The British Chamber of Commerce Shanghai
ESTABLISHED 1915

China Legal Trends
2016 Q2

Legal

Executive Summary

Welcome to the 2016 Q2 issue of the British Chamber of Commerce Shanghai quarterly *China Legal Trends* update. A number of the Chamber's member law firms have provided us with recent essential insights and updates on a variety of important legal developments within China.

This issue highlights the taxation policy on cross-border e-commerce (Circular 18). The biggest change is the introduction of positive lists, which prohibit anything not on the lists and replaces the previous negative list system.

Also addressed is the current state of law in China in relation to data protection and cyber security, as well as future developments in this area. Companies should ensure they comply with Chinese specific regulations and continually audit practices to confirm compliance.

Another aspect concerns the "Judicial Interpretation" related to corruption and bribery, which provides further clarification in this area. The monetary threshold for prosecutions has been increased and the legal interpretation of what constitutes a bribe is extended in a number of areas, thereby having potential implications for the compliance policies of companies operating in China.

The final development involves provisions on internet search services and mobile apps. These provisions impose new obligations on search results control, verification of identity, and data processing.

We sincerely thank Baker & McKenzie LLP, Clyde & Co LLP, O'Melveny and Myers LLP and Mayer Brown JSM for their contributions to this issue, and their continued support of the Chamber.

Our thanks also go to those Legal Focus Group members and Chamber staff who have been working hard on this issue.

Best Regards,

Janet Qu
Chairwoman, Legal Focus Group, The British Chamber of Commerce Shanghai

The British Chamber of Commerce Shanghai
ESTABLISHED 1915

Contents

China: Major Policy Changes to Cross-border E-Commerce Program and the Implications on Sale of Unregistered Products

Baker & McKenzie LLP

May 2016

In the end of March, China's Ministry of Finance ("**MOF**"), General Administration of Customs ("**GAC**") and State Administration of Taxation jointly promulgated the Circular on Taxation Policy on Cross-Border E-Commerce Retail Importation (Circular Cai Guan Shui [2016] No. 18, or "**Circular 18**"). Circular 18 entered into force as of April 8, 2016.

Circular 18 has two major implications: (a) new types of taxes are to be levied on goods imported under the cross-border e-commerce program ("**Program**"), and (b) the regime changes from a previous negative list to a positive list of goods permissible under the Program. Within 10 days, two positive lists ("**Positive List I**" and "**Positive List II**") were issued by the tax, customs and quality supervision authorities under Circular 18's framework, together with two clarifications to the positive lists issued by the CFDA. On top of those, the GAC further circulated a notification to explain certain practices under the new regime.

Highlights of the changes are summarized below, and full English translations to the series of regulations are attached.

New Categories of Taxes Applicable

Previously, Personal and Parcel Article Tax ("**PPT**"), a duty designed to facilitate importation of personal articles for personal consumption by postal and courier services or carry-on luggage, was applicable to the Program. This has caused an unfair price advantage on goods sold under the Program and the same goods imported under normal commercial channel because goods would be subject to import duty and VAT under the normal commercial import. One of the objectives is to remedy the situation by changing the tax payable under the Program.

Under Circular 18, goods under the Program are subject to other import taxes instead, specifically: (a) customs duty, (b) value-added tax ("VAT"), and (c) consumption tax.

The rates of these taxes vary depending on the product's tariff classification under the Tariff Schedule. For a parcel valued lower than RMB2,000 (approximately USD320), the customs duty will be exempted, and a 30% discount will be given to the VAT and consumption tax.

In the meantime, the tax authorities also amended the current PPT schedule, providing for substantially higher tax rates. Under the revised schedule, PPT will continue to be applied to "personal articles" but are not imported under the Program.

By increasing PPT rates, China intends to divert sales from unregulated foreign websites to the approved and closely supervised e-commerce platforms under the Program.

Positive List System

Perhaps the biggest change is the positive list system. Previously, it was a negative list regime where all goods could be imported under the Program if the goods were not listed on the negative list. Circular 18 created a "positive list" system where only goods listed on the Positive List can be imported under the Program.

• ***Two Positive Lists***

The first Positive List ("**Positive List I**") was issued on 6 April 2016, and then on 15 April a second Positive List ("**Positive List II**").

