

VIVIEN CHAN & Co.

YOUR GREATER CHINA LAWYERS

HONG KONG | BEIJING

NEWSLETTER

issue 10 . 2016

IP UPDATE



Anna Mae Koo PARTNER

MA (Law) (Hons), University of Cambridge (Prince Philip Scholar)

- Asialaw Rising Star Lawyer in Intellectual Property 2018
- Techstars Mentor 2015
- IP Rising Star (Euromoney Women in Business Law Awards) 2013
- Litigation Committee Member, International Bar Association
- Anti-Counterfeiting Committee (2018), Internet Committee (2014-2016), INTA



Ann Xu CO-HEAD OF BEIJING OFFICE

PRC Licensed Trademark Attorney
BA (Capital Normal University)
MIP (Franklin Pierce Law Center)

SIPO Releases Draft Amendment of Guidelines for Patent Examination for Public Comments

On 27 October 2016, the State Intellectual Property Office (SIPO) released the Draft Amendment of Guidelines for Patent Examination for Patent Examination ("Draft Amendment") for public comments. Highlights of the key proposed changes are as follows:-

(1) ALLOWING FOR INVENTIONS INVOLVING BUSINESS METHODS

Business method patents are traditionally not accepted by SIPO as it is considered to only be a mental activity lacking in technical features. Innovations relating to e-commerce have thereby suffered a lack of protection. As such, and in response to rapidly growing online businesses in China, SIPO has now revisited this provision.

As provided under Article 25 of the current Chinese Patent Law, rules and methods merely for mental activities shall not be granted a patent. In this Draft Amendment, SIPO is proposing a clarification to state that as long as a patent contains technical features, the fact that it contains business rules or methods does not bar it from being patentable.

According to SIPO, the purpose of this amendment is to enhance protection on innovations related to e-commerce related business methods. This is in response to the rapid growth of new business process businesses on the internet.

(2) DRAFTING OF APPARATUS CLAIMS INVOLVING SOFTWARE PROGRAMS

It has been provided in the current Guidelines that claims of an invention patent application relating to computer programs may be drafted as process claims or apparatus claims. If it is drafted as an apparatus claim, the description of it as an apparatus is required. In this Draft Amendment, SIPO proposes to remove such a requirement and allow apparatus claims of inventions that are related to computer programs to contain not only the hardware, but also the computer program.

Under the current practice, drafting apparatus claims relating to computer programs is very similar to drafting apparatus claims that are related to methods or functions of hardware. Confusion may be caused if the claim is directed to an invention which comprises of technical features of both computer program and hardware. Such amendment will allow claims for such types of inventions to be drafted in a more straightforward manner so as to avoid any confusion in claim interpretation.

(3) SUPPORTIVE EXPERIMENTAL DATA IN THE CHEMICAL FIELD

For patent applications in the chemical field, it is specifically provided in the current Guidelines that inventions need to be verified by experimental data. Whether the disclosure of description is sufficient is judged based on the initial application documents filed. Any embodiments or experimental data submitted after the date of filing will not be taken into consideration.

In this Draft Amendment, SIPO proposes to allow the late filings of experimental data to be considered, provided that the experimental data must be capable of being derived from the application's disclosure by a person skilled in the art.

This amendment will not make significant changes to the current practice in drafting chemical patent applications. The applicant, in any case, must disclose in the description, all available experimental data which he/she believes would be useful to support the intended technical effect of the invention. This amendment may provide an option for the applicant to respond to an office action should the claims be rejected due to a lack of support from the description. However, it will be the responsibility of the applicant to convince the Examiner that the intended technical effect is derived from the initial disclosure of the application, and to be shown by the later filed experimental data.

(4) AMENDMENTS TO CLAIMS IN INVALIDATION PROCEEDINGS

Currently, the ways to amend claims in invalidation proceedings are generally limited to Deletion of a Claim, Combination of Claims, and Deletion of a Technical Solution.

In this Draft Amendment, SIPO proposes to include Combination of Claims within Deletion of a Claim to simplify the structure. SIPO also proposes to relax the limitation to include Further Definition of a Claim and Correction of Obvious Mistakes. It is also in the proposal that Further Definition of a Claim should be defined as adding one or more technical features contained in other claims to the claim that is to be amended. These changes are intended to address the practical needs for more flexible ways in making amendments to claims in an invalidation proceeding.

(5) SUSPENSION TIME LIMIT OF RELEVANT PROCEDURES DUE TO THE COURT'S RULING ON PROPERTY PRESERVATION

As provided in the current Guidelines, there is a general time limit of 6 months on the suspension of a relevant procedure in SIPO due to a property preservation ruling issued by the Court. This time limit is extendable but shall not exceed 12 months in total.

In order to assist the execution of property preservation rulings issued by the Court, this Draft Amendment eliminates such time limit. Instead, the relevant procedure shall be suspended in accordance to the time limit of the property preservation stated in the civil ruling and the Notification on Assistance in Execution. As patent infringement cases may take years to complete due to the mechanism of stay pending invalidation proceedings nowadays, this is expected since the existing time limit of 12 months is no longer applicable and practical in assisting the execution of property preservation for patent cases in general.

