Teneo

The Global CEO Advisory Firm

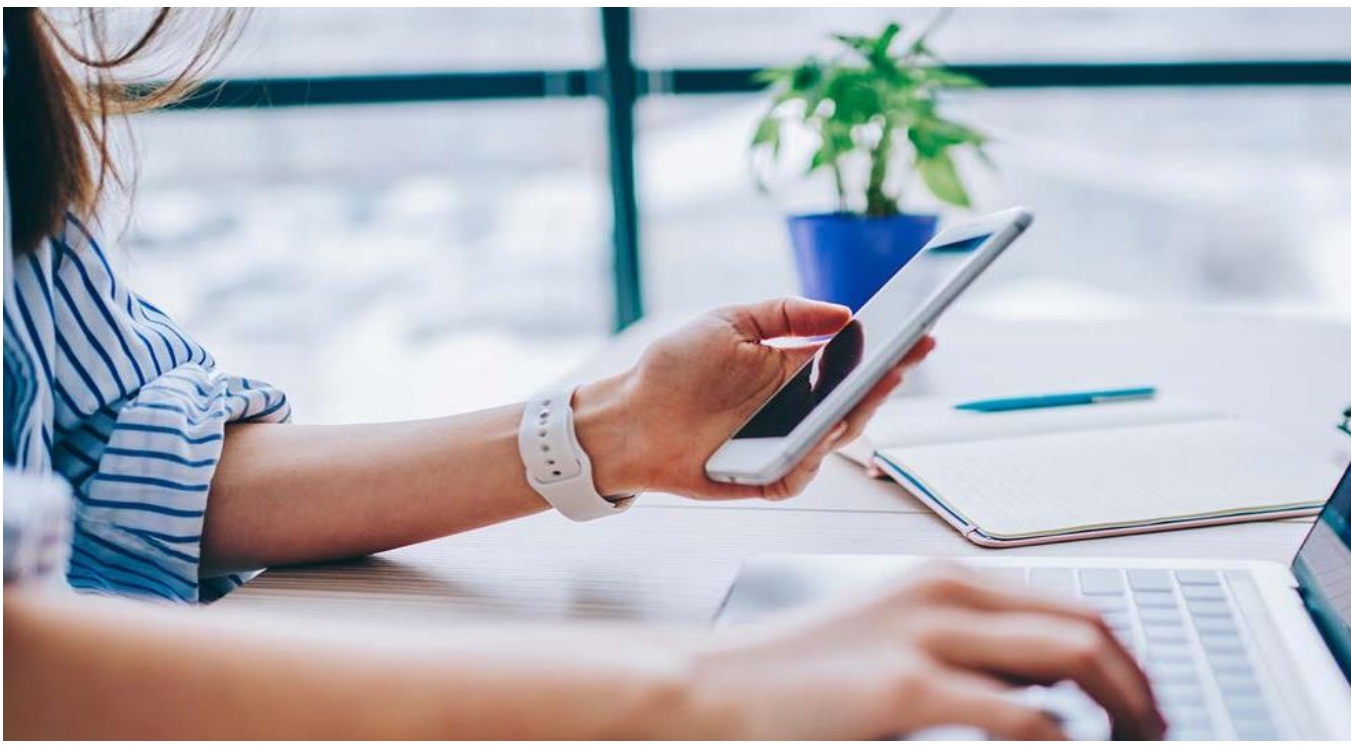
China Cybersecurity and Data Regulation: What Multinationals Should Know

October 2021

China implements a troika of cybersecurity and data regulation laws

Multinational firms operating in China currently face a heightened degree of uncertainty. The trade war between the US and China continues unabated despite the change in the US administration and China continues to clamp down on its tech giants while also implementing a wide range of regulations aimed at limiting the actions of large corporations across sectors. These sources of uncertainty are interconnected, and the implications can be far reaching.

This paper provides an overview of how ongoing geopolitical tensions between China and the US have manifested in the cyber and data policy arenas, highlights key provisions of China's three cybersecurity and data regulation laws – two of which have been implemented and one pending – and explores key considerations for multinationals operating in the market. It concludes with recommendations for how these companies can position themselves to minimise risk in this complex environment.



