data localization. When a Network Operator needs to transfer such data overseas, it must demonstrate the necessity of data export, and conduct a self-security assessment or submit to an official security assessment when a threshold test is met.

Revised draft guidance indicates that an official security assessment by the Chinese authorities would involve: (i) establishing a working group to conduct the assessment by way of "remote testing" and "on-site inspection," and preparing an assessment report; (ii) an expert committee appointed by the Cyberspace Administration of China (CAC) or sector regulators reviewing the report and providing recommendations on whether the proposed data transfer

shall be approved; and (iii) the CAC or sector regulators making a final determination.

The substantive criteria of security assessments is still under development. The current draft envisions a two-pronged test. The first prong, whether the transfer is “lawful, legitimate and necessary,” is a threshold requirement. The second prong evaluates the risks associated with the transfer by examining both the nature of the data being transferred and the likelihood of security breaches involving such data and the level of the impact of such incidents. Despite any surface resemblances to the GDPR, the CSL does not provide affirmative mechanisms such as BCRs and standard data protection clauses for a business to get approval. Nor does it provide any derogations present in the GDPR.

Data compliance requirements

In addition to data localization and security assessments, Network Operators are required to comply with various other measures related to cybersecurity and personal data protection.

Network Security

- **Designate security personnel** – Appoint personnel responsible for network security (Article 21)
- **Implement security protocols** – Establish internal security management systems according to a tiered network security protection system guideline (to be released by the State Council) (Article 21)
- **Adopt appropriate technological measures** – Adopt appropriate technologies to investigate, prevent and combat cyberattacks (Article 21)
- **Establish complaint-reporting procedure** – Disclose how a security complaint can be reported, establish and implement the reporting procedure (Article 49)

Personal Data Protection

- **Consent** – Obtain consent before collecting personal data, the collection of which must be related to the services of the Network Operator (Article 41)
- **Notice** – Explicitly state the purpose, means and scope of the collection and use of personal data (Article 41)
- **Breach notification** – In the event of a data breach, notify the affected individuals, report the breach to the relevant government departments and take remedial actions (Article 42)
- **Data access** – Delete or amend personal data on users’ request (Article 43)

Content Monitoring

- **Monitor user content** – Monitor content published by users (Articles 46-47)

- **Remove illegal content** – Remove unlawful user content (Article 47)
- **Record and report** – Report unlawful content to authorities and keep records (Article 47)

CII operators are required to engage in similar cybersecurity practices as Network Operators, along with some additional requirements, such as ensuring network products and services that might affect national security shall go through a security review (Article 35).

Supply chain accountability

Important network products and services that may implicate China’s national security and their supply chain will be subject to a security review by the sector regulator to ascertain whether they are “secure, controllable, and transparent.” The term “secure and controllable” has not been formally defined, but appears to be understood by commentaries to mean preference of domestic products with backdoor access to the government over foreign products and technologies. Sector regulators will assess supply chain security risks associated with all stages of the life cycle of products, and their key components.

Enforcement so far

The CAC, the primary authority charged with supervising and enforcing the CSL, has been focusing its enforcement effort on user-content monitoring pursuant to Articles 47-48 of the CSL as part of the effort to “clean up” the Internet. Already, the Chinese government has imposed maximum fines on technology giants operating in China for failing to adequately censor banned user content on their websites, such as pornography, violence, and politically harmful content.

Furthermore, the government has indicated that it will conduct a targeted review of the privacy policies of selected Internet and mobile products/service providers, many of which are recognized business leaders in China. Articles 40-50 of the CSL set forth obligations of Network Operators in collection, use, disclosure and processing of personal information.

The CSL is also being enforced at the local level. The local branches of the Ministry of Industry and Information Technology (“Public Security Bureau” or PSB) have also begun investigating incidents involving violations of Article 21 requiring, *inter alia*, adoption of measures based on assigned security grade and keeping of logs for six months or more.

Penalties

The CSL provides monetary, criminal and operational penalties for failure to comply. For instance, under Article 66, companies that violate data localization may face fines of between RMB 50,000 and 500,000 (~ USD 7,500 – 75,000),

the closure of websites or revocation of business licenses or permits. Additionally, personnel directly in charge can be individually fined between RMB 10,000 and 100,000 (~ USD 1,500 – 15,000). Finally, Network Operators may be subject to five to 15 days of detention for violating certain provisions (Articles 63, 67).

Other related (draft) laws and guidelines

Interpretations on several issues concerning the application of law in the handling of criminal cases involving infringement of citizens' personal information (effective June 1, 2017): clarifies the scope of Article 253 of the PRC Criminal Law (amended in 2015) imposing criminal sanctions on anyone who, in violation of relevant state rules, sells or discloses personal information without an individual's consent. For example, Article 9 mandates that any network service provider who fails to manage network security and refuses to make corrections as ordered by authorities, causing serious breaches of personal information, shall be sentenced to criminal detention or fixed-term imprisonment of no more than three years, concurrently or separately subject to a fine.

The administrative provisions on mobile Internet applications information services (effective August 1, 2016): applies to mobile app stores and providers, requiring, *inter alia*, providers to satisfy six requirements to operate in China, including the need to verify a new app user's identity; to report to the relevant government agencies, users whose published content violates laws; and to record user logs and keep them for at least 60 days.

The administrative provisions on Internet information search services (effective August 1, 2016): requires, *inter alia*, search service providers and mobile app providers to monitor user content for improper content such as violence, terrorism, fraud or pornography.

