



NEWSLETTER

LIFANG & PARTNERS 立方观评

No.42
2016. 11

- ◇ Some Key Rules Set Out in the Latest Supreme Court Interpretations on the Application of China's Patent Law
- ◇ IP Protection at Trade Fairs in China
- ◇ A Comparative Study between Network Security Legislations in the US and China



Some Key Rules Set Out in the Latest Supreme Court Interpretations on the Application of China's Patent Law

INTRODUCTION

The Interpretations by the Supreme People's Court on Several Issues Relating to the Application of Law over Patent Infringement Disputes II (hereinafter as the Interpretations) was promulgated on March 22, 2016 and came into effect on April 1, 2016 (Interpretations I was released in 2009). The purpose is to fix various knotty issues that exist in current patent litigation disputes, such as lengthy time period, difficulties in obtaining proofs, and insufficient monetary damages. It is expected that the Interpretations will greatly impact the practice of patent litigation law.

The Interpretations focus on providing specific rules for the determination of the infringement as well as of the liabilities of the infringer, in order to ensure the appropriate application of the patent law and give consistency to court decisions.

This article will focus on four aspects of the Interpretations: 1) Principles applied to claim construction; 2) The provisions of "indirect infringement;" 3) Exceptions to injunctions; 4) Rules of evidence; and 5) A newly introduced practice of "dismiss and re-file of a lawsuit."

a. Claim construction shall combine protection for the patentee with certainty for third parties, with more stress on the defining power of the claims

Articles 5 through 12 of the Interpretations provide that, the extent of the patent protection is defined by the preamble section of the independent patent claims and all those features relating to product functions, use environment, preparation method, and modifier terms attached to numerical features.

Article 6 states, examination files of divisional patent applications and effective court decisions can be used to interpret the scope of patent protection. Patent examination files include two types: first, all written submissions made by the patent applicant or patentee in the course of the patent examinations, reexaminations, and validity reviews; second, written documents issued by the State Intellectual Property Office (SIPO) and the Patent Reexamination Board (the Board), e.g. office actions, minutes of meetings and hearings, effective decisions on requests for review and invalidation. A point worth noting is the inclusion of meeting and oral hearing records made out the patent administration authorities.

Article 7 focuses on close-ended claims for composition products. It affirms the past practice of the patent law and the provisions of the Guidelines for Patent Examination since 1993.

Article 8 defines "functional feature" and application of the doctrine of equivalents. In assessing whether a functional feature is identical with or equivalent to the patent claim, reference of time shall be the time when the alleged infringement occurs. In general, the Interpretations limit the effect of functional features by setting for a stricter standard, "performing the same function and achieving the same result with substantially the same means," than the general doctrine of equivalents that requires "substantially" the same function and "substantially" the same result.

b. Guideline in respect to "Indirect Infringement" leaves room for improvement.

Article 21 of the Interpretations, based on Article 9 of the Tort Law, clarifies two types of indirect infringing acts: first, one who knowingly, and for business purposes, provides to others materials, equipment, parts, intermediates, etc., which have a particular use for the implementation of a patent; second, one who knowingly, and for business purpose, actively induces others to infringe upon a patent. Regardless the types of the indirect infringement, it is not a strict liability tort. Indirect infringement can only arise when the accused indirect infringer has at least some knowledge and intent regarding the patent and the infringement. A patentee also needs to prove direct infringement to establish liability for indirect infringement.

As direct infringement is the precondition for establishing indirect infringement, in the case where the end user or reproducer of the patentee's a technical solution is not for production or business purposes, that individual or entity cannot be held liable for direct infringement; and thus, the inducer or contributor is not liable for indirect infringement either.

c. Exceptions to injunctions put restriction on a patentee's rights

With respect to injunction, the most common remedy in intellectual property litigation, the Interpretations provide two exceptions in articles 25 and 26 to prevent over-stretch of the patentee's monopolistic rights.

Article 25, built upon Article 70 of the Patent Law, and allows continuing use of the infringing products by "good faith users" who satisfy the following three conditions: 1) they are unaware that the products infringe upon other's patents; 2) they can prove the products come from legitimate sources; and 3) they can prove that reasonable consideration has been paid.

According to the previous Supreme Court interpretations released in 2009, "use" may cover the case where a product infringing upon a patent for invention or utility model is used as a component or part to manufacture another product. However, selling such other product constitutes as "infringing sale." ¹ Therefore, the

¹ Article 12 Where the products that infringe upon the patent right for invention or utility model are used as components and parts to manufacture another product, the People's Court shall hold that such act constitutes the use as prescribed in Article 11 of the Patent Law; where such another product is sold, the sale shall be held by the People's Court to constitute the sale as prescribed in Article 11 of the Patent Law.