Geopolitical tension, cybersecurity and data regulation collide

Longstanding geopolitical competition between the US and China entered new territory in 2017, when the Trump administration in the US signalled a new hard-line policy that manifested in a tit-for-tat trade war of escalating sanctions and countersanctions. Against this background, cybersecurity and data emerged as a key field of battle.

As the trade war escalated, China implemented a sweeping cybersecurity law in June 2017 aimed at domestic cyber data management and online security. This was followed by a series of US laws with extraterritorial reach. In March 2018, the US implemented the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), which authorises US law enforcement agencies to demand access to online information wherever it is stored.

While the CLOUD Act suggests that the US intends to regulate cyber and data activities overseas in line with US interests, it was regulatory moves in August 2020 that really caught global attention. On 5 August 2020, the Trump administration implemented the "Clean Network" program, which excludes the Chinese telecom giant Huawei from 5G infrastructure networks in the US and in allied countries and territories that joined the program based on national security grounds. This was followed quickly by a 6 August 2020 executive order that essentially banned Tik Tok in the US on national security grounds, mandating that the service's US operations be sold to a "friendly" operator.

China countered with the September 2020 launch of the "Global Initiative on Data Security". The initiative – which does not carry the force of law but was drafted to contribute "Chinese wisdom to international rules-making in this area"[1] – lays out eight principals in areas such as personal data protection, overseas data practices by multinationals, data storage and cross-border data security.

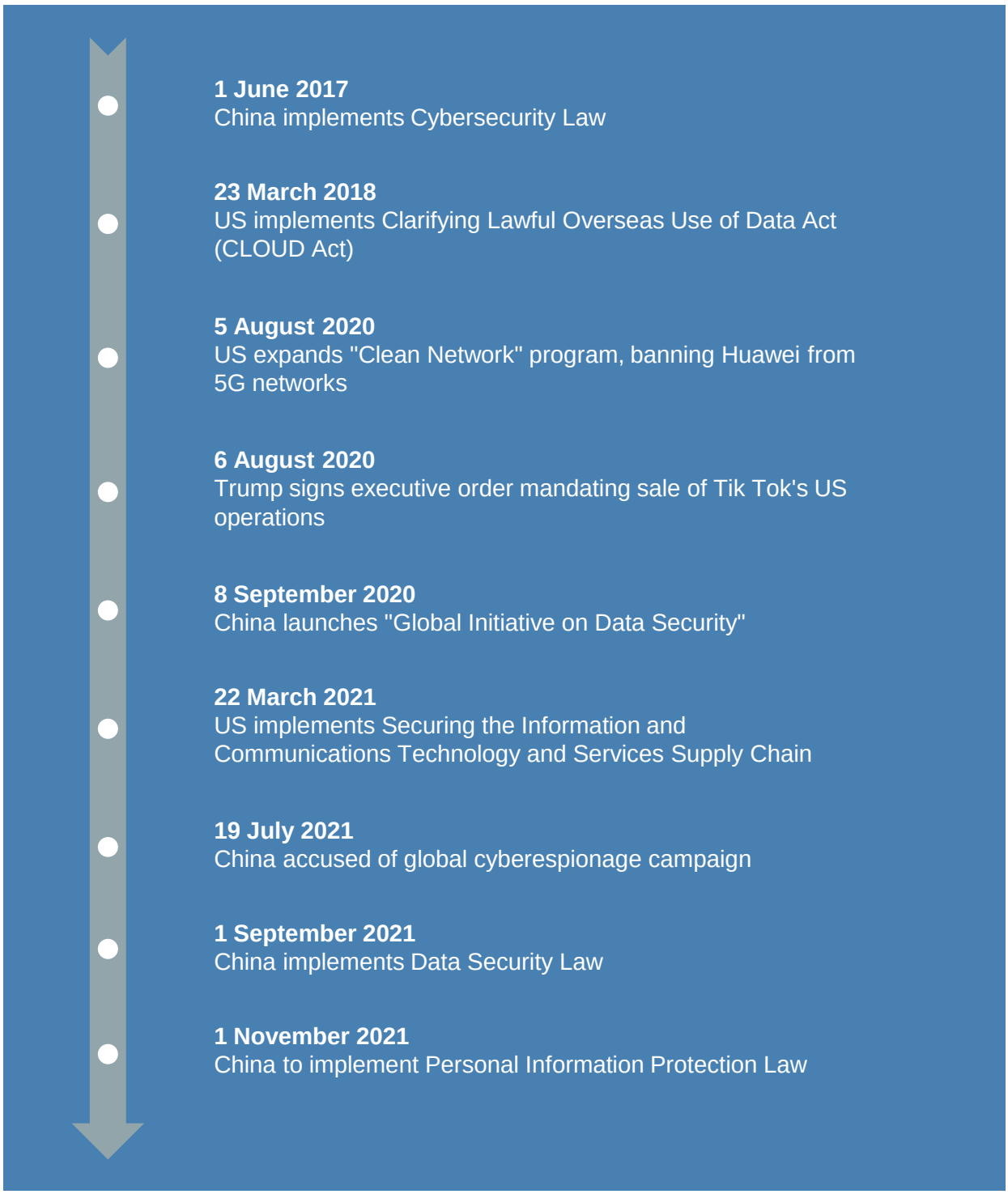
As President Biden took office in January 2021, China watchers wondered what the new administration would mean for US-China relations. The answer was soon clear, with the new administration doubling down on a hardline China policy.

