GPS Technology Quarterly

VPN Regulations and Implications for Business

February 2018

New data flow enforcement is impacting MNC's China operations

Regulators are imposing tighter control over internet services that many companies use to connect to outside of China, including VPNs and webservers. The operational impact of this development could impact:

- Access to local email via web pages
- Remote access to files and folders hosted on servers in China
- Connections between China offices and offices/data centers outside of China

Unlicensed services are being blocked

During the fourth quarter of 2017, in three eastern Chinese cities, two different national telecoms companies delivered letters to their Chinese and MNC customers explaining that without a proper license, all data traffic to specific ports[1] will be blocked. The letters also asked for multinational corporate customers to pledge that they would not use the internet to "violate the interests of the state."

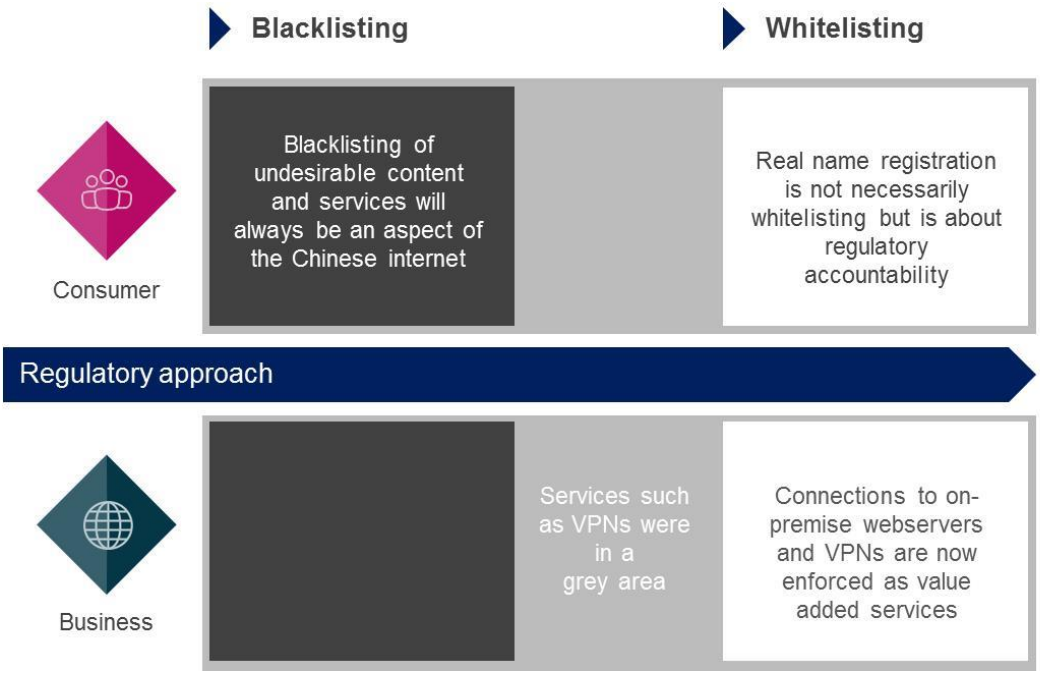
Control Risks spoke with some organizations regarding the sudden disruption of their on-premises web operations. In some cases telecoms providers did not give any advance warning. The application of the regulations (and blocking of data traffic) was only discovered when IT support teams contacted the telecoms provider as part of the troubleshooting process.

[1] These "ports", part of the addressing system for internet traffic, are those used by webservers to provide unencrypted (HTTP, port 80) and encrypted (HTTPS, port 443) access to a web site. Port 8080, often used by IT teams to support a secondary web service on a server, is also specifically mentioned in the letters.

Some companies reported the blocking of their cross-border IPSec VPN services[2] (a common corporate VPN) between their China locations and offices/data centers abroad. This was initially expected to be short term disruption, timed to coincide with the 19th Party Congress. However, the problems have persisted and align with the planned closing of certain ports.

Rules are moving from grey to white

While enforcement of licensing requirements by telecoms companies is notable in of itself and the expected blocking of site-to-site VPNs is a long-dreaded further tightening of China's internet controls, this development is consistent with China's overall objectives in controlling information flows and the technologies that deliver it.



China's regulatory framework specific to VPN and website use has long been in place, but the rules were extremely vague with little to no enforcement. VPN use, therefore, was in the grey. It appears now, though, that the government is moving to a "whitelisting" approach. Whitelisting essentially bans everything that is not approved, registered, or reviewed by the government.

[2] IPSec (Internet Protocol Security – a collection of open source protocols) is a common technology to create and maintain a secure, encrypted connection between two locations such as a remote office and a data center. It uses UDP ports 500 and 4500 as channels over a network.

The Ministry of Industry and Information Technology (MIIT) is in charge of China's telecommunications sector. The following table outlines MIIT's key regulations governing VPN use:

