Morrison & Foerster Client Alert

September 16, 2014

A Brave New World?

Recent Challenges Facing Foreign IT Companies in China

By Gordon Milner, Paul McKenzie and Jing Bu

On September 1, 2014, China's Ministry of Industry and Information Technology (**MIIT**) issued the *Guiding Opinions on Strengthening Network Security in the Telecommunications and Internet Sectors* (《关于加强电信和互联网行业网络安全工作的指导意见》; the "**Opinions**"). Issuance of the Opinions is merely the latest in a series of developments evidencing an increased focus by Chinese regulators on network security, as well as a growing distrust of foreign technology and foreign IT companies (**FITCs**). This client alert briefly summarizes the main provisions of the Opinions and discusses more broadly the current regulatory and policy environment in China for FITCs.

The Opinions seek to clarify how MIIT will interpret and enforce existing Chinese telecommunications regulations governing network security. Like many Chinese laws, the telecommunications regulations are drafted using very broad language that leaves significant scope to the regulator to set implementation policies. As such, although they do not technically constitute new laws, the Opinions do, in effect, establish new rules, conditions and enforcement policies that are likely to impact FITCs doing business in China. The Opinions focus on strengthening network security in both private and public infrastructure. Amongst other things, the Opinions:

- require bid invitation documents for the procurement of key software and hardware to expressly stipulate network security requirements;
- regulate the security aspects of the collection, storage, use and destruction of users' personal information; and
- encourage mobile app stores to establish and improve systems to verify the identity of app developers and to test the security of apps in order to identify and blacklist malicious applications.

Please see the Appendix for further detail regarding the content of the Opinions.

UNITED STATES

California

Tiffany Cheung	(415) 268-6848
Peter Day	(650) 813-4231
Rebekah Kaufman	(415) 268-6148
Christine E. Lyon	(650) 813-5770
David F. McDowell	(213) 892-5383
Purvi G. Patel	(213) 892-5296
Andrew Serwin	(858) 720-5134
William L. Stern	(415) 268-7637
Nancy R. Thomas	(213) 892-5561
David M. Walsh	(213) 892-5262

New York

Cindy Abramson	(212) 336-4178
Melissa Crespo	(212) 336-4354
John F. Delaney	(212) 468-8040
Michael B. Miller	(212) 468-8009
Sotirios Petrovas	(212) 336-4377
Suhna N. Pierce	(212) 336-4150
Marian Waldmann Agarwal	(212) 336-4230
Miriam H. Wugmeister	(212) 506-7213

Washington, D.C.

Patrick Bernhardt	(202) 887-8771
L. Richard Fischer	(202) 887-1566
Adam J. Fleisher	(202) 887-8781
D. Reed Freeman, Jr.	(202) 887-6948
Libby J. Greismann	(202) 778-1607
Julie O'Neill	(202) 887-8764
Cynthia J. Rich	(202) 778-1652
Andrew M. Smith	(202) 887-1558
Nathan David Taylor	(202) 778-1644

EUROPE

Berlin

Hanno Timner	49 30 72622-1346

Brussels

Joanna Łopatowska	32 2 340 7365
Karin Retzer	32 2 340 7364
Alja Poler De Zwart	32 2 340 7360

London

Ann Bevitt	44 20 7920 4041
Amy Collins	44 20 79204180
Susan McLean	44 20 79204045

ASIA

Beijing

Paul D. McKenzie	86 10 5909 3366

Hong Kong

Gordon A. Milner	852 2585 0808

Singapore

Daniel P. Levison	65 6922 2041

Tokyo

Toshihiro So	81 3 3214 6568
Yukihiro Terazawa	81 3 3214 6585

BACKGROUND

Issuance of the Opinions appears to be part of a broader focus by Chinese regulators on network security, which comes at a time of growing distrust of foreign technology and FITCs. This policy appears to have arisen, at least partly, as a response to the revelations regarding security agency activities made by U.S. government contractor, Edward Snowden. The geopolitical climate may also have been exacerbated by the U.S. government's imposition of restrictions on products from Huawei, ZTE and other Chinese telecommunications equipment manufacturers and its indictment in May 2014 of five Chinese military officials for allegedly stealing American companies' trade secrets.