(6) INFORMATION ON PENDING APPLICATIONS ALLOWED FOR PUBLIC CONSULTATION

Currently, with respect to an invention patent application which has been published but not been granted with a patent right, the public can only access official notifications issued before the date of the publication.

In this Draft Amendment, SIPO proposes to include notifications, search reports and decisions issued in the substantive examination procedure in the contents allowed for public consultation. According to SIPO, such amendments are to enhance the dissemination of technologies and to increase transparency of the patent examination process.

It is believed that such amendments would make monitoring of competitors' patent applications easier. Based on the notifications issued in the substantive examination procedures of competitors' patent applications, companies may evaluate their competitors' chance of success in obtaining patent rights and take preemptive actions accordingly.



Anna Mae Koo PARTNER

MA (Law) (Hons), University of Cambridge (Prince Philip Scholar)

- Asialaw Rising Star Lawyer in Intellectual Property 2018
- Techstars Mentor 2015
- IP Rising Star (Euromoney Women in Business Law Awards) 2013
- Litigation Committee Member, International Bar Association
- Anti-Counterfeiting Committee (2018), Internet Committee (2014-2016), INTA



Ken Hung

ASSOCIATE

BBA (Law), University of Hong Kong
LLB, University of Hong Kong

Cyber Security Law: Reinforcing the Great Firewall

The Cyber Security Law (the "Law") was passed by the Standing Committee of the National People's Congress on 7 November 2016 and will come into effect on 1 June 2017. The Law is in line with the Chinese government's determination to maintain internet safety and national security; and to protect the interests of the public through censorship and stringent regulations. While the majority of the articles remain intact, several amendments were made to the final version to re-emphasize China's intention to further bolster cyber security and raise penalties for breaches of the Law. It is important for domestic and foreign entities who operate in China to understand the Law, as it has wide applicability.

WHO WILL BE REGULATED

Article 2 stipulates that the "construction, operation, maintenance and use of the network within China" shall be governed by the Law. This is fairly wide as it covers all networks that are being **used** in China. The newly added Article 75 further establishes that other than injunction measures, the assets of foreign companies, organizations or individuals engaging in activities, which endanger the critical information infrastructure, may at the discretion of the public security department of the State Council, be frozen. While it remains to be seen how this will be enforced given that the entities or individuals are not located in China, network operators including the owners, administrators of networks and network service providers should be aware of their obligations arising under this Law, which will be discussed below.

KEY OBLIGATIONS FOR NETWORK OPERATORS

Article 21 provides for the implementation of a "graded network security protection system" which requires network operators, inter alia, to establish internal security

management systems, to adopt technical measures for monitoring and recording the status of network operations and preserve network logs for no less than 6 months.

Network operators providing network access, domain name registration services, phone access, or information publication or instant messaging services are required to identify the real identity of the users when signing service agreements or confirming the production of services (Article 24).

KEY OBLIGATIONS FOR CRITICAL INFORMATION INFRASTRUCTURE OPERATORS

To address previous concerns on the ambiguity of the Law, sectors that are qualified as "critical information infrastructure" are clearly specified to include public communications and information services, energy, transportation, water conservancy, finance, public services and e-commerce governance (Article 31). Despite not being an exclusive list, the revised definition gives additional guidance to the focus of sectors that are subject to security checks.

Operators of critical information infrastructure are required to store citizens' personal information collected and generated by the critical information infrastructure operators and other important data (Article 37) within China. The change in the second draft limiting the scope to "important business information" was not retained. Overseas disclosure of such information is only allowed after security assessments by the authorities, the threshold of which is still subject to further clarification.

DATA PROTECTION

Greater emphasis has been placed on privacy protection with assurance given to informants that their identities shall be kept confidential (Article 14) and that the use of end users' data shall be restricted to protecting cyber security (Articles 30).

PENALTIES

The Law introduces heavier penalties than previous drafts for violation of the Law. Engaging in activities that endanger cyber security or providing tools or assistance to those who endanger the same is subject to a fine ranging from RMB50,000 to RMB500,000 (US\$7,250 to US\$72,500), in addition to being detained for a period of up to 15 days.

Network operators failing to request real identity information from users may also be fined a similar amount and the responsible individual shall be fined RMB10,000 to RMB100,000 (US\$1,500 to US\$15,000).

Individuals and organizations are responsible for their use of the internet, and are prohibited from setting up websites, chat groups that are used to commit fraud, teach others how to commit a crime, produce or sell any prohibited or controlled goods.

MOVING FORWARD & CONCLUSION

The Cyber Security Law introduces serious penalties and sanctions, and affects all entities, domestic or foreign, who use or control a network that can be used in China. There is however, still a lot of uncertainty as to the implementation and enforcement of these sanctions, and to some of the details of the interpretation of the Law. We therefore await the practice guidelines and implementing regulations to be issued with regards to the Law, and will update once these are announced. Regardless, an audit of one's own network use in China is recommended to avoid potential contravention of the Law.