Draft Encryption Law: if adopted, will be the first Chinese statute governing encryption. China's State Cryptography Administration (SCA) is authorized to oversee investigations of encryption-related incidents. Telecom and ISPs are required to provide decryption support for the purposes of national security and criminal investigation and to keep such cooperation confidential.

Decision on removing a batch of administrative approval requirements (September 22, 2017): no longer requires approval of using foreign-made commercial encryption products by foreign entities and individuals in China. However, importing the limited types of foreign-made encryption hardware listed in the catalogue issued by the SCA and China's General Administration of Customs still requires approval.

Draft e-commerce law: requires e-commerce operators (defined to include companies doing business on their own website, e-commerce platform providers and stores operating on the e-commerce platforms) to comply with the CSL. Obligations include, *inter alia*, content monitoring for IP violations, fraud and false advertisement.

Draft information security standards: provides guidance on how to fulfill security obligations imposed by the CSL and others, even though the standards are voluntary and not legally binding. The set was released by China's National Information Security Standardization Technical Committee (NISSTC) covering: (i) personal information, (ii) cybersecurity, (iii) big data, (iv) certain devices and (v) industrial control systems.

Draft regulation for the protection of the CII: provides guidance on the duties and obligations of an operator of CII. For example, CII operators must cooperate with the CAC in cybersecurity information sharing and allow sector regulators to conduct cybersecurity inspections and assessment when needed.

The three-step path to CSL compliance



- 1 Conduct a CSL compliance-risks assessment with a focus on content monitoring, IT procurement, and cross-border data transfer
- 2 Conduct in-depth data due-diligence for new or existing mission-critical business operations in China
- 3 Conduct a comprehensive data audit of the China operations

Contact us



Xiaoyan Zhang
Counsel
San Francisco
+1 415 659 5957
xzhang@reedsmith.com

Xiaoyan is counsel in Reed Smith's IP, Tech & Data Group's San Francisco office. Xiaoyan has more than 15 years of combined legal and high-tech industrial experience. Xiaoyan advises clients extensively on privacy and cybersecurity issues in Asia, in particular, China's new Cybersecurity Law, as well as cross-border technology transactions with China. She also advises clients on IP and cybersecurity and privacy-related issues in complex technology and outsourcing transactions involving e-commerce, licensing, and emerging technologies, such as cloud, AI and block chain.



Ariana Y. Goodell
Associate
San Francisco
+1 415 659 4739
agoodell@reedsmith.com

Ariana's practice focuses on cybersecurity and data privacy counseling for clients in sectors such as technology, apparel, and medical device. Ariana has counseled clients on a variety of data privacy and cybersecurity issues, such as corporate governance, cross-border data transfers including Privacy Shield, regulatory compliance with U.S. privacy laws and global privacy laws including the GDPR and China's new Cybersecurity Law and negotiating data processing and other technology-related agreements.



Maytak Chin
Associate
San Francisco
+1 415 659 5937
mchin@reedsmith.com

Maytak Chin is a member of the Complex Litigation Group with diverse expertise in trade secrets litigation, pre-litigation issues and governance matters. Maytak counsels her clients on a wide range of matters, including on compliance and cybersecurity issues for cloud-based services. Her litigation experience lends a keen eye towards identifying areas of potential liability and methods for remedying the risk.

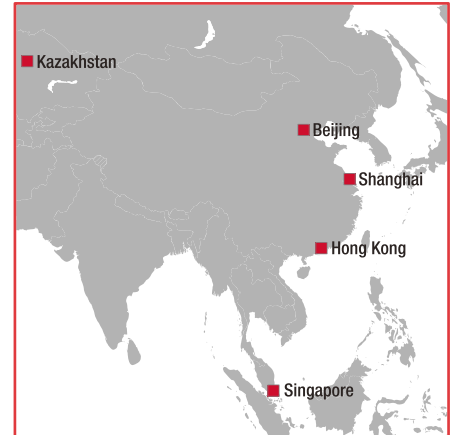


Cong Liu
Associate
Shanghai
+86 21 6032 3127
cong.liu@reedsmith.com

Cong focuses her practice on corporate and commercial matters in China, including foreign direct investments, cross-border mergers and acquisitions, trade finance privacy and cybersecurity issues, and internal investigations. Cong also has experience in handling Foreign Corrupt Practices Act (FCPA) and other compliance matters.

Reed Smith is a dynamic international law firm, dedicated to helping clients move their businesses forward.

Our long-standing relationships, international outlook, and collaborative structure make us the go-to partner for speedy resolution of complex disputes, transactions, and regulatory matters.



This document is not intended to provide legal advice to be used in a specific fact situation; the contents are for informational purposes only. "Reed Smith" refers to Reed Smith LLP and related entities. © Reed Smith LLP 2018

ABU DHABI
ATHENS
BEIJING
CENTURY CITY
CHICAGO
DUBAI
FRANKFURT
HONG KONG
HOUSTON
KAZAKHSTAN
LONDON
LOS ANGELES
MIAMI
MUNICH
NEW YORK
PARIS
PHILADELPHIA
PITTSBURGH
PRINCETON
RICHMOND
SAN FRANCISCO
SHANGHAI
SILICON VALLEY
SINGAPORE
TYSONS
WASHINGTON, D.C.
WILMINGTON

reedsmith.com