As a result, many leading FITCs are encountering market challenges in China. By way of example, in the last three months:

- PRC government procurement agencies have dropped Symantec's and Kaspersky's security software as well as certain laptop computers and other IT products from the U.S. from the list of technology permitted for government procurement, citing security concerns;
- China state owned enterprises (**SOEs**) have reportedly been prohibited by the Chinese government from procuring services from U.S. consulting companies[1];
- The use of Microsoft's Windows 8 operating system has been prohibited by the central government's procurement department, purportedly for security reasons; and
- The State Administration of Industry and Commerce has conducted raids on Microsoft's China offices alleging breaches of the PRC Anti-Monopoly Law in connection with "undisclosed compatibility issues in Windows and Office, in addition to bundling of software, and document authentication".

Much has been written about the obvious link between these developments and recent U.S. policy, with many commentators suggesting that the countries are engaged in a reciprocal "tit for tat" process. However, it is important to understand that, beyond the geopolitical headlines, there are clearly other factors that are driving developments in China, many of which predate recent tension in the China-U.S. relationship. In particular, China's twelfth "Five Year Plan" (2011-2015), which was approved by the National People's Congress in March 2011, specifically identifies network and information security as a key priority and focuses on domestic control over related hardware and software.

It is perhaps no coincidence that the current policy has coincided with the "coming of age" of a growing number of Chinese IT companies with strong technical capabilities and extensive political clout. Concerns over the security of foreign IT products have aligned with a desire to grow China's own IT industry and have been used as a justification for promoting indigenous Chinese technologies and vendors over those of FITCs. As a result, it seems likely that the new market reality has a degree of permanence and will outlive any geopolitical rapprochement between China and the U.S.

[1] There has been some debate as to whether the this purported exclusion is consistent with the commitments China made upon its accession to the World Trade Organization (**WTO**) that SOEs would "make purchases and sales based solely on commercial considerations" and that the Chinese government "would not influence, directly or indirectly, commercial decisions on the part of [SOEs]". Discussion of implications under WTO rules are beyond the scope of this Alert.

THE EXISTING REGULATORY ENVIRONMENT

One notable aspect of the recent news stories is that none of the sanctions, investigations and other government actions have involved new laws *per se*. Rather, as MIIT has done in the Opinions, the Chinese authorities have so far largely utilized powers and enforced restrictions under existing laws and used the tremendous leverage afforded by the domination of most key markets' large SOEs.

Chinese regulations already include specific security-related provisions that may see enhanced enforcement in the future. The most notable are the *Administrative Measures for the Graded Protection of Information Security* (信息安全等级保护管理办法; the "**Measures**") issued by the Ministry of Public Security (**MPS**) in 2007, which designate various grades of information systems and stipulate mandatory security measures applicable to each grade. Among other things, the Measures require that, for certain types of information systems, the developer or manufacturer of the information security products to be used in the systems must be incorporated in China as an independent legal person, and must be invested in or controlled by Chinese citizens, Chinese legal persons or the state; and the "core technology" and "critical components" of the information security products to be used in the systems are required to have "locally owned, independent" intellectual property rights.

With the kind of enhanced enforcement of existing regulations that the Opinions call for, FITCs operating in China would be well advised to review their compliance status even in the absence of any new laws.

POTENTIAL NEW LAWS

Not only enhanced enforcement of existing regulations but also promulgation of new laws and regulations governing network security may be in the offing.

