



Llinks Corporate and M&A Bulletin
January 2019

上海
上海市银城中路 68 号
时代金融中心 16 楼和 19 楼
邮编: 200120
电话: +86 21 3135 8666
传真: +86 21 3135 8600

北京
北京市建国门北大街 8 号
华润大厦 4 楼
邮编: 100005
电话: +86 10 8519 2266
传真: +86 10 8519 2929

香港
香港中环皇后大道中 5 号
衡怡大厦 27 楼
电话: +852 2592 1978
传真: +852 2868 0883

伦敦
1F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

www.llinkslaw.com

SHANGHAI
16F/19F, ONE LUJIAZUI
68 Yin Cheng Road Middle
Shanghai 200120 P.R.China
T: +86 21 3135 8666
F: +86 21 3135 8600

BEIJING
4F, China Resources Building
8 Jianguomenbei Avenue
Beijing 100005 P.R.China
T: +86 10 8519 2266
F: +86 10 8519 2929

HONG KONG
27F, Henley Building
5 Queen's Road Central
Central, Hong Kong
T: +852 2592 1978
F: +852 2868 0883

LONDON
1F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

master@llinkslaw.com

Is it legal to bypass great firewall?

By Xun Yang

The Shaoguan Public Security Bureau of Guangdong Province has recently imposed an administrative fine of RMB1,000 on an individual who bypassed the great firewall, based on the accusation of violating Article 4 and Article 10 of the *PRC Provisional Rule for International Connection of Computer Networks* (the “**Interconnection Rule**”), that prohibits the establishment and use of illegal communication channels.

The news triggered hot discussions. Some companies, including, in particular, multinational companies concerned their own practices to bypass the great firewall. I feel pleased that my various legal advices given to multinational companies regarding this subject since early this century when I focused my practice on cyber security matters always identified the legal risks associated with bypassing the great firewall and pointed out the ways to mitigate the risks.

Nowadays, the government has strengthened the administration over cyber security. And as a result, the legal risks associated with bypassing the great firewall are increasing. However, the legal principles remain unchanged, that is, the use of VPN for the

如果您需要本出版物的中文本,
请与下列人员联系:

郭建良: +86 21 3135 8756
Publication@llinkslaw.com

For more Llinks publications,
please contact:

Roy Guo: +86 21 3135 8756
Publication@llinkslaw.com

Llinks Law Offices
www.llinkslaw.com

Is it legal to bypass great firewall?

connection to servers outside of China itself is not illegal but adoption of certain technical measures and managerial measures are advisable to control the risks arising from the connection to the internet from overseas incidental to the use of VPN.

I. Legal requirements under the Interconnection Rule

Generally speaking, the Interconnection Rule imposes the following two requirements on the international connection of computer networks.

- (1) The connections to overseas computers must go through an export channel permitted by the China government; and
- (2) The connection to internet must go through an access network permitted by the government.

Among the two requirements, the first one is usually complied with: generally speaking, if a connection is provided by one of the “Three Big Carriers,” the international connection goes through an export channel permitted by the China government. VPNs which multinational companies may lease for connecting its China entities with their overseas companies are also constructed on the export channels permitted by the China government. Only in rare situations some companies build up connections by themselves through subscriptions for overseas connection services.

The second abovementioned requirement prohibits the so-called “bypassing the great firewall.” This requirement demands that a connection to internet go through an ISP recognized by the China government and via an access network operated by it. As a result, the ISP is able to block visits to illegal websites which fall within the government’s blacklist. This requirement reflects national sovereignty in the cyber space. The connection to the internet through an access network outside of China violates this requirement.

II. Attitudes of various government agencies towards bypassing the great firewall

Generally speaking, the public security bureaus take a serious approach towards bypassing the great firewall. And their enforcement of the laws is increasingly strengthened. The industrial and telecommunication bureaus take a relatively relax attitudes towards bypassing the great firewall.

The Interconnection Rules was issued as early as 1996 but there is only few cases decided based on it. Thus, the activities of bypassing the great firewall are considered connivance for a long period of time. This situation has been changing since 2012 when the government started paying much attention to cyber

Is it legal to bypass great firewall?

securities. Consequently, there are an increasing number of cases involving bypassing the great firewall.

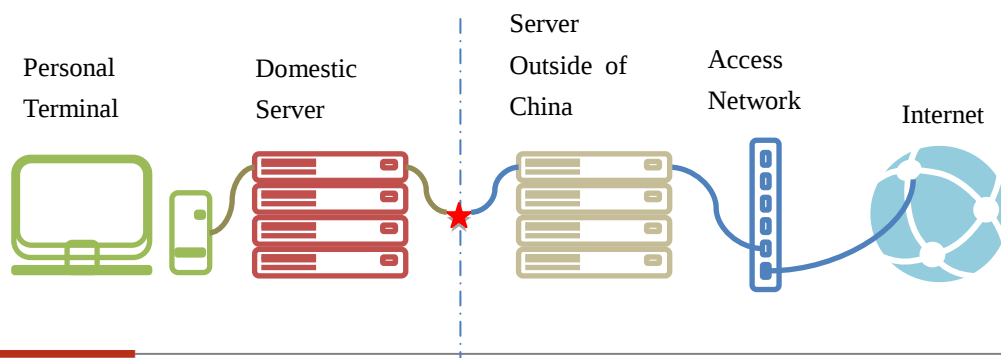
From the point of view of the industrial and telecommunication bureaus, according to the *Notice on Further Regulations on Internet Data Center Business and Internet Service Provision Business* issued in 2012, and the *Notice on Clearance on Internet Network Access Service Market* issued in 2017, the focus of their enforcement is to prohibit illegal operations of internet access business and other cross-border network connection business. These regulations, however, do not prohibit companies from using VPNs for its own business and management purpose. They remain silence as to whether the use of internet connection function incidental to use of VPN is considered legitimate.