In March 2021, the Biden administration's Department of Commerce implemented Executive Order 13873 on Securing the Information and Communications Technology and Services (ICTS) Supply Chain, which calls for oversight of all cross-border transactions that include infrastructure related to areas such as financial services, energy and agriculture and software, hardware or services related to communications or sensitive personal data. This was followed in July 2021 by accusations from the US and its allies that China was engaged in a widespread global cyberespionage campaign that included the Microsoft Exchange hack. China responded with a claim that "the United States is the world's largest source of cyber-attacks".

1. http://https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1812951.shtml
2. www.xinhuanet.com/english/2021-07/20/c_1310072999.htm

China has since made significant progress in implementing a comprehensive regulatory framework via a troika of cybersecurity and data regulation laws that comprise the aforementioned Cybersecurity Law; the Data Security Law which came into effect on 1 September 2021 and the Personal Data Protection Law that will take force from 1 November 2021.

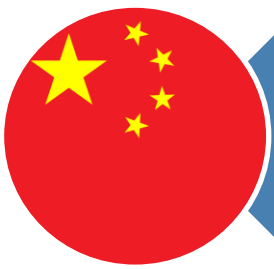
Figure 1: Key US-China cybersecurity and data regulation milestones



Global landscape: Approaches to cybersecurity and data regulation differ by jurisdiction

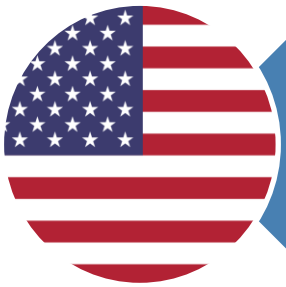
With lines drawn and the US and China waging a policy conflict in the areas of cybersecurity and data management, it is worth taking a step back and reviewing the key differences between approaches to these areas in global markets. Figure 2 highlights the policy approaches to cybersecurity and data management in China, the US and the European Union (EU).

Figure 2: Key global cybersecurity & data regulation priorities



Regulatory focus: Prevent private companies from accessing users' data and strengthen government oversight

Legislative progress: Cyber Security Law (1 June 2017); Data Security Law (1 September 2021); Personal Data Security Law (1 November 2021)



Regulatory focus: Scrutinise commercial use and sale of data as a commodity while facilitating corporate use of data

Legislative progress: CLOUD Act (23 March 2018); Securing the Information and Communications Technology and Services Supply Chain (22 March 2021)

Regulatory priority: Protect privacy and individual rights against encroachment by companies and governments

Legislative progress: EU Cybersecurity Act (27 June 2019)

China cybersecurity and data regulation policy roundup

Against this backdrop of escalating regulatory action, multinational companies operating in China or doing business with related companies or individuals should be aware of the implications of the key laws governing cybersecurity and data management in the region. This section takes a closer look at the three key regulatory regimes already in play or coming into force in China – the Cybersecurity Law, the Data Security Law and the Personal Information Protection Law. See Page 14 for more details on the government agencies in charge of cybersecurity and data regulation compliance.