“user” under Article 25 of the new Interpretations shall only “use,” but not “offer for sale or sell” infringing products to avoid a cease order.

Article 26 provides for the national interests and public interests exception where the defendant(s) may give reasonable compensation to the patentee, without discontinuance of what has been found as infringing acts.

d. The rules of presenting proof in determining the amount of damages are amended to redress difficulty in obtaining evidence and low award of damages.

Article 27 is a highlight of the Interpretations and a hopeful attempt to solve current problems relating to evidence submission and low compensation in patent litigation. It follows the basic principle that “the burden of proof is on him who claims” but provides for the transfer of such burden and lowers the standard of proof in special circumstances.

Pursuant to Article 27, if actual losses, caused to the claimant, are in dispute and difficult to be determined; claimant has presented preliminary evidence - includes, but not limited to, annual reports, marketing and publicity materials, and online transaction records - that the infringer gained interests from the infringement; and relevant financial documents are in the sole possession of the infringer, the court may order the infringer to disclose these documents. If the infringer refuses to oblige the court order without cause or provides false documents, the court can then calculate the infringer’s gains based on the arguments and evidences presented by the claimant, even if preponderance of the evidence has not been met.

e. “Dismiss and re-file” system is introduced to prevent lengthy litigation.

China has bifurcated proceedings for patent litigation. While infringement is determined by the courts, invalidity challenges are heard by the Patent Reexamination Board (the “Board”), but the Board decisions are subject to court

Whoever manufactures another product by using the products that infringe upon the patent right for industrial design as components and parts and sells the same shall be held by the People’s Court to constitute the sale as prescribed in Article 11 of the Patent Law, except that such products infringing the patent right for industrial design only have technical functions in such another product.

Under the circumstances as stipulated in the preceding two paragraphs, if there is division of labor and cooperation between the sued infringers, the People’s Court shall hold that such infringers have committed joint infringement.

review. This often leads to prolonged litigation shuttling between the Board and the court. However, as the chance is small for the court to overturn a Board decision (less than 20% as shown in a 2015 study report), Article 2 of the Interpretations states, court may directly dismiss a patent infringement case, if the involved patent is declared invalid by the Board. Should the Board decision be overturned in subsequent judicial review, the claimant can re-file a lawsuit against the alleged infringer. Though it may help reducing litigation length and costs, new framework in patent legislation is required to better fix the problem.

f. Conclusion

In addition to the above, other major issues are also covered in response to demands from judicial practice. For instance, Article 13 of the Interpretations improves application of estoppels; Article 18 specifies provisional protection period for invention patents; Article 24 provides for essential patents in recommendatory nationwide, local, and industry standards; and Article 14 introduces the “design space” concept into the assessment of infringement upon industrial design patents, to adjust the effect of varied attention given to different products by the average consumer.

To sum up, the Interpretations have addressed some salient issues in current patent law practice and are expected to have profound significance for the future.

---By Lifang Patent Team

IP Protection at Trade Fairs in China

In China, IP right holders may assert their rights in a variety of ways, including inter alia litigations, administrative complaints and Customs IP protection. This Article will focus in particular upon a less commonly known enforcement mechanism — the Exhibition Intellectual Property Protection (EIPP). As we shall see, the EIPP is a more straightforward and efficient means. It empowers IP right claimants to file a direct complaint with organizers of an exhibition and request a prominent protection against infringement or passing off.