From the point of view of the public security bureaus and the procuratorate offices towards the use of VPN and the bypass of the great firewall, they have clearly strengthened enforcement against illegal sales and provision of VPN since 2012. During prosecutions, they accuse these activities either as: (1) illegal operation, or (2) provision of programs and tools to facilitate intruding into or illegal control over computer systems. The first accusation is obvious. The latter suggests that the use of VPN may be considered intruding into or legal control over computer systems. Fortunately, up to now, there is no person who has ever been criminally convicted for the use of VPN.

The abovementioned administrative penalty imposed on individual for its bypassing the great firewall is, as far as I know, the first case where an individual is penalized for bypassing the great firewall. This may indicate that the public security bureaus have strengthened the enforcement against behaviors of bypassing the great firewall.

III. Practical issued for multinational companies

As I understand, many multinational companies, due to business reasons, integrate their IT systems to the global systems by connecting their local servers to their regional or global servers. The IT structure is illustrated below.



Is it legal to bypass great firewall?

Multinational companies adopt such IT structure due to the following reasons: (1) to share information and resources internally; (2) to visit companies' private cloud or to manage their business on cloud; (3) to speed up the visits to overseas websites; and (4) to allow China based personnel to visit some blocked websites due to business reasons. Obviously, this IT structure does not satisfy the requirements under the Interconnection Rule because it enables China-based personnel to connect to the internet through access networks outside of China.

In reality, the government must have knowledge about the existence of this IT structure. However, as far as I know, there is no company which has ever been penalized merely for adopting this IT structure, because companies usually have legitimate business reasons to use such structure.

IV. Practical suggestions

Although, there is no multinational company which has ever been penalized for adopting the abovementioned networking structure, considering the increasing strengthened cyber security legal regime, some companies have been taking measures to adjust its IT practice and to revise its IT structure in order to mitigate its risks. These measures include:

- (1) To build up dual channels for internet connections for domestic employees (or most of the domestic employees): with respect to domestic employees, companies block the internet connecting functions through its servers outside of China, and provide a separate connection to internet through a domestic access network.
- (2) To set up internal gateway screening: some companies voluntarily block the access to illegal or sensitive websites by taking reference to China government's "black list" and taking into consideration the companies' own information security requirement (which will likely be a more important reason), or provide access only to websites which are necessary for the business.
- (3) To establish internal management systems, to formulate IT usage manuals and to provide routine trainings, which require that employees only use the networks in compliance with the PRC law requirements and that companies retain network operational logs according to the *Cyber Security Law*. As such, if an employee misuses VPN or the overseas connection to internet, the company will have a defense.

Is it legal to bypass great firewall?

Contact Details

If you would like to know more information about the subjects covered in this publication, please feel free to contact the following people or your usual Llinks contact.

Author	
Xun Yang Tel: +86 21 3135 8799 xun.yang@llinkslaw.com	
Shanghai	
David Yu Tel: +86 21 3135 8686 david.yu@llinkslaw.com	Bernie Liu Tel: +86 21 3135 8678 bernie.liu@llinkslaw.com
Selena She Tel: +86 21 3135 8770 selena.she@llinkslaw.com	Nicholas Lou Tel: +86 21 3135 8783 nicholas.lou@llinkslaw.com
Dali Qian Tel: +86 21 3135 8676 dali.qian@llinkslaw.com	Kenneth Kong Tel: +86 21 3135 8777 kenneth.kong@llinkslaw.com
David Wu Tel: +86 21 6043 3711 david.wu@llinkslaw.com	David Pan Tel: +86 21 3135 8701 david.pan@llinkslaw.com
Elyn Jiang Tel: +86 21 6043 3710 elyn.jiang@llinkslaw.com	
Beijing	
David Yu Tel: +86 10 8519 2266 david.yu@llinkslaw.com	Bernie Liu Tel: +86 10 8519 2266 bernie.liu@llinkslaw.com
Yuhua Yang Tel: +86 10 8519 1606 yuhua.yang@llinkslaw.com	
Hong Kong(in Association with Dennis Fong & Co., Solicitors)	
David Yu Tel: +86 21 3135 8686 david.yu@llinkslaw.com	Sandra Lu Tel: +86 21 3135 8776 sandra.lu@llinkslaw.com
London	
Yuhua Yang Tel: +44 (0)20 3283 4337 yuhua.yang@llinkslaw.com	