Positive List I contains 1,142 goods items and Positive List II contains 151 items. Positive List II was widely seen to clarify the position on health food products and also widen the list to include certain fresh food products. The lists are based on the Harmonised System Code ("**HS Code**"), the universal system for customs authorities to classify goods. The way to interpret the Positive Lists is to first check the goods in question and find the most appropriate HS Code(s) from the HS Code database system and then check against the Positive Lists I and II to see if the relevant HS Code is there. If it is listed on the Positive List, then one will have to check if there are additional requirements listed on the specific HS Code.

• ***CFDA Clarifications***

Shortly after Circular 18 was effective, CFDA issued two Clarifications - one on April 13 focusing on infant formula milk, cosmetic and formula food for special medical purpose; one on April 15 on health food and medical device products.

Below is our short analysis and understanding of how the following products would be treated under the Program.

• ***Infant Formula***

Infant formula was listed under HS Code 19011010 on Positive List I. But there is a note on the HS Code which says: "excluding infant formula which are required to be registered under the Food Safety Law but has not been registered". This was widely

interpreted to mean that while infant formula milk code is listed, only those that have already been registered can be imported under the Program.

In the April 13 CFDA Clarification, CFDA reiterates the registration requirement but at the same time acknowledged that the procedures to register infant formula have not been finalized yet, which means that it is not possible to obtain any such registration at this time or in the near future. As a result, a grace period until January 1, 2018 has been granted where infant formula without registration can still be imported under the Program until then.

• ***Cosmetics***

Cosmetic products are covered by a number of HS Codes under Positive List I (e.g., 33030000 for "perfume", 33042000 for "eye make-up preparations", and the catch-all code 33049900 for "other beauty or makeup preparations"). However, under Positive List I, all those Codes have a note stating "excluding cosmetics imported for the first time".

In the CFDA April 13 Clarification, CFDA stresses that product registration/recordal requirement is needed. And since the registration/recordal system has been in place for many years (with some 136,000 registrations/recordals already on the CFDA's database), CFDA saw no reason to exempt the requirement. This means that effective immediately, all cosmetic products must have been registered/recorded with CFDA before they can be imported under the Program.

• ***Formula food for special medical purposes***

Formula food for special medical purposes may be covered by various food-related HS Codes, e.g., 19011090 for baby food.

The CFDA in its clarification treats formula food for medical use similar to infant formula. The CFDA recognized that registration should be required under the Food Safety Law, but the registration procedures will not take effect until July 1, 2016. Therefore, a grace period until January 1, 2018 was granted.

• ***Health food***

The HS Code system does not contain a general code for health food or nutritional supplements. Depending on the nature of the product and the ingredients contained, different health food products may be listed under different HS Codes. For example, vitamin products are under HS Codes 2936 class and its subclasses whereas fish oil would be under HS Codes 15043000 (animal oil and fat, oil from marine mammal) or HS Code 1506 (oil or fat from other animals). This means that for health food, one will

have to check the product and its ingredients to see which HS Codes the product should be classified, and then cross-check if such HS Codes are on the Positive Lists.

For many other health food products such as vitamins and fish oil, Positive List I contains a remark – "excluding food products that are not general food products, or are special food products which registration/recordal is legally required" – in the relevant HS Code column. This exclusion note was interpreted to mean that the all products would be excluded if there is a local registration/recordal requirement.

Then Positive List II and a second CFDA Clarification were issued in a few days' time to clarify the situation with health food. Positive List II repeated the HS Codes relevant to health food already on Positive List I. While Positive List II removed the exclusion note previously on Positive List I, it referred to a few general notes. Note 2 further refers to the April 15 CFDA Clarification. In that Clarification, CFDA confirmed that the CFDA's administrative measures for health food registration or recordal will come into force as of 1 July 2016. The CFDA stated that at that time (July 1), registration or recordal with the CFDA should be obtained for all health food products imported into China, including those products sold under the Program. It has been interpreted by industry that CFDA implied a grace period until 1 July 2016, but this is not confirmed one way or the other by CFDA or the local CIQ. What seems to be clear is that registration/recordal will be required for health food products after 1 July 2016.

That said, we would like to point out that there may be some nutritional supplement products that could still be allowed as they are not subject to registration / recordal requirements. For example, whey protein, a popular nutritional supplement, is under HS Code 040410 (whey protein, concentrated or not) on Positive List I, and there is no exclusion note attached. So presumably, it is a product which could be allowed without involving any registration/recordal with the CFDA.