What is EIPP

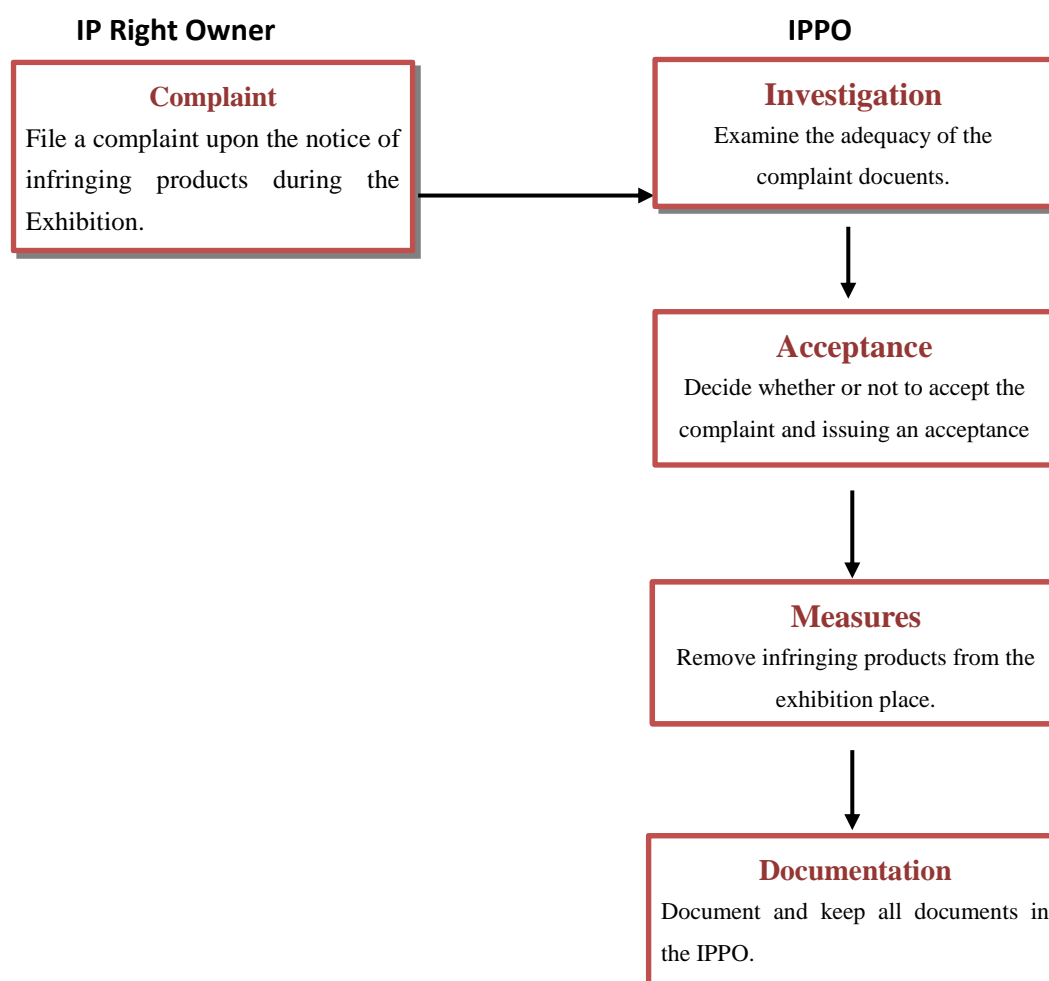
The EIPP is enshrined in the Protection Measures for Intellectual Property Rights (Measures) during Exhibitions, which was published and came into force on March 1, 2006. Following the Measures, local authorities issued their supplemental regulations in order that the EIPP can be implemented efficiently. The EIPP applies to the protection of patents, trademarks and copyrights in all kinds of exhibitions, including trade fairs, expositions, commodity fairs and trade shows (collectively “exhibitions”) that concern the economic and technical trade conducted in mainland China.

According to the EIPP, organizers of an exhibition or trade show shall strengthen the coordination, supervision and investigation in relation to the IPRs protection during the exhibition dates, and safeguard the legitimate rights and interests of IPR owners. Should an exhibition last for at least 3 days, an IP Protection Office (IPPO) must be set up inside the Exhibition venue. The IPPO will have to operate throughout the entire exhibition. It shall be composed of personnel from the organizer of the exhibition, the administrative department of exhibition, the local IPRs administrative department in charge of patents, trademarks and copyrights. The office is set to perform certain functions and duties, such as reviewing IPR complaints, investigating accused infringing products and exhibitors, and taking necessary actions to halt infringement activities in the exhibition.

Due to the structure of the IPPO, the EIPP is somehow considered as a special form of administrative complaint during the lifespan of an exhibition.

It is designed to provide efficiency and convenience for the IP owners. Below is a brief flowchart of the EIPP.

Flowchart of EIPP



Generally the complaint will be examined and processed swiftly whereas measures will be taken when the complaint is accepted. Thus, the use of EIPP offers immediate and effective protection of IP rights before the exhibition closes.

EIPP in China Import and Export Commodity Fair (Canton Fair)

Since its inauguration in 1957, the Canton Fair has emerged to be the most influential exhibition in China, known for having the longest history, highest level, largest scale, most complete kinds of products, broadest distribution and largest business turnover available to overseas buyers. The Fair is held biannually in Guangzhou in spring and autumn.