It is important to note that the below sections highlight key points of these laws and should not be considered legal advice on regulatory requirements or implications.

Cybersecurity Law — Effective: 1 June 2017

Overview:

- Focuses on cyber data management and security, but does not regulate other forms of data
- Covers data that originates in China, any data imported from overseas and activity that compromises China's cyber infrastructure

Applies to:

- Telecommunications and network owners and operators
- Service providers, including those who deliver information via networks
- Infrastructure operators
- Domestic or overseas individuals or organisations

Key requirements:

- Regularly review cybersecurity and data management to ensure critical risks are addressed
- Regularly review protection of private information in the course of collection, use and dissemination
- Carefully monitor data being transmitted out of China or received from overseas
- Establish defined roles with clear responsibility for cybersecurity and data privacy
- Monitor networks in real time and establish incident reporting processes
- Establish and regularly practice crisis/incident response plans

Enforcement:

- Under the purview of the Cybersecurity Administration of China, the Ministry of Industry and Information Technology and the Ministry of Public Security
- Potential regulatory action includes fines of up to RMB1 million, business suspension and/or revocation of business license

Data Security Law — Effective: 1 September 2021

Overview:

- Covers a wide range of data, including online and offline data storage and processing
- Classifies data under three categories based on its sensitivity and relevance to matters such as the economy and national security: 1) core state data; 2) important data; and 3) general data
- Establishes a National Security Review system to identify data activities with implications for national security
- Classifies data operators as: 1) operators of critical information infrastructure (CII) for important industries and sectors; and 2) non-CII operators

Applies to:

- All private and public data collection, storage and processing in China
- Private and public data collection, storage and processing outside of China that could harm the nation's national security, public interest or the rights of Chinese citizens or entities

Data Security Law (con't)

Key requirements:

- Comply with all requirements in the 2017 Cybersecurity Law, including local storage of data collected or generated in China
- Establish data security management systems to safeguard data
- Hold regular data security training sessions for staff
- Conduct regular data security risk assessments
- Implement mechanisms for identifying and notifying relevant parties of data security risks and/or breaches of data security
- Individuals and entities must secure government permission before providing data stored in China to any foreign law enforcement agency

Enforcement:

- Under the purview of the Ministry of State Security, the Ministry of Public Security and the Cybersecurity Administration of China
- Business fines ranging from RMB1 million to RMB10 million depending on the severity of the effects of the data law violation
- Individual fines ranging from RMB10,000 to RMB2 million
- Potential business suspension and/or revocation of business license

Personal Information Protection Law — Effective: 1 November2021

Overview:

- Covers the collection, processing and protection of personally identifiable information both online and offline

Applies to:

- Any individual or entity processing personal information in mainland China
- Overseas institutions processing personal information overseas related to product or service offerings in China or analysing the behaviours of individuals in China
- State entities

Key requirements:

- Users of information must prominently inform individuals in plain language who is using the data, contact information, why and how data will be used and the rules that will govern its use
- Data processors must obtain consent to use from fully informed individuals or the legal guardian of an individual under 14 years of age and may not deny products or services to individuals who do not provide consent
- Entities using personal data are liable for breaches of the PIPL on their part or on the part of third parties that they provide data to
- Personal data can be retained only for the shortest period necessary to meet the needs of the services being provided
- Personal data must be deleted if the individual withdraws their consent to use the data, the entity no longer provides the products or services for which the data was collected or the data is no longer required for the original purpose it was obtained
- Before transferring personal data across borders, data processors must: 1) pass a state security assessment; 2) sign contracts to ensure overseas use of the data will not violate the PIPL; and 3) ensure compliance with all other relevant data laws

Enforcement:

- Under the purview of the Cybersecurity Administration of China
- Fines of up to RMB50 million or 5% of the previous year's turnover

Cybersecurity and data regulation in action

The three cybersecurity and data regulation laws are part of a trend of Chinese authorities rationalising the nation's relevant legal framework and stepping up enforcement.

Over the past few years we have seen a stream of enforcement actions under laws regarding antitrust, unfair competition, consumer rights protection and now data security. In this section, we look at a few high-profile incidences of regulatory action specifically targeting data security. These cases predate the implementation of the Data Security Law, so they cannot be cited as a direct example of the law in action, but are still instructive.