• ***Medical devices***

Positive List II contains some HS Codes that may cover medical devices (e.g., 30059090 for "sterile suture materials and sterile tissue adhesives for surgical wound closure" and 90184990 for "other instruments and appliances, used in dental sciences").

The CFDA acknowledged that the HS Codes used on Positive List II cannot exactly mirror the classification of medical devices under China's regulatory framework. If any goods should be considered as medical devices under PRC law, they should be registered or recorded with the CFDA before they are allowed to be imported. Again, this means that product registration/recordal requirement is necessary for medical device products.

Goods Shipped Before April 8 Exempted

Circular 18 and the Positive Lists caused huge impact on the cross-border e-commerce operation. Local inspection and quarantines authorities ("**CIQ**") basically stopped all imports of above-mentioned products during the initial stage. Many vendors were caught by surprise and pleaded to the authorities on more lenient treatment of the goods already shipped before Circular 18 came into effect. Then GAC on April 18 issued a notification to local CIQs which essentially allows goods not on the Positive Lists but already in the bonded zones to continue being sold until the inventory is exhausted. For shipments already dispatched before April 8, CIQs would also allow them to enter the bonded zones as long as the bill of lading of the shipment is dated before 8 April 2016. And once in the bonded zones, CIQs should allow the products to be sold.

The situation is far from settled at this point. We are closely monitoring the development. There may be further changes near 1 July 2016 when the new health food registration/recordal system becomes effective. We will keep you informed of any major developments.

Electronic Growing Pains: Cyber Security and Data Protection in the People's Republic of China

by Richard Bell
Clyde & Co LLP
June 2016

Introduction

The protection of data, whether it be personal information or trade secrets, and the vulnerability of that data to misuse for commercial gain are issues that Governments all around the world grapple with. China is no exception, and with good reason. At the close of 2015, China had over 680 million active internet users and online retail transactions of over RMB 3877.3 billion. By 2020, China's e-commerce market is predicted to be larger than those of the U.S., the UK, Japan, Germany, and France combined.

With the huge growth in internet subscribers and e-commerce in China, data protection and cyber security have become increasingly important. In February of this year it was reported that Taobao, China's largest online retailer, was the victim of a cyber-attack in which hackers successfully compromised more than 20 million user accounts linked with the site. This is just one high profile example of the many data protection and cyber security issues that have arisen in China in recent years.

In this article we look at the current state of the law in China in relation to data protection and cyber security. We also look at the future of data protection and cyber security law and discuss proposed new laws. We then set out ten key questions companies operating in China should ask when considering their data storage and e-commerce policies.

Data protection laws in China

China, unlike other Asia Pacific states such as Singapore and Hong Kong, does not currently have a stand-alone data protection or cyber security law. Instead, the rules around data protection and cyber security are fragmented across multiple laws and regulations, with oversight typically left to industry-specific regulators.

General law requirements

At the broadest level, data protection in China is afforded to all citizens through the Constitution of China which contains a general principle on protecting the freedom and privacy of correspondence. While the Constitution does not provide a cause of action in and of itself, the Tort Law of China gives individuals whose civil rights and

interests have been infringed the right to make a claim against the infringing party. Such civil rights and interests include, among other things, the right to privacy.
The State may also bring an action under the Criminal Law, whereby there are various offences that relate to purchasing, selling or otherwise acquiring personal information of citizens.

The State also imposes privacy of information through the Resident ID Card Law, which requires businesses that collect identifying information of citizens contained on identity cards to keep such information confidential.

The Decision on Strengthening Network Information Protection (the "Act") provides more specific regulations on the collection and use of the personal data of citizens with companies subject to a range of penalties for failing to comply. In addition, the Act gives citizens a right to request their information to be deleted and provides a private cause of action for an infringement of their rights pursuant to the Act.

Industry specific requirements

China has enacted a number of industry specific regulations that provide additional rules. The most relevant of these regulations is the Consumer Rights Law, which imposes obligations on businesses in the collection and handling of consumers' personal information, the key requirement being that consumers' personal information cannot be collected without their consent. There also exists a significant range of industry-specific regulations within the telecommunication, banking, and healthcare sectors.

The guidelines

In 2013, in response to rapid growth in the use of data and the Internet, the government enacted the Information Security Information Guidance on Protection of Personal Information of Public and Commercial Service Information ("the Guidelines"). The Guidelines are a set of non-binding guidelines that apply to all private entities and are designed to protect the personal information of individuals. The Guidelines provide guidance on the collection, processing, transferring and deletion of personal information; how computer networks that handle personal information should be maintained; and the appropriate responses to take when information has been mishandled.

While the Guidelines are non-binding they are significant in that they are an amalgamation of current regulations and represent best practice within China.

Cyber security laws In China

In enacting regulations, China has tended to treat cyber security as a distinct issue to that of data protection. Current laws that do address cyber security tend to do so in an indirect manner. The first of these, the State Secrets Law, makes it an offence to improperly handle information designated a state secret. In January 2016 China also enacted the Anti-terrorism Law which is intended to identify people and activities, including those discussed online that threaten public and government security. Significantly, the Act requires that telecom operators and Internet service providers give technical support and assistance, including decryption solutions to police and national security authorities.

The future of data protection and cyber security law in China

The most significant development in cyber security is expected to come with the introduction of a law modeled after the Cyber Security Law of the People's Republic of China (Draft). The main of objective of the Draft Law is to preserve national security by enabling the government to have more control over networks and data security. If enacted in its present form, the Draft Cyber Security Law will codify currently scattered Internet censorship rules, provide a comprehensive regulatory regime for cyber security and impose legal obligations on network operators and network service providers.

In addition, it is expected the insurance sector will also see the introduction of specific regulations with the recent release of the Draft Regulation of Information of Insurance Institutions in October 2015.

Ten key questions

Taking into account the regulatory regime in China, we set out below ten key questions companies operating in China should ask themselves when considering data protection and cyber security issues:

1. Are you responsible for the protection of personal information?

Chinese regulators have chosen to place the responsibility for data protection on the businesses that collect this data. Under the Guidelines, businesses that collect, process and retain the personal information of individuals have a positive duty to provide proper safeguards and protection for this information. This includes auditing internal security systems and having emergency plans in place in the event that data is leaked, lost, damaged, tampered or improperly used.

2. What type of information do you handle?

Not all information is equal and a central tenant of the Guidelines is the type of information that is handled. Information is categorized as either Personal Sensitive

Information or Personal General Information. This categorization of information is significant because if the information is Personal General Information, the subject of that information may be deemed to give tacit consent to its collection and use (subject to a number of exceptions). If the information is Personal Sensitive Information express consent is required. The Guidelines provide a number of criteria to assess whether information is sensitive which broadly turns on the degree to which the information may identify or harm an individual if leaked. All other information that is not sensitive information is considered general information.

3. How do you collect information?

The Guidelines make it a point to note, repeatedly, that information should not be arbitrarily collected. The collection of information should be done with an informed purpose which is clearly and specifically stated. In collecting information there should a clear method and process and only the minimum amount of information required to achieve the informed purpose should be collected.

4. Do you tell the user what you are doing?

Some things are best kept secret, but according to the Guidelines the fact that you are collecting personal information and what you are doing with that information is not one of them. The Guidelines require businesses to be transparent in their collection of information, such that information is not collected in a concealed or undisclosed manner, and relevant matters, as outlined in the Guidelines, are disclosed to the person whose information is being collected.

5. Do you ask permission first?

It is a primary requirement of the Guidelines that businesses receive consent to the collection and use of an individual's personal information.

Express consent must be received where:

- the information is considered personal sensitive information;
- the information is to be transferred to a third-party;
- the information is to be transferred overseas, even if that transfer is to a related entity;
- the information is personal sensitive information and it is to be retained after it has been processed;
- the information is to be retained for a period longer than disclosed to the subject of the information.

For general information the subject may be deemed to give tacit consent, except where the information falls under one of the above exceptions.

6. How do you process and manage information?

Although the Guidelines' rules for the processing of information are not as detailed as other sections they nevertheless stipulate a number of requirements. Primarily, there must be an established system for the processing of personal information and the information should only be processed for the purposes disclosed and consented to by the subject of that information. In addition, while the information is retained, it must not be assessed by anyone that does not have a connection with the purpose for which the information is being processed.

7. Do you allow the user to check their own information?

An aspect of the Guidelines which may be considered more related to cyber security, is the requirement that a business must keep a record of the personal information they possess and the status of that information. Correspondingly, the Guidelines also allow a person whose information has been collected the right to request whether the business retains any of their personal information, the contents of the information, and the status of processing that information. Where a person's personal information is incorrect the Guidelines provide that they have a right to request the correction of that information.

8. Do you transfer information to a third party or an associated entity?

It is common for companies to transfer information internally, to a related entity overseas, or to a third party. However, the Guidelines put some limitations on this. The Guidelines require that the subject of the information be informed of and consent to the transfer to a third-party or overseas, even if that transfer is to a related entity.

9. Do you delete information?

The Guidelines include provisions which provide that where a subject of information requests the deletion of their personal information with just reasons, businesses are required to delete such information. Moreover, businesses are also required to delete information once the informed purpose of collecting that information has been achieved or the disclosed time-limit has elapsed. Where it is necessary to retain the information beyond this period any identifying details of the information must be removed.

10. Have you got a user agreement?

Risks posed by cyber security issues can be mitigated through a correctly drafted user agreement. While that may involve some expense, having a user agreement that is up to date with the law and complies with best practice will often be the best defense against an action by the regulator or user.

Conclusion

China is a huge market for all things related to the internet and e-commerce. That market is growing, but with that growth comes the pain of potential security breaches and cybercrime.

With increasing requirements for data protection and cyber security, and increasing industry specific regulation, there is now a strong basis for companies to review their data protection and cyber security practices and policies. Companies, particularly those operating in multiple jurisdictions, must ensure they comply with Chinese specific regulations and not simply adopt practices and policies formulated for other markets. In addition, companies should be aware that data protection and cyber security are no longer issues to address on a one off basis, but rather are ongoing matters that should be continually audited and updated to ensure compliance.

China Law Update: Judicial Interpretation on Corruption and Bribery Crimes

O'Melveny & Myers LLP
June 2016

On April 18, 2016, the Chinese Supreme People's Court and the Chinese Supreme People's Procuratorate jointly issued the *Interpretation of Several Issues concerning the Application of Law in Handling Criminal Cases related to Corruption and Bribery* (the "**Judicial Interpretation**"). It became effective immediately. The Judicial Interpretation provides further clarification to the 2015 *Amendment IX to the Chinese Criminal Law* (the "**Amendment IX**") regarding corruption and bribery crimes. This Judicial Interpretation is important in that it adjusts the monetary thresholds for bribery prosecutions and sentencing, includes "intangible benefits" in the crime of official bribery, clarifies that a thank-you gift after improper benefits are sought still constitutes bribery, and clarifies when leniency may be given. These changes have important implications for the compliance policies of companies operating in China.

Adjusts Monetary Thresholds for Bribery Prosecutions and Sentencing

The Judicial Interpretation raises the monetary threshold for most prosecutions for the crime of accepting bribes by state functionaries from RMB5,000 (approximately US$760) to RMB30,000 (approximately US$4,600).[1] This does not mean that an amount below RMB30,000 is a safe harbor. If the amount of accepted bribes is between RMB10,000-30,000 (approximately US$1,500-4,600), criminal liability may still occur if one of the eight situations mentioned in the Judicial Interpretation occurs. These include such things as having a prior record of party discipline or administrative penalty due to corruption, records of criminal prosecution for intentional crimes, etc.[2] The monetary threshold for the prosecution of a crime of accepting bribes by a non-state functionary is set at two and five times the amount of the threshold for the crime of accepting bribes by a state functionary in cases involving a "relatively large amount" and a "huge amount," respectively.[3]

As for the crime of offering bribes to state functionaries, the Judicial Interpretation raises the monetary threshold for criminal prosecution from RMB10,000 (approximately US$1,500) to RMB30,000 (approximately US$4,600), unless certain circumstances are involved, such as bribing three or more state functionaries; giving bribes with illegal gains, etc.[4] The monetary threshold for prosecution of the crime of offering bribes to non-state functionaries is set at two times the amount of the threshold for the crime of offering bribes to state functionaries.

In addition, the Judicial Interpretation further clarifies certain terms used in the Amendment IX for sentencing standards, such as "relatively large amount," "huge amount," "especially huge amount," "serious circumstances," and "especially serious circumstances," etc. Amendment IX is intended to change the previous practice of determining sentencing merely based on the amount of improper payments, which

resulted in some cases where the amount of bribes was the same but the sentencing was drastically different. The Amendment IX puts emphasis on both the amount of improper payments and some specific factors. The Judicial Interpretation provides further implementation rules in this regard. This is intended to make sentencing fairer and to reflect the more complex economic and social circumstances that have come into play since the Chinese Criminal Law was first revised in 1997.

Clarifies definition of bribes to include certain intangible benefits

The Judicial Interpretation clarifies that for the crime of bribery, "money and property" includes money, articles, and property interests.[5] "Property interests" include material benefits that can be converted into money, such as home renovation, debt relief, etc., and other benefits that require the payment of money, such as membership service, travel, etc.[6] This is the first time that the judicial authority clarifies that intangible benefits are a type of bribe for the crime of official bribery. The judicial interpretation "*Opinion Concerning Several Issues in the Application of Law in Cases of Commercial Bribery*" issued in 2008 provides that bribes in the context of commercial bribery include intangible benefits.[7] The Judicial Interpretation bridges the gap and provides prosecutors and judges with a clear basis for prosecuting and adjudicating official bribery cases in which intangible benefits are involved. Also, the 2008 judicial interpretation only provides that the amount of such intangible benefits should be calculated at the amount actually paid. The Judicial Interpretation adds that the amount concerned can also be calculated at the amount payable.[8] This is to address situations in which services, travel or other intangible benefits may have been deliberately undervalued by bribe givers.

Clarifies the element of "corruptive intent" for the crime of accepting bribes by state functionaries

The Judicial Interpretation clarifies the situations in which officials can be considered to be "seeking benefits for others" when determining the crime of accepting bribes by state functionaries. Under the Judicial Interpretation, promise to seek benefits for others should be considered as "seeking benefits for others."[9] This is similar to how the U.S. Foreign Corrupt Practices Act is applied in some cases.[10] In addition, if an official clearly knows that a person offering a bribe has in mind a specific request seeking the official's help, the official will be considered to be "seeking benefits for others."[11] This is intended to address situations in which officials accept money or property from bribers who do not raise requests for help explicitly but have some unspoken understanding with the officials regarding benefits sought. Also, if nothing has been requested from an official in the performance of his or her duties but that official afterwards accepts money or property from others based on such performance, that official will be considered to be "seeking benefits for others."[12] In practice, there have been arguments in some cases that gifts given to officials after the officials performed their duties should not be considered as bribes. The Judicial Interpretation targets such situations and clarifies that a thank-you gift received after benefits are sought or received still constitutes bribery. This new rule has implications

for companies' compliance policies. Usually, companies pay more attention to the prohibition on gift giving to officials while an important regulatory application or decision is pending before the officials. Now it becomes more important for companies to also pay attention to establishing or improving policies on gift giving and entertainment to officials after a regulatory decision is made or approval is rendered.

Furthermore, the Judicial Interpretation provides that an official should be considered to have the intent of accepting bribes if the official does not return or turn in the bribes solicited or accepted by a person specially related to the official (the "Specific Interested Person") after the official knows such fact.[13] Such Specific Interested Person includes close relatives, lovers, or anyone who has a common interest with an official.[14] This signals that companies should also consider setting rules for gift giving and entertainment to people specifically related to officials in the compliance policies.

Leniency and voluntary disclosure

Amendment IX tightened the conditions for punishment to be reduced or waived for the crime of giving bribes to state functionaries. Specifically, Article 390 of the PRC Criminal Law provides that if the circumstances of crime are relatively minor and the briber plays a critical role in detecting a major case or if he/she performs any major meritorious services, he/she may be given a mitigated punishment or be exempted from punishment.[15] The Judicial Interpretation further defines "relatively minor crime" and "major case" and illustrates the circumstances considered as "playing a critical role in detecting a major case," as mentioned in the foregoing Criminal Law provision. The determination of "relatively minor crime" and "major case" mainly will depend on the term of imprisonment and influence of the case.[16] As for determining what constitutes "playing a critical role in detecting a major case," the Judicial Interpretation lists four circumstances that mainly focus on the voluntary confession important for investigating a major case.[17]

---

[1] The *2011 Criminal Law of the People's Republic of China* Articles 383 & 386 and the*Judicial Interpretation* Article 1.

[2] The *Judicial Interpretation* Article 1.

[3] *Id.* Article 11.

[4] *Interpretations on Several Issues Concerning Application of Law for Handling Criminal Cases of Bribe Offering* (关于办理行贿刑事案件具体应用法律若干问题的解释), released by the Supreme People's Court and the Supreme People's Procuratorate on December 26, 2012 and effective on January 1, 2013, Article 1, and the Judicial Interpretation Article 7.

[5] The *Judicial Interpretation* Article 12.

[6] *Id.*

[7] *Opinion Concerning Several Issues in the Application of Law in Cases of Commercial Bribery* (关于办理商业贿赂刑事案件适用法律若干问题的意见), released by the Supreme People's Court and the Supreme People's Procuratorate on November 20, 2008 and effective upon release, Article 7.

[8] The *Judicial Interpretation* Article 12.

[9] The *Judicial Interpretation* Article 13.

[10] For example, See *U.S. v. Monsanto* (D.D.C. 2005) and *SEC v. Monsanto Co.,* No. 05-0014, (D.D.C. 2005), where a $50,000 bribe was authorized by a Monsanto officer to pay to a senior Indonesian environment official who promised to revoke a government decree, but was ultimately unsuccessful as the official never actually authorized the revocation.

[11] The *Judicial Interpretation* Article 13.

[12] *Id.*

[13] *Id.* Article 16.

[14] *Opinions on Issues relating to the Application of Law in the Handling of Criminal Cases Involving the Acceptance of Bribes* (关于办理受贿刑事案件适用法律若干问题的意见), released by Supreme People's Court and Supreme People's Procuratorate on July 8, 2007 and effective upon release, Article 11.

[15] The *Criminal Law of the People's Republic of China* (revised in 2015) Article 390.

[16] The *Judicial Interpretation* Article 14.

[17] *Id.*

China Releases Regulations on Internet Search Services and Mobile Apps

by Gabriela Kennedy and Xiaoyan Zhang
Mayer Brown JSM
5 July 2016

On 25 June 2016, the Cyberspace Administration of China ("CAC") published its new Administrative Provisions on Internet Information Search Services (the "Search Provisions"). Three days later, the Administrative Provisions on Mobile Internet Applications Information Services (the "Mobile Provisions") were released. Both Provisions will come into effect on August 1, 2016.

The Search Provisions impose several new obligations on Internet information search service providers ("Search Providers"), which are broadly defined as entities that "utilize computer technology to collect and process information on the Internet for retrieval by users". This includes search engines and social media providers. Search Providers shall: (1) adopt information security management systems to enable the review and real-time inspection of the information by the relevant government agencies, and protection of personal information; (2) not post or allow obscene content and other content prohibited by laws; (3) block the search results prohibited by laws and report them to the CAC; (4) provide search results that are objective, impartial and authoritative; (5) mark paid search results and segregate them from natural search results; and (6) establish comprehensive systems for public complaints and reports.

The release of the Search Provisions was triggered by the death of a young man, who chose a hospital based on an Internet search on a Chinese search engine but received ineffective hospital treatment not yet fully approved.

The Mobile Provisions govern mobile Internet application providers ("Mobile Providers") where mobile Internet applications refer to "application software obtained through pre-installation or downloads and which is used in mobile smart terminals to provide information services to users." Mobile Providers need to satisfy six requirements when operating in China: (1) verify new app users' mobile phone numbers and other identity information; (2) abide by the principles of legality, propriety and necessity when collecting and processing personal data; (3) have sanctions in place for users who publish content that violates applicable laws and regulations, and report the same to the relevant government agencies; (4) not access location, address books, cameras, audio recording or other functions unrelated to the service provided or bundle the application with unrelated applications without users' express consent; (5) respect and protect intellectual property rights ("IP"); and (6) record user logs and keep them for at least sixty days.

The Mobile Provisions also impose some similar obligations on mobile Internet application stores ("Mobile Stores"). For example, Mobile Stores are required to share management responsibilities by verifying the legitimacy of the Mobile Providers and requiring them to respect users' privacy and IP rights.

The Mobile Provisions are aimed to curtail the use of mobile apps that incite violence, terrorism, fraud, or pornography, or infringe users' privacy according to the CAC. The number of mobile Internet users in China stood at 619 million in 2015 and over four million mobile applications are currently available from domestic Mobile Stores with the number increasing rapidly.

While both Provisions impose obligations on providers to sanction content and report violations to government agencies, they do enhance users' overall online privacy and IP. Specifically, the requirement that express consent must be given before accessing certain functions of a mobile device may prove critical in managing any threats to mobile privacy.

These articles are provided for general information purposes only, and do not represent the views or opinions of the British Chamber of Commerce Shanghai.