Due to its significance, more and more Chinese manufacturers attend the Fair for the purpose of showing, promoting or selling their products to international buyers. However, some products are suspects of infringement or passing-off disputes. In order to protect IP rights, the organizer of Canton Fair has implemented strict EIPP rules to investigate or raid booths of the exhibitors whose products are subjects of complaint. The measure has been a remarkable success. Table 1 below analyses the statistics of IP investigations and decisions made by the organizer of Canton Fair since 2010.

Table 1

| Canton Fair | Time | Number of IP Complaints | Number of Complained Exhibitors | Number of investigated infringers |
|--------------------|-------------|--------------------------------|--|--|
| No. 113 | April 2013 | 542 | 554 | 354 |
| No. 112 | Oct. 2012 | 484 | 671 | 336 |
| No. 111 | April 2012 | 386 | 504 | 233 |
| No. 110 | Oct. 2011 | 653 | 834 | 484 |
| No. 109 | April. 2011 | 616 | 826 | 486 |
| No. 107 | April 2010 | 639 | 829 | 530 |

An Example of EIPP Protection

We have represented numerous international companies and assisted them with the enforcement of IP rights in the Canton Fair. For instance, we advised a leading appliance UK-based company on the protection of its IP rights in the Canton Fair.

The company has had a worldwide phenomenal success with the novel appliances it develops. Naturally, the products are under global patent protection. In China, it has received tens of design, invention and utility model relevant to its bladeless fans.

The company noticed that products identical or similar to its designs and patents had been sold in Europe, America, Australia and other regions, and that a large percentage of the products were originally made in China. Retained by the company, we thoroughly reviewed the evidence and adopted a comprehensive IP protection strategy which includes both administrative and legal remedies. In view of the fact that the infringing products were made in China and exported to other countries, we decided to take advantage of the EIPP in Canton Fair so as to prevent those products from being introduced to overseas buyers. We filed complaints and requested the IPPO to inquire into the infringing products and expel them out of the Fair. This strategy has been proved of great success. Table 2 below shows our achievements in four consecutive Canton Fairs.

Table 2

| Fair session | Infringing exhibitors found | Complaints filed | Infringements confirmed |
|--------------|-----------------------------|------------------|-------------------------|
| 110th | 55 | 20 | 15 |
| 111th | 28 | 20 | 18 |
| 112th | 20 | 18 | |
| 113th | 9 | 7 | 7 |

Followed up with the EIPP actions, we delivered warning letters to the exhibitors whose infringement activities were confirmed and made certain settlements with them, whilst securing favourable results to the company. On the other hand, we initiated legal proceedings against 10 infringers. Evidence acquired through the EIPP actions contributed a great deal to our evidence lists.

Via the administrative EIPP protection and other legal channels, the number of infringers declined drastically. The company found that infringing products in international markets were on the decline.

Conclusion

Though it might seem complex and time-consuming to enforce IP rights in China, IP right owners are advised to consider integrating administrative and legal remedies when pursuing the cessation of infringing activities. Knowing the efficiency and its potential role in evidence collection, the EIPP protection shall draw more attention of the owners.

---By Lifang Patent Team

A Comparative Study between Network Security Legislations in the US and China

On 8 Dec 2016, China and the United States held the third high-level dialogue on cyber crimes and related matters. It is re-asserted that the two state parties will continue to cooperate in the investigation of internet crimes or malicious acts initiated in either the territory of China or the US, in order that businesses are protected from infringement of intellectual property rights, and are thereby enabled to secure their competitive advantages.¹ In the view of how innovative internet technologies are reshaping our society, whereas incidents of international internet terrorism and cyber attacks are plenty, we feel obliged to treat international network security as an issue of vital importance.

Part I — Construction of Cyber-security System for the Protection of Critical Information Infrastructure

Increasingly, conventional infrastructure of physical existence is integrating with the digital system of information. These facilities store and manage affairs of national security, state administration, national economy and livelihood of the people, forming a cornerstone that keeps our civil society running in proper order.² Naturally, the two state parties value highly the construction of a cyber-security system for the protection of those critical information.

A reading draft of the Cyber-security Law of the People's republic of China (the PRC Cyber-security Law *hereinafter*) made an attempt to list the scope of critical information infrastructure. Notwithstanding, the law officially issued in Nov 2016 removed the list,³ providing merely that the scope of those infrastructure and

¹ 'China and the US re-affirmed their cooperation against internet crimes and malicious acts' (9 Dec 2016, China News) <<<http://www.chinanews.com/gn/2016/12-09/8088319.shtml>>> last accessed on 14 Dec 2016.