The highest profile case to date has been the action against Didi Global, the variable interest entity owned by Didi Chuxing, China's largest ride hailing service. The day after its 2 July 2021 US IPO, the Chinese Administration of Cyberspace (CAC) announced the results of its review of Didi. The Didi case is noteworthy for Chinese and international companies, as it is the first time Beijing has specified that a review was in response to national security concerns.

Didi continues to operate in China while addressing the regulatory review findings, but its apps have been removed from app stores to prevent new client acquisition.

While the Didi case is domestic in terms of enforcement, international investors and partners have already suffered collateral damage – the company's share price has declined significantly since the regulatory decision was announced, erasing billions in shareholder value.

That said, the extraterritorial nature of the three cybersecurity and data regulation laws suggest that it is only a matter of time before a foreign-owned multinational company falls afoul of the rules. The only high-profile case to date that has included a multinational company regards data security scrutiny of electric carmaker Tesla.

On 19 March 2021, the Chinese military banned the use of Tesla cars by all employees and barred Tesla cars from entering military facilities due to concern over the data being collected by on-board cameras and sensors. On 12 May, the CAC issued regulations governing automobile data security management, stipulating that personal data should be stored safely and car owners should be able to access it. Tesla responded on 25 May, announcing that it would open a new data centre to store domestic customer data in China. BMW, Daimler and Ford quickly followed with announcements that they will also set up data centres in China to comply with the CAC directive.

Both of these cases can be interpreted within the framework of the three cybersecurity and data regulation laws, and are indicative of the regulators' intentions. From this perspective, it is instructive that both examples represent direct action against companies that deliver mass-market products and services, and thus can be interpreted as safeguarding the cybersecurity and data interests of the general public.

Cybersecurity and data regulation in action

Prior to the 2017 enactment of the Cybersecurity Law, China's approach to cybersecurity and data regulation could be characterised as piecemeal; there were numerous pieces of regulation, legislation and non-binding guiding documents related to these issues. With that in mind, China has undertaken a concerted effort over the past four to five years to develop a legal framework for dealing with cybersecurity and data regulation that aligns these piecemeal rules.

What has resulted is a comprehensive framework comprising the three laws discussed above – the Cybersecurity Law, Data Security Law and Personal Information Protection Law – which codify approaches to cybersecurity, electronic and other forms of data, corporate data practices and the treatment of personal data. While some of the provisions in these laws are open to interpretation, and we will have to wait and see how regulators and the court apply the laws and judge offenders, there are certain key takeaways for multinationals. The following page outlines key considerations for multinational companies across a range of operational considerations.

Key China cybersecurity and data regulation law considerations for multinational corporations

	Immediate	Near term	Longer term
Strategy	Conduct an **in-depth review** of the three laws to determine and plan for their relevance to operations in China and globally.	**Implement cybersecurity and data management policies** that meet the requirements for operations in China and abroad.	Ensure **strategic planning** fully incorporates the implications of the three laws, with particular emphasis on risk management.
Operations	**Establish clear responsibility** for complying with cybersecurity and data management regulations and form action teams to address needs.	**Ensure the letter of the three laws are addressed**, including data residency, data transmission and cybersecurity requirements.	**Revise IT policies and adjust infrastructure** to meet legal needs, including how data centres are used and establishing systems to track and manage data retention.
Employees	**Communicate the implications** of the laws clearly to employees and make them aware of where internal responsibility for compliance rests.	**Establish education programs** to meet the training needs specified in the laws.	**Incorporate cybersecurity and data management law requirements into corporate culture** and consider factoring into employee review criteria.
Supply Chain & Partners	**Undertake a comprehensive supply chain and partnership audit** to identify all aspects that are subject to the laws and highlight potential challenges.	**Develop supply chain and partnership policies** that reflect domestic and international implications and engage directly with each third-party to address requirements and mandate compliance.	**Include cybersecurity and data management as key criteria** in supply chain management and the evaluation and selection of partners across markets.
External Relations	**Clearly and publicly communicate** that cybersecurity and data management are being treated as important issues and show alignment with the law.	**Actively engage with regulators, the community and professional organisations** to evaluate and address cybersecurity and data management concerns.	**Track and document compliance measures** to show alignment with the laws if questions arise. Also consider participating in related government and industry consultation exercises, conferences or events.
Investor Relations	Conduct an **in-depth review** of the laws and proactively highlight risks and opportunities for investors. Show investors that risk management processes reflect the implications of the laws.	**Evaluate legal requirements and update risk disclosure filings** with regulators and exchanges as necessary to show compliance.	**Communicate cybersecurity and data management practices in disclosure documents** such as the annual report.