For example, the State Internet Information Office of China (**SIIO**) announced on May 22, 2014 that China would adopt cyber security review rules in the "near term", which will require that all important technology products and services affecting national security or the public interest be subject to a "cyber security" review. The text of the announcement is not publicly available. As such, details as to both the scope of products and services subject to the review and the review standards and procedures remain unclear. Recent reports suggest that the following terms are likely to apply:

- **Scope**: All important IT products and services to be used in computer systems affecting national security or the public interest, including, for example, computer systems in the financial and telecommunications sectors, will be subject to the cyber security review, *whether produced by foreign or Chinese companies*. Reports suggest that products and services for use by the general public will not be subject to the cyber security review.
- **Subject Matter**: The security of and control over the technologies used in the applicable products and services will be the focus of the review. Reports suggest that it may be necessary to submit software source code for review. Further, non-technology aspects of the products and services, such as the background of the product manufacturers and the service suppliers, may also be subject to review. This aspect of the review would likely disadvantage FITCs.
- **Ongoing compliance**: A clearance issued to a product or service may be subsequently revoked if the authority changes its analysis based on additional facts.
- **Consequence**: Products and services that fail the review will be prohibited from being used in any Chinese computer systems related to national security or the public interest.

OPPORTUNITIES

Perhaps paradoxically, there remains an intense appetite in China for foreign technology to modernize domestic industries and China's growing middle class continues to present an extremely valuable potential market for FITCs.

It is clear from the recent spate of enforcement and investigation activities that a "business as usual" strategy may no longer be an effective or indeed safe approach to taking advantage of these opportunities. To this end, we are working with a number of major FITCs to develop new, more sustainable, approaches to business in China. These typically involve building a strong local image and demonstrating a commitment to China. Key strategies include:

- working with strategic SOEs;
- showing "skin in the game" by investing in an onshore joint venture with a Chinese partner;
- bringing higher tier technologies to China; and
- avoiding discriminatory pricing practices.

KEY TAKE-AWAYS

(1) FITC businesses in China have been subject to greatly increased regulatory scrutiny and government intervention. Much of this has been implemented through a more proactive stance toward the enforcement of existing rules – which means that FITCs operating in China would be well advised to review their compliance status even in the absence of any new laws.

(2) The new regulatory environment may have been triggered by recent geopolitical events, but it is likely to continue notwithstanding any political rapprochement.

(3) Domestic Chinese technology companies are rising in prominence and are likely to be favored under the evolving regulatory regime. In order to compete effectively, FITCs may need to review how their businesses are structured in China with a view to building confidence in the local market.

For more information about our people and services and the resources we offer such as our treatise setting out the U.S. and international legal landscape related to workplace privacy and data security, "*Global Employee Privacy and Data Security Law,*" or our free online Privacy Library, please visit: http://www.mofo.com/privacy--data-security-services/ and "like" us on Facebook at http://www.facebook.com/MoFoPrivacy.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.

APPENDIX

Summary of *Guiding Opinions on Strengthening Network Security in the Telecommunications and Internet Sectors* (《关于加强电信和互联网行业网络安全工作的指导意见》工信部保[2014]368号); the "Opinions", issued by China's Ministry of Industry and Information Technology (MIIT) on September 1, 2014.

MIIT issued the Opinions to its local branches, telecommunications carriers, the National Computer Network Emergency Response Technical Team/Coordination Center, MIIT's Telecommunications Research Academy, Guiding Center of Vocational Ability Identification of MIIT, China Association of Communications Enterprises, Internet Society of China, domain name registration management entities and "other relevant entities".

The Opinions observe in an introductory paragraph that great strides have been made in responding to official calls to emphasize construction of network infrastructure and to accelerate the development of the online economy, but network security remains a major concern. They highlight issues such as the increasing frequency of network attacks both domestically and from abroad, the increasing sophistication of network attacks and problems with network security introduced through new technology and business models. Challenges in assuring network security that the Opinions identify include underdevelopment of security systems and mechanisms, the inadequacy of technological capabilities, and a low level of security and controllability of key hardware and software. The Opinions include as goals improving security of telecommunications infrastructure as well as business networks, increasing technological capability relevant to network security, strengthening protection of network data and user information, and promoting the application of secure and controllable key hardware and software.