² See Mǎn Yì Lì, 'Methods to Protect Fundamental Cyber-security Infrastructure To be Formulated — An Interview with Wang Daolí, the Head of The Third Research Center for Cyber-security Law under the Ministry of Public Security of the People's Republic of China' (2016) 7 *Secrecy Science and Technology*, 10

³ The list includes networks of critical information, military networks, administrative networks above city-level, and other such networks of internet service providers used by the mass.

methods of protection shall be stipulated by the State Council, and defining critical information infrastructure as those which in the event of destruction, disruption or breach will possibly harm the national security, public interest, national economy and livelihood of the people.¹

Repeated revisions of the law have demonstrated how prudent legislators are being with the definition of critical information infrastructure. In practice, the majority of core technologies that Chinese information technology products use are imported. Over 2000 computer systems of great significance are connected to the public network. The problem is that, with little to none security measures, most of those systems are vulnerable to potential cyber-attacks.²

To this date, China has established numerous cyber-security institutions, including inter alia the National Information Security Standardisation Technical Committee, China Information Technology Security Evaluation Centre, National Computer Network Emergency Response Technical Coordination Center of China, and the National Computer Virus Emergency Response Center. There is nonetheless a lack of concrete strategy guiding clearly the construction of cyber-security facilities. Thus far the existing laws and regulations are abstract and difficult to enforce.

In comparison, the construction of cyber-security system in the US appears to be more mature and well-developed. On 12 Feb 2014, the White House published a document that is called 'Framework for Improving Critical Infrastructure Cyber-security'. It purports to further strengthen the cooperation between the Federal Government and the private sector in order that cyber-security of the critical internet infrastructure can be reinforced. The guiding document is divided into three parts: Framework Core, Framework Implementation Tiers and Framework Profile. Development of the 'Framework for Improving Critical Infrastructure Cyber-security' formulates a common tongue for the risk management of all critical infrastructure sectors, and in the meantime ensures that extensibility and technological innovations are optimised.

¹ See 'The Cyber-security Law of the People's Republic of China' (Xinhua) <<http://news.xinhuanet.com/politics/2016-11/07/c_1119867015.htm>> Last accessed on 13 Dec 2016

² Ruǐ Wáng, 'The Increasingly Prominent Subject of National Cyber-security: Opening of the High-level Forum on the Safety of Critical Information Infrastructure' (2016) 18 Computer & Network, 18

To that end, firstly, it is envisioned that (i) the critical infrastructure operators be enabled to run independently with the use of standardised guidance and time, (ii) acknowledging the globalization of internet security risks, globalised standards, guidance and time be adopted for the framework implementation and the other applicable cross-border practices.¹ The Federal Government of the United States emphasized in the publication that the framework is designed for the voluntary implementation of the state governments, enterprises and foreign corporations. It is nonetheless hoped that the framework will be implemented and used as an internationally applicable standard.

Part II — Network Security Information Sharing & Privacy Protection

Mass collection of information traffic on the internet brings about not only substantial economic value. It is also extremely important for the maintenance of national security and combat against terrorism. Via the collection, screening and analysis of internet data, the state enforcement agencies can possibly put a stop to the criminals before they could act, and prevent the damage from occurring or worsening. Notwithstanding, mass data surveillance could hardly avoid the infringement of privacy of individual citizens, causing an inevitable dilemma.

Prior to the publishing of the PRC Cyber-security Law, the laws of China did not impose upon the issue of network security information sharing any direct regulation. Scattered laws can be found at the National Security Law of China, the Regulations of the People's Republic of China for Safety Protection of Computer Information Systems and the Regulation on Internet Information Service of the People's Republic of China.²

The PRC Cyber-security Law, filling up the void, provides that the national cyberspace administration and the relevant departments shall have authority to put internet service providers under surveillance in accordance with law.³ The national

¹ See Xiángāng Liú & Xīng Chén, 'Framework for Improving Critical Infrastructure Cyber-security — Part I' (2016) 7 Information Technology & Standardization, 43—44

² Xiǎomíng Zhào, 'A Brief Discussion about Network Security Information Sharing' (2006) 10 Network Security & Application, 39.