China government agencies in charge of cybersecurity and data regulation law compliance

Cyberspace Administration of China (CAC)

Also known as the Office of the Central Cyberspace Affairs Commission, the CAC is both a government organisation and a department of the Chinese Communist Party (CPC). Therefore, the CAC has power over all ministries when it comes to cybersecurity and data regulation.

The CAC is responsible for all work related to cyberspace administration, including information dissemination, promoting the building of a relevant legal framework and providing guidance, coordination and supervision for all Internet-related content management. The CAC is also the supervisor of State Council ministries responsible for telecommunications network operation, access server providers and IP distribution management. It is the most important government stakeholder for the cyberspace administration and security management.[3]

Of China's three cybersecurity and data regulation laws, CAC plays a role in oversight of the Cybersecurity Law, the Personal Data Protection Law and the Data Security Law (at the general data security level).

Ministry of Industry and Information Technology (MIIT)

MIIT is responsible for planning for, monitoring of and guidance on the development of major infrastructure and technical equipment and for promoting the development of the information technology and telecommunication industry.

MIIT's role in cybersecurity administration mainly involves the building of network infrastructure for telecoms and the internet; assessing and encouraging new technology use; reviewing and administering relevant network market access and providing guidance for industry development. MIIT was responsible for cyberspace security administration before this responsibility was re-assigned to CAC in 2015. Now MIIT serves a supporting role in areas of national data and information security but remains a key stakeholder in relevant industries.[4]

Of China's three cybersecurity and data regulation laws, MIIT plays a role in oversight of the Cybersecurity Law.

3. Description translated and paraphrased based on: http://www.cac.gov.cn/2014-08/01/c_1111903999.htm
4. Description translated and paraphrased based on: https://www.miit.gov.cn/gyhxxhb/jgzz/art/2020/art_4a8ec0f5dc754b30be418107d0de6c1b.html

Ministry of Public Security (MPS)

The MPS is the lead department in charge of public security within China. Its responsibilities include the investigation and enforcement of illegal activities that impact industries such as food and drugs, finance, transportation, cyberspace, etc. It is also involved in addressing crime, terrorism, drug and narcotics abuse and related illegal activity, among other areas. The MPS plays a key role in cyberspace security administration as it carries out data tracking, runs investigations and undertakes any other enforcement-related work.[5]

Of China's three cybersecurity and data regulation laws, MPS plays a role in oversight of the Cybersecurity Law.

Ministry of State Security (MSS)

MSS is known as the secret service department of the State Council. It is mainly in charge of espionage/counter-espionage. Its involvement in cybersecurity covers the high-security investigations and relevant planning and strategic guidance.[6]

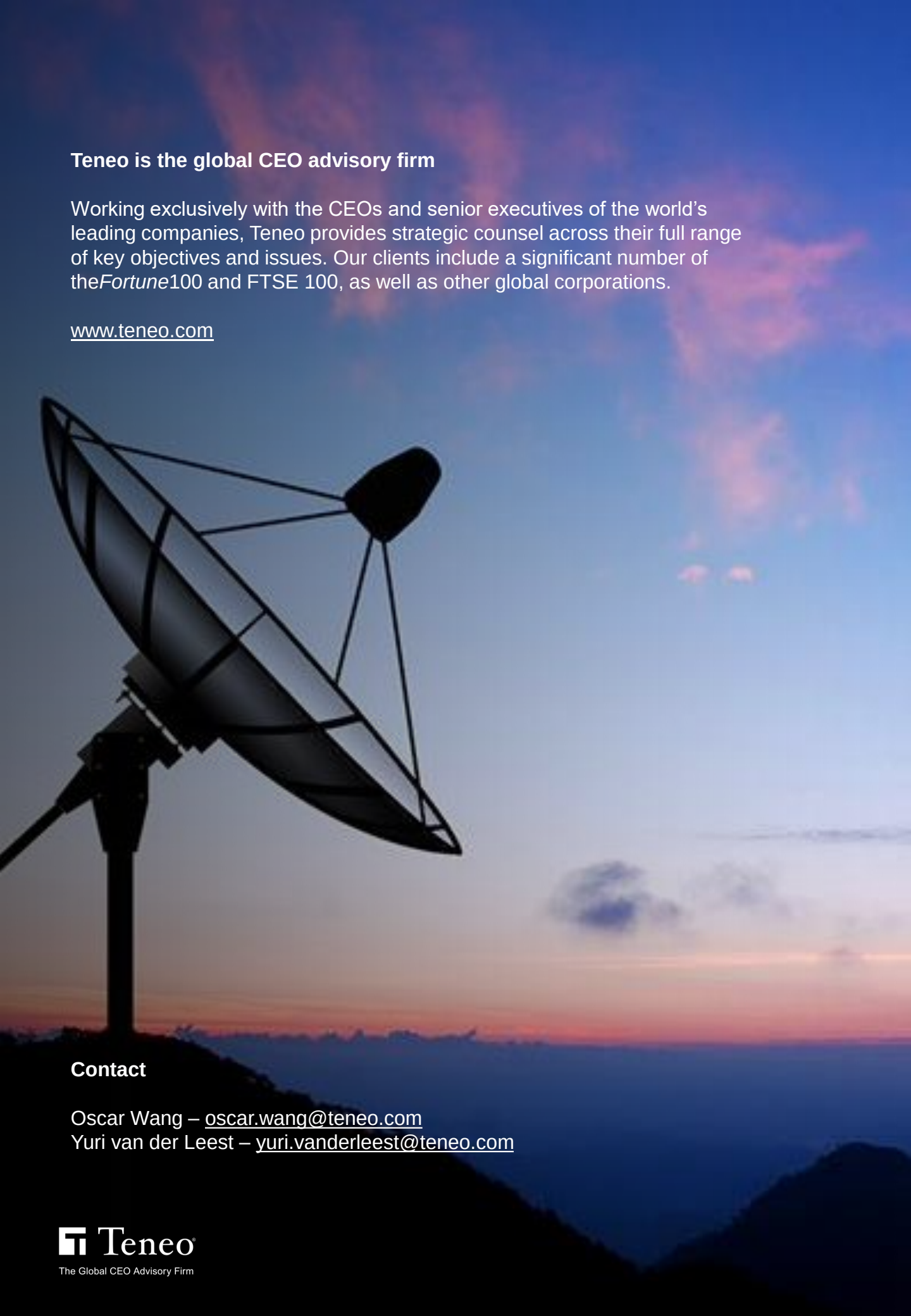
Of China's three cybersecurity and data regulation laws, MSS plays a role in oversight of the Data Security Law (at the national security level). That said, multinational companies with questions or issues related to the three cybersecurity and data management laws are recommended to reach out to other responsible agencies rather than reaching out directly to the MSS.

Sector-specific Oversight

In addition to the above agencies, specific ministries in China are responsible for oversight and application of the three cybersecurity and data regulation laws within their relevant sectors:

- Ministry of Transport
- Ministry of Finance
- China Banking and Insurance Regulatory Commission
- China Securities Regulatory Commission
- Ministry of Natural Resources
- Ministry of Education
- Ministry of Science and Technology
- National Health Commission

5. Description translated and paraphrased based on: www.mps.gov.cn
6. Description translated and paraphrased based on: https://baike.baidu.com/item/%E5%9B%BD%E5%AE%B6%E5%AE%89%E5%85%A8%E9%83%A8/56671164?fr=aladdin



Teneo is the global CEO advisory firm

Working exclusively with the CEOs and senior executives of the world's leading companies, Teneo provides strategic counsel across their full range of key objectives and issues. Our clients include a significant number of the*Fortune*100 and FTSE 100, as well as other global corporations.

www.teneo.com

Contact

Oscar Wang – oscar.wang@teneo.com
Yuri van der Leest – yuri.vanderleest@teneo.com

Teneo
The Global CEO Advisory Firm