The Opinions then set out eight key tasks and five compliance measures, as summarized below.

1. **Key Tasks**

   a) ***Strengthening the security of network infrastructure and business systems***: The Opinions call for enhanced implementation of MIIT's 2010 *Measures for the Administration of Communication Network Security Protection* (《通信网络安全防护管理办法》), and related standards, including in relation to the grading of computer information systems and conduct of risk evaluations of computer information systems. They also require that a clear responsibility system be established so that it is evident which department or individual is responsible for security of a computer system.

   b) ***Improving network security emergency response capability***: The Opinions call for enhanced implementation of MIIT's 2009 *Emergency Response Plan for Public Internet Network Security* (《公共互联网网络安全应急预案》) and exhort recipients of the Opinions to formulate and periodically review network emergency plans and coordinate responses to network emergencies.

   c) ***Protecting security environment of the Internet***: The Opinions call for enhanced implementation of MIIT's *Trojan Horse and Botnet Monitoring and Response Mechanisms* (《木马和僵尸网络监测与处置机制》, issued in 2009) and *Mobile Internet Malware Monitoring and Response Mechanisms*《移动互联网恶意程序监测与处置机制》, issued in 2011) and establish mechanisms for monitoring and dealing with phishing websites. Measures the Opinions contemplate include maintenance of relevant databases, cooperation with law enforcement in regard to online crimes and inclusion of clear duties of users in regard to network security in websites' terms of use.

d) ***Promoting application of secure and controllable hardware and software***: The Opinions call for adoption of a national network security review mechanism. The Opinions also state that, as required by MIIT's 2014 *Measures for the Administration of Bidding for Telecommunications Construction Projects* (《通信工程建设项目招标投标管理办法》) in projects for procurement of key hardware and software, network security should be considered and bid documents should be specific about security requirements.

e) ***Strengthening protection of network data and users' personal information***: The Opinions call for enhanced implementation of MIIT's 2013 *Provisions on Protection of Personal Information of Telecommunications and Internet Users* (《电信和互联网用户个人信息保护规定》). The collection, storage, use and destruction of "personal information" shall be in strict compliance with applicable personal information protection regulations.

f) ***Strengthening security management of mobile app stores and apps***: The Opinions call for enhanced security management of applications and application stores. The application store operators shall establish the systems for application developer identity verification, application security review, removal of malicious applications, and customer complaint response services.

g) ***Strengthening network security management of new technologies and new business models***: The Opinions call for improvements in respect of research on, and risk evaluation of, the network security of new technologies and new business models, such as cloud computing, big data, the Internet of things, mobile Internet and next generation Internet.

h) ***Improving the capability to maintain network security***: The Opinions call for further research and development of advanced network security technologies.

2. **Compliance Measures**

a) ***Establish closer supervision and inspection of network security***: The Opinions call for closer supervision and inspection of telecommunications enterprises by regulatory authorities. The Opinions promote the establishment of network security certification systems for telecommunications and Internet industries.

b) ***Increase role of industry associations and professional institutions***: The Opinions call for the increased role of industry associations and professional institutions in enhancing network security. Industry associations and professional institutions are encouraged to issue industry guidelines on network security and provide professional training to industry players.

c) ***Implement enhanced corporate responsibility***: The Opinions call for greater corporate responsibility on the part of basic telecommunications companies, value-added telecommunications companies and domain name registration and management entities to enhance network security. These entities are called upon to improve network security systems and allocate sufficient human resources for relevant work.

d) ***Increase more capital investment***: Basic telecommunications companies, value-added telecommunications companies and domain name registration and management entities must increase their capital investment in network security systems in order to keep pace with technology and with their business development.

e) ***Build a stronger professional team***: The Opinions call for the building up of stronger professional teams by basic telecommunications companies by way of introducing professional certification and license systems for network security professionals and providing on-the-job professional training.