Baker McKenzie FenXun
奋迅 · 贝克麦坚时

Technology, Media & Telecommunications/ Data Privacy
China

Client Alert
October 2018

Ministry of Public Security issued rules on supervision and inspection internet security

Since the *Cybersecurity Law of the PRC* ("**CSL**") took effect in June 2017, the Public Security Bureaus (the police and security authority in China, "**PSB**") in many Chinese provinces and cities have been one of the most active government authorities in the enforcement of the CSL. Despite that many provisions of the CSL are too general and need to be detailed and clarified through implementation rules and regulations, many of which are yet to be finalized, the PSBs (mainly their Cybersecurity Protection Division or commonly known as the "Internet Police") have, by drawing upon the statutory powers and responsibilities stipulated under *the Law on People's Policy of the PRC* and other regulations and rules issued by the Ministry of Public Security Bureau ("**MPS**") concerning protection of security of computer network systems that became effective long before the issuance of the CSL and their extensive law enforcement organization and manpower across the country, rigorously (and in some instances, aggressively) taken enforcement actions on companies and individuals that violated the CSL. For instance, although the MPS issued the draft regulations concerning multi-level (cybersecurity) protection scheme ("**MLPS**") in late June of 2018 with the intent to implement the "new" MLPS proposed under the CSL, in some provinces and cities, the PSBs had referred to the 2007 version of the MLPS rules and required network operators located within their respective jurisdictions to conduct security protection certification. It was also reported that the PSBs in some cities investigated certain big data companies' allegedly "illegal" processing and sharing of personal information.

However, in the absence of updated and consolidated departmental rules issued by MPS, the enforcement powers of MPS under the CSL had been constrained. The lack of a clear delineation between the enforcement powers and regulatory authority of the MPS and those of other government authorities such as the Cyberspace Administration of China and the Ministry of Industry and Information Technology could also undermine the effective implementation and enforcement of the CSL. Hence, five months after the issuance of the draft version for solicitation of public comments, MPS finalized and issued the *Rules on Supervision and Inspection of Internet Security by Public Security Bureaus* on September 30, 2018 (the "**PSB Internet Security Rules**") which are aimed to provide guidance to the PSBs in respect of their supervision and inspection of the state of performance of cybersecurity obligations by "Internet service providers" and "units utilizing network". The start date for the implementation of the PSB Internet Security Rules will be November 1, 2018.

Who will be subject to PSBs' supervision and inspection?

Instead of referring to the broadly-defined terminology of "network operators" used under the CSL, the PSB Internet Security Rules state that "Internet service providers" and "units utilizing network" (which technically speaking will all be network operators for the purpose of the CSL) will be subject to the

Baker McKenzie FenXun
A Leading Chinese and International Law Joint Platform

For further information, please contact:

Zhenyu Ruan
Partner
+86 21 6105 8577
zhenyu.ruan@bakermckenziefenxun.com

PSBs' supervision and inspection. More specifically, the following "internet service providers" and "units utilizing network" are listed under the PSB Internet Security Rules:

(a) those that provide Internet access services, Internet datacentre (IDC) services, content delivery (CDN) services and domain name services;

(b) those that provide internet information services;

(c) those that provide Internet surfing services to the public; and

(d) those that provide other Internet services.

According to the *Rules on the Technical Measures for the Protection of the Internet Security* issued by MPS in November 2005 (the "**MPS 2005 Rules**"), "Internet service providers" shall mean the units that provide Internet access services, Internet datacentre services, Internet information services and Internet surfing services, and "units utilizing network" shall refer to units that connect to and use the Internet for its own application. By contrast, the PSB Internet Security Rules expanded the scope of "Internet service providers". In addition, as companies incorporated in China that intend to use servers or data centre connected with public communications network for service offering would generally need to obtain non-commercial ICP recordal pursuant to the regulations governing Internet information services, technically speaking, any entity holding non-commercial ICP recordal would be captured by the PSB Internet Security Rules.

The scope of the catch-all category of those that provide other Internet services remains to be clarified. For instance, it is not entirely clear if companies that operate "Internet of Things" or "Internet of Vehicles" type of business would fall within this category and therefore be subject to supervision and inspection by the PSBs pursuant to the PSB Internet Security Rules.