Regulation / Development	Key Provisions
Administration of International Communications Gateway Exchange Procedures 国际通信出入口局管理办法 (2002, MIIT)	▸ This regulation differentiates between two different types of VPN use: ▪ VPN service to access to international networks must obtain approval from MIIT. ▪ VPN established for intranet access (such as corporate VPN use) be filed with MIIT.
Classification Catalogue of Telecommunications Services 电信业务分类目录（2015 年版） (2015, MIIT)	▸ VPNs are categorized as a Value Added Telecom service (VAT). ▸ The latest catalogue in 2015 lists VPNs as a Class I VAT, which is related to national security and thus extremely difficult for foreign companies to secure.
Notice on Cleaning Up and Regulating the Internet Access Service Market 工信部关于清理规范互联网网络接入服务市场的通知 (2017, MIIT)	▸ MIIT's notice for telecos to clean up unlicensed telecom operations, including VPNs, with an overall deadline of March 31, 2018. ▸ This notice is what is currently driving the telecos to require corporate compliance with existing regulations.
Cross-border Data Communications Services Policy Briefing Session 跨境数据通信业务政策宣贯会 Held by CAICT, China Telecom, China Mobile and China Unicom (January 2018)	▸ China Academy of Information and Communications Technology (CAICT) is a think tank under MIIT. They recently held a policy briefing with China's three major telecom providers on VPN developments where they stipulated: ▪ MNCs can rent directly within China, international dedicated lines (including VPNs) provided by the three basic telecommunications operators, to connect to their corporate networks and equipment. ▪ MNCs can rent directly from overseas international dedicated lines (including VPNs) provided by the three basic telecommunications operators, or commission an overseas operator to do so, to connect to their corporate networks and equipment.

What does this mean for companies in China?

Companies operating any kind of on-premises service accessible from the internet (e.g. websites, VPNs) should determine if the service is compliant:

- All on-premises web servers require an internet content provider (ICP) bei'an (ICP 备案) license.[3] This license is issued by MIIT and the local PSB, and must be registered by a Chinese national. A similar license is required for e-commerce websites (ICP Zheng, ICP 经营许可证). (see table)
- Established IPSec VPNs or software-defined wide area networking (SD-WAN)[4] should be considered "at-risk". They are likely to be blocked in the near future and may not be reliable for critical business functions.
- Clients now need to consider alternative connectivity solutions such as leased lines and MPLS. These will be provided directly or indirectly[5] by a local telecoms provider and should be appropriately licensed through the contracting process with the provider.
- While VPN connectivity over the internet in China is restricted, companies who wish to ensure the security of their wide area connections may wish to operate a VPN within the leased line/MPLS with an appropriate security architecture at both ends of the connection. Please note that while Control Risks is not aware of any disruption to these types of VPNs, they also could be potentially regulated in the future.
- While not currently a focus for regulators, companies should be vigilant for enforcement regarding internet access. Companies providing unrestricted internet access to employees and guests (via Wi-Fi, for example) may be considered by regulators as service providers, potentially making the company accountable.

[3] While this has been required for some years and is necessary for external hosting of a website, it is now definitively required for local hosting of web servers.

[4] SD-WAN solutions mimic the stability and functionality of conventional dedicated line wide area networks, but operate over local internet connections. While they are an effective and increasingly popular solution for companies, they still run over a network and whatever port they may use to establish and/or maintain a connection can be blocked.

[5] Irrespective of the contracting entity, all wide area networking solutions (leased lines, MPLS, etc.) are delivered physically and operated by a local Chinese telecoms company.

ICP registration to open ports 80, 8080, 443 ***NB: these procedures vary between regions*	
Agency	**Procedure**
Communication Administration (ICP)	1. Original copy of business license 2. ID of main responsible person 3. ID of responsible person of the website
Public Security Bureau (PSB)	1. Filling online application form on PSB website. After the form is submitted, PSB would determine if further detailed verification is needed.
Internet Service Provider (ISP)	1. Original copy of business license 2. ID and certificate of employment of legal person 3. Certificate of domain 4. Official stamp

Government Recommendations

On January 31, 2018, AmCham Shanghai and Control Risks held a briefing with members ranging from large multi-nationals to Small Medium Enterprises (SMEs) to discuss these developments and potential advocacy that AmCham can conduct with the Chinese government on the VPN issue. Recommendations include:

- The government should allow companies to keep established site-to-site VPNs, potentially by permitting corporations to file their site-to-site VPNs with the government as outlined per the International Gateway regulations. Mandatory use of dedicated lease lines is particularly burdensome for companies, both financially (costs run in the several thousand USD a year) and operationally (to set up and maintain the dedicated network infrastructure). This, in turn, may affect those companies' ability to appropriately manage the overall costs of their China operations.

- So that companies can ensure the continued operation of their businesses in China, the government should provide more details on which technologies for cross-border data connections are considered compliant with regulations; the application process to certify cross-border data connections; and which service providers are authorized to sell and support cross-border data connections.

- Corporations should be able to run VPNs on top of dedicated lease lines to secure their communications. The government should provide clarity on legal status of these VPNs.

About the Author

Control Risks is a specialist risk consultancy. Based in multiple offices on all continents, we are committed to helping our clients build organizations that are secure, compliant and resilient in an age of ever-changing risk and connectivity.

We believe that responsible risk taking is at the core of our clients' success. We have unparalleled experience in helping clients solve the challenges and crises that arise in any ambitious organization seeking to convert risk into opportunity globally. The insight and depth of experience we have gained over more than forty years proves invaluable in giving our clients the intelligence they need to grasp opportunities with greater certainty. Learn more at **www.controlrisks.com**.

For inquiries, please contact Jim Fitzsimmons (**Jim.Fitzsimmons@controlrisks.com**) or Carly Ramsey (**Carly.Ramsey@controlrisks.com**).

About the GPS Program

AmCham Shanghai's Government Policy Support (GPS) Program is dedicated to helping members navigate the impact of industrial policy on business. Drawing from the knowledge of industry experts in business, academia, and government, GPS provides members with the latest policy developments and valuable insights into how these translate into commercial opportunities and challenges for companies.

This report is the first in a series of quarterly reports available exclusively to GPS Program members. For more information, please contact **gps@amcham-shanghai.org**.