漢坤律師事務所
HAN KUN LAW OFFICES

Newsletter

4th Edition of 2017

Legal Updates

Legal Updates

1. The Unveiling of Cybersecurity Reviews (Authors: David TANG, Min ZHU)

On May 2, 2017, the Cyberspace Administration of China ("**CAC**") issued a trial version of the *Measures for the Security Review of Network Products and Services (Trial)* ("**Trial Measures**"), which are slated to become effective on June 1. The Trial Measures are another supporting document of the Cybersecurity Law that is intended to enact the cybersecurity review requirements of Article 35 of the Cybersecurity Law, following its issuance on November 7, 2016.

Changes in the Trial Measures

Compared to the original draft for comment version of the measures ("**Draft**") issued by CAC on February 4, 2017, the Trial Measures make a number of clear adjustments, which mainly include:

a. References to the "public interest" have been removed throughout the regulation. We understand that "public interest" is an ambiguous and broad concept that may lead to a scope that is beyond the boundaries of the cybersecurity review. Thus, the removal of public interest provides for a clearer regulatory scope for the Trial Measures, and is also more in line with the original focus of national cybersecurity review.

b. The security review criteria have been made clearer. The Trial Measures expressly stipulate that the cybersecurity review includes static reviews (security risks of the products and services themselves) and dynamic reviews (supply chain security risks to products and key components, including in the process of production, testing, delivery and technical support), based on the secure and controllable requirements.

c. Reiteration of key industries and sectors. In coordinating with the Critical Information Infrastructure ("**CII**") provisions in Article 31 of the Cybersecurity Law, the Trial Measures reiterate that the key areas subject to cybersecurity reviews are public communications, information services, energy, transportation, water conservancy, finance, public services and e-government, and others key industries and sectors. It is worth mentioning that the Trial Measures remove the "party and government offices" language found in the Draft. We understand that party and government offices have their own security review mechanism, so it is unnecessary to specifically regulate these entities in the Trial Measures.

Main Content of the Trial Measures

The Trial Measures contain the following aspects that are worthy of note:

a. No administrative access approvals, focus on concurrent and post-event regulation

Throughout the Trial Measures, emphasis is placed on concurrent and post-event regulation rather than setting new market access administrative licensing for network product and service providers. The Trial Measures stipulate in Article 2 that "important network products and services purchased for networks and information systems that relate to national security must pass a cybersecurity review." Article 3 further provides that "cybersecurity reviews of network products and their providers and supply chains shall be carried out by a combination of enterprise commitment and social supervision, of third-party evaluations and continuous government oversight, and of laboratory testing, on-site inspections, online monitoring and background investigations."

b. Security Review Criteria: Secure and controllable

From the outset of cybersecurity legislation, "secure" and "controllable" have been the two concepts that are most referred to by legislators and regulators, and the Trial Measures again confirm these concepts as the basic principles guiding the Cybersecurity Law and its implementation. Article 4 of the Trial Measures states that security reviews shall focus on security and controllability, including: 1) security risks of the products and services themselves, and the risk of being illegally controlled, interfered with or interrupted in the course of operating; 2) supply chain security risks to products and key components; 3) risk of illegal collection, storage, processing and use of user information by providers of such products and services; 4) risks of harming cybersecurity and users' interests, and 5) other risks that may harm national security.

Of these criteria, 1) and 2) evaluate the ability to defend against risks, and 3) and 4) prohibit active infringing conduct. These criteria give consideration to both the active and passive aspects of cybersecurity, but remain concepts in principle. Without further guidance, it is difficult to predict the scope and standard of cybersecurity reviews in practice, and the relevant reviewers appear to be left with broad discretion in this regard.

c. Multi-party participation, striving for due process

The Trial Measures primarily place emphasis on the cybersecurity review process, as shown by Articles 5 to 10. These articles reflect administrative participation and due process under the modern administrative procedure law.

For example, from the perspective of participants, the Trial Measures involve the cybersecurity review commission (a newly established agency), cybersecurity review office, cybersecurity review experts committee, third-party institutions, national industry associations, users, competent departments in their respective industries and sectors, CII protection departments, and, from the perspective of process, the Trial Measures refer to expert evaluations, social supervision and public participation, among others.

It is clearly observable, however, that the final decisions relating to cybersecurity reviews are to be made by government regulators. Therefore, in contrast to the principle of simplifying administrative procedures, referred to as "small government and big society," legislators still desire to exert a certain

degree of greater governmental power in the area of cybersecurity.

d. Reviews to be commenced by regulatory departments

The Trial Measures also make clear the procedures for launching cybersecurity reviews. Article 8 of the Trial Measures state that the cybersecurity review office shall commence security reviews in accordance with the relevant national requirements, and take into consideration the suggestions of national industry associations and user feedback. Article 9 requires that competent departments of key industries and sectors, such as finance, telecommunications, energy and others, shall organize cybersecurity reviews of network products and services within their respective industries and sectors according to the national cybersecurity review requirements.

Compared to the Draft, the Trial Measures remove the application by enterprises as an option to commence cybersecurity reviews. That is to say, enterprises no longer have the right to initiate security reviews, and, in necessary situations, most can only promote security reviews via industry associations or other indirect means. This is also consistent with the government's position mentioned above, the government is inclined to adopt active administration and proactive regulation for cybersecurity matters.

e. Security assessment reports: A black list for cybersecurity reviews?

Article 13 of the Trial Measures state that the cybersecurity review office will release assessment reports on the security of network products and services from time to time. No report format or content requirements have currently been provided. However, information we have gathered from the legislative process suggests that the assessment reports will not only include information on network products and services and their providers that pass reviews, but will also include a listing of those products, services and providers that have not passed. This information may be developed into an information disclosure system based on the "white list" and "black list," that may affect and direct the industry guidance.

In addition, a CAC official has said that the regulator will treat enterprises and products from China and other countries equally during cybersecurity reviews, and will not direct efforts at products and services from specific countries or regions, nor limit foreign products from entering the domestic market. However, as the cybersecurity reviews focus on "national security," it remains to be seen whether the reviews will raise certain invisible barriers to market access in China for products and services provided by foreign enterprises or domestic joint-ventures.

Advice

Strictly speaking, cybersecurity reviews for network products and services do currently exist. There are certain national quality standards, industries access and enterprise qualification requirements for special industries, products and services, and enterprises themselves may have their own product security and industry standards. Until now, however, no specialized regulation has been enacted to

confirm a unified system and standard for such cybersecurity reviews. The issuance of the Trial Measure marks the commencement of nationally-led cybersecurity reviews.

The Trial Measures are still a basic guidance for the cybersecurity review of network products and services based on its current content, which will require further development and refining. Such issues include, for example, organizing the cybersecurity review commission and experts committee, identifying third-party institutions, evaluating criteria that affect national security and related review processes and working rules.

While detailed regulations are on the way, the related penalties are clear. According to Article 65 of the Cybersecurity Law, CII operators using products or services which have not undergone or have failed security reviews will be ordered by the competent department to stop such use and may be subject to a fine equivalent to more than 1 but less than 10 times the purchase price, and the supervisor directly in charge and other persons directly responsible will be subject to fines ranging from 10,000.00 yuan to 100,000.00 yuan. It can thus be said that the penalty ceiling is relatively high.

We would therefore recommend that network operators and providers of network products and services, especially CII operators in key industries and sectors, conduct self-reviews of network products and services they have purchased or which they provide to others in order to make improvements according to the secure and controllable requirement, and keep open communications with industry regulators and industry associations, and to watch for further developments in this area.

==========

2. Personal Information Protection from the Perspective of Criminal Law (Authors: David TANG, Min ZHU, Will HUANG)

On May 9, 2017, the Supreme People's Court and the Supreme People's Procuratorate held a press conference to release the *Interpretations of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Concerning the Application of Law in the Handling of Criminal Cases Involving Infringement of Citizens' Personal Information* (the "**Interpretations**"), which will be effective from June 1, 2017.

To protect citizens' personal information, in 2009, the crimes of "illegally selling or providing of the personal information of citizens" and "illegally acquiring the personal information of citizens" were added in *Amendment VII to the Criminal Law of the People's Republic of China*. In 2015, *Amendment IX to the Criminal Law of the People's Republic of China* combined the two crimes into one, the "infringement of citizens' personal information." The Interpretations set forth more practical conviction and sentencing criteria for the infringement of citizens' personal information and mark a

milestone for the criminal protection of citizens' personal information.

Several key concepts

The Interpretations make clearer several concepts regarding the crime of "infringement of citizens' personal information" stipulated by Article 253A of the *Criminal Law of the People's Republic of China* (the "**Criminal Law**"):

a. **Citizens' personal information:** Article 1 of the Interpretations expands the scope of "citizens' personal information" from personal identification information to identification and activity information, which includes names, identity document numbers, correspondence and contact information, addresses and other identification information, account passwords, property status, whereabouts and other activity information relating to particular natural persons.

b. **Provision:** Article 3 of the Interpretations specifies that the "provision of citizens' personal information" not only includes the act of providing personal information of citizens to particular persons, but also refers to releasing such information through the information networks or through other channels. In addition, citizens' personal information that is legally collected can still be considered the "provision of citizens' personal information" if the collector of the information provides it to others without the consent of the information subject, unless the information has been processed, the particular person cannot be identified, and the information cannot be recovered after processing.

c. **Unlawful acquisition:** Article 4 of the Interpretations specifies two standards for determining the "unlawful acquisition of citizens' personal information" stipulated by Article 253A of the Criminal Law, which refer to acquiring citizens' personal information by way of purchase, acceptance or exchange in violation of the relevant provisions of the State, or collecting such information during the process of performing duties in violation of the relevant provisions of the State.

What are "serious circumstances"?

According to Article 253A of the Criminal Law, "serious circumstances" constitutes the prerequisite for the crime of "infringement of citizens' personal information." The Interpretations specify the relevant standards for determining "serious circumstances" based on different forms of conduct. Article 5 of the Interpretations sets forth clear standards for determining the illegal acquisition, sale or provision of citizens' personal information. Article 6 sets forth standards for determining "serious circumstances" regarding "illegally buying or accepting citizens' personal information for lawful business activities." The Interpretations specify the standards for determining "serious circumstances" based on the information type and quantity, usage of information, identity of the information subjects, subjective viciousness and other aspects:

a. **Information type and quantity:** There are various types of citizens' personal information. The Interpretations set forth different standards for what constitutes "serious circumstances" based

on the importance of different types of personal information as detailed below:

No.	Information Type	Determining Standard
1	Information on whereabouts, communication, credit information, property information.	More than 50 pieces
2	Accommodation information, communication records, health and physiological information, transaction information and other personal information that may affect personal and property safety.	More than 500 pieces
3	Citizens' personal information other than that described above.	More than 5,000 pieces

b. Amount of illegal income: People commonly sell or illegally provide citizens' personal information for profit. Therefore, the Interpretations stipulate that receiving illegal income over RMB 5,000 is a "serious circumstance."

c. Usage of information: Different uses of citizens' personal information that is illegally obtained, sold or provided, will result in varying degrees of harm to information subjects. Therefore, the Interpretations stipulate that the following circumstances are "serious circumstances":

i. selling or providing information on citizens' whereabouts, which is used by others for the commission of a crime;

ii. knowing or should have