In terms of "units utilizing network", it seems that companies accessing the Internet only for its internal daily business activities would not fall within the ambit of the PSB Internet Security Rules. However, as such units utilizing network would still be considered network operators for the purpose of the CSL, legally, the PSBs would still have the power to supervise their state of compliance with cybersecurity protection requirements, but pursuant to the 2005 MPS Rules and the new MLPS regulations (once finalized and implemented by MPS).

Notably, as Chinese nationals are permitted to register and host websites, they are also subject to the PSBs' supervision and inspection in accordance with the PSB Internet Security Rules.

Which level of PSBs to take charge of internet security supervision and inspection?

PSBs of country-level and above will have the authority to take charge of internet security supervision and inspection in accordance with the PSB Internet Security Measures. In certain cities such as the four municipalities directly under the central government, the district-level PSBs are considered the equivalent of country-level PSBs and therefore have the authority to exert

the relevant supervision and inspection powers on the applicable companies domiciled within their districts.

Which areas of conducts will be subject to PSBs' internet security supervision and inspection?

PSBs shall have the authority to conduct supervision and inspection on "Internet service providers" and in-scope "units utilizing network" in respect of their compliance in terms of the following obligations imposed by the CSL:

(a) whether the recordal formalities for networking unit (i.e. the entity that connects to and utilizes the Internet) have been complied with and whether the basic information (and corresponding changes) concerning the unit providing Internet access and the user (i.e. the that connects to and utilizes the Internet) has been reported (to the competent PSB);

(b) whether systems for cybersecurity management and standards of operations have been formulated and implemented and whether person(s) responsible for cybersecurity has been designated;

(c) whether technical measures for recording and retaining users registration information and Internet access log data in a legal manner have been taken;

(d) whether technical measures to safeguard against computer virus, cyber attack, cyber intrusion, etc. have been adopted;

(e) whether measures have been adopted to prevent the publication or dissemination of information prohibited by laws and administrative regulations in the course of public information services (such as operation of any websites or apps that are publicly accessible);

(f) whether technical support and assistance have been provided in accordance with requirements imposed by laws to PSBs for defence of national security, prevention and investigation of terrorist activities or criminal investigation; and

(g) whether cybersecurity levelled protection obligations stipulated by laws and administrative regulations (i.e. requirements imposed by the CSL and the MLPS regulations) have been complied with.

Aside from these conducts that would generally be subject to supervision and inspection by the PSBs, depending on the specific type of Internet services involved (i.e. Internet access services, Internet datacentre services, content delivery services, domain name services and Internet surfing services to the public), the competent PSBs would also have the authority to inspect the state of compliance of specific conducts. In addition, during the time period involving major cybersecurity protection tasks for the State (e.g. during the annual plenary sessions of the National People's Congress or certain major national political events) or in the case of those units that are the key targets of terrorist attack, the PSBs may conduct specific security inspection on those Internet service providers and units utilizing network charged with the relevant tasks.

The PSB Internet Security Rules also provide that the PSBs may also conduct inspection on Internet service providers and units utilizing network as to whether a malicious program has been set up and utilized.

In addition, Internet service providers and units utilizing network under any of the following circumstances would be subject to heightened supervision and inspection by the competent PSBs:

(a) relevant (Internet) services having been commenced within a year;

(b) cybersecurity incident or law-breaking and criminal case having occurred in the preceding two years; and

(c) administrative penalty having been imposed by the PSB for failure to comply with the statutory cybersecurity rules and standards.

This last item means that if an Internet service providers or a units utilizing network was subject to penalty by the competent PSB for breach of cybersecurity protection requirements, it would then be subject to heightened scrutiny afterwards. However, it is silent under the PSB Internet Security Rules as to how long from the penalty decision such a company can be relieved of such heightened scrutiny.

It should be highlighted that while the compliance with data privacy requirements is not specifically listed as one of the conducts subject to supervision and inspection of the PSBs, whether or not an Internet service providers or a units utilizing network has stolen or otherwise obtained through illegal means personal information or illegally sold or illegally provided personal information to others would also be subject to inspection and investigation by the PSBs. In this regard, Article 23 of the PSB Internet Security Rules replicates the second paragraph of Article 64 of the CSL by providing that these conducts discovered by the PSBs in the course of carrying out Internet security supervision and inspection but are not serious enough to constitute criminal offense, the PSBs would impose penalty in accordance with the CSL.