³ Arts 43 & 44, The PRC Cyber-security Law

cyberspace administration shall also coordinate the relevant departments to carry out collection, analysis and report of network security information, and issue warning should the need arise. In the light of the above regulations, in practice there is no conventional mechanism of network security information sharing in China. Because the state administration is authorised to carry out surveillance, obtain and use all network information, sharing is no longer necessary. This, however, may lead to potential misuse or abuse of information by the state agencies.

In the US, sharing of network security information has long been a subject of much controversy, due to the vagueness of key provisions, wide scope of immunities warranted to the technology and manufacturing companies as well as authorization clauses that encourage state agencies to carry out surveillance activities. For the above reasons, the Congress refused to pass several legislations on the subject matter.¹ However, since the beginning of the Obama Administration, there were even more attempts to create governing rules on network security information. Later, the Senate passed the Cybersecurity Information Sharing Act of 2015. (CISA hereinafter) This piece of legislation has been a notable stride since the passing of the Cyber Intelligence Sharing and Protection Act in 2014 on the regulations of network security information sharing.

The CISA aims to grant technology and manufacturing companies with two specific permissions. Firstly, companies may adopt measures in response to network security risks; secondly, in order to protect their rights and property, companies are permitted to set up a department and monitor the information systems. Meanwhile, the legislation attempts to introduce a multi-layered privacy protection mechanism in the formulation of the information sharing model. In general, various provisions of the CISA have demonstrated the plural ends that the US wants to achieve with the law, being (1) the elimination of legal obstacles and other unnecessary risks of litigation, (2) the construction of a information sharing model to be used by the public and private sector on a voluntary basis and (3) establishment of a coordination mechanisms in the face of network security threats.²

¹ See Tóng Wú, 'The United States: The Cybersecurity Information Sharing Act — Impact and Response' (2016) 2 *Secrecy Science and Technology*, 50

² See Shěnkùò Wú & Qín Chén, 'Analysis of the Cybersecurity Information Sharing Act of 2015 by the US Senate' (2016) 1 *China Information Security*, 130

In brief summary, despite the fact that the publishing of the PRC Cyber-security law has to an extent supplemented the laws of China governing network security, the legal framework is relatively incomplete and practice experience is lacking. By contrast, albeit the American experience appears more mature, it is not necessarily inferred that China must follow the exact footsteps.

For instance, China and the US do not adopt the same approach in the formulation of an information sharing system, given the vastly different circumstances of the two countries. In the US, 85% of the critical information infrastructure is owned and operated by private enterprises. As such, the Federal Government is inevitably bound to focus on the sharing of network security information between the state agencies and the private sector.¹ On the other hand, critical information infrastructure

in China is mostly under the control of state-owned enterprises or the Central Government.² Mass information surveillance is attainable in the Chinese context. Also, the transitional development of China and the Chinese cultural traditions influenced the values and choices of law-makers in China, whereas the value of privacy is viewed more strictly in the US. China and the United States do not share an exact same understanding of basic human rights and t

¹ Mínghǔ Mǎ, Tíng Fāng & Yuè Wáng, 'Insights from the US Network Security Information Sharing Model' (2016) 3 Journal of Information (Qíng Bào Zǎ Zhì),18

² See Mǎn Yì Lǐ [n 2] 18

IMPORTANT INFORMATION

This Newsletter has been prepared for clients and professional associates of Lifang & Partners. Whilst every effort has been made to ensure accuracy, no responsibility can be accepted for errors and omissions, however caused. The information contained in this publication should not be relied on as legal advice and should not be regarded as a substitute for detailed advice in individual cases.

For more information, please visit our website at en.lifanglaw.com. If you have any questions, please contact us at info@lifanglaw.com or

Beijing Office

Address Room 1105, Tower A, Nan Xin Cang International Building,
No.A22, Dongsishitiao Street, Dongcheng District, Beijing,
P.R.China 100007

Telephone (86-10) 64096099

Fax (86-10) 64096260,64096261

Guangzhou Office

Address Room 3806, Building G, G.T.Land Plaza, No. 16, Zhujiang East
Road, Zhujiang New Town, Tianhe District, Guangzhou P. R.
China

Telephone (86-20)85561566, 85561660, 38898535

Fax (86-20)38690070

Wuhan Office

Address Room 1002, Tower C, Han Street Headquarter International,
No.171 Zhongbei Road, Wuchang Dist, Wuhan, Hubei, P. R.
China

Telephone (86-27) 87301677

Fax (86-27) 86652877

Seoul Office

Address Room 1120, Anam-Tower, 311, Teheran-ro, Gangnam-gu,
Seoul, Korea

Telephone +0082 02 69590780