What methods of Internet security supervision and inspection can be carried out by PSBs?

In general, the PSBs may conduct (a) onsite inspection and check or (b) remote examination and check. The PSBs may designate cybersecurity service institutions with requisite technical capabilities to assist with onsite inspection and check as well as remote examination and check.

According to the PSB Internet Security Rules, the PSB may conduct remote examination and check in order to determine if cybersecurity vulnerabilities exist with an Internet service providers or a units utilizing network. In order to conduct remote examination and check, advance notification of the time and scope of the examination shall be notified to the relevant entity or be made public.

Due process such as preparation of records of inspection and check being conducted, signature of the records by at least two policemen and the technical assistance personnel of designated cybersecurity service institution involved, signature of the records by the in-charge person of the entity being

subject to inspection and check (in case of onsite inspection and check) is also provided for in the PSB Internet Security Rules.

The PSC Internet Security Rules specifically require that the PSBs and their relevant personnel as well as designated cybersecurity service institutions and their personnel involved in conducting the inspection and check must keep strictly confidential personal information, privacy, business secrets and national secrets obtained during the course of inspection and check, and must not divulge, sell or illegally provide the same to others or use such information for purposes other than protection of cybersecurity.

What are the administrative penalties for breach of the PSB Internet Security Rules?

As the PSB Internet Security Rules are, by nature, a piece of ministry-level departmental rules, the MPS does not have the authority to create and impose administrative penalties that are not specifically stipulated under the national laws. Hence, where the PSB concluded that a company failed to comply with the relevant cybersecurity protection requirements or where a company refused or obstructed the PSBs to conduct supervision and inspection, the competent PSB would have the authority to penalize such entity in accordance with the relevant provisions of the CSL or, where the conducts constituted violation of the *Counter-Terrorism Law of the PRC* (the "**CTL**"), in accordance with the CTL.

What are the implications to corporations?

On the face of the relevant provisions of the PSB Internet Security Rules, not all network operators would be subject to supervision and inspection of the PSB pursuant to the PSB Internet Security Rules. However, as "provision of Internet information services" are broadly defined under the relevant regulations concerning Internet information services and due to the regulatory requirements on use of server or datacentre connected to the public communications network in China, the PSB Internet Security Rules could still have a sweeping scope of application, and any corporation that has non-commercial ICP recordal would technically be captured. Even if a company does fall within the scope of the PSB Internet Security Rules, the PSBs will still be able to exert its powers on such company in respect of its cybersecurity compliance pursuant to the MPS 2005 Rules and the upcoming new version of the MLPS regulations.

Generally speaking, the PSB Internet Security Rules are more rules of administrative procedures to enable the implementation and enforcement of the CSL by the PSBs. Hence, MPS has not altered or significantly extended the cybersecurity related requirements stipulated under the CSL in the PSB Internet Security Rules. However, through the promulgation of the PSB Internet Security Rules, MPS does reiterate and clearly define the specific scope of powers and responsibilities of the PSBs in respect of the enforcement of the relevant requirements of the CSL.

We expect that once the PSB Internet Security Rules come into effect in November 2018, the local PSBs will gradually step up the implementation and enforcement of the relevant cybersecurity protection rules contained in the CSL. As some of the cybersecurity protection requirements will still largely depend on the specific rules and requirements to be detailed under the MLPS regulations, the issuance of the PSB Internet Security Rules could

be read to mean that the new version of the MPLS regulations will also soon to be finalized and issued by MPS.

Although the PSB Internet Security Rules provide that the PSBs shall give advance notice or otherwise publicize the proposed remote examination and check to determine the existence of cybersecurity vulnerabilities of particular entity(ies), we are aware of instances where the PSBs in some cities had not strictly followed such procedural requirements. It remains to be seen if the PSBs would strictly follow the procedural requirements stipulated under the PSB Internet Security Rules in conducting remote inspection and check.

www.bakermckenziefenxun.com
www.bakermckenzie.com
www.fenxunlaw.com

Baker McKenzie FenXun (FTZ)
Joint Operation Office
Unit 1601, Jin Mao Tower
88 Century Avenue, Pudong
Shanghai 200121, PRC

Tel: +86 21 6105 8558
Fax: +86 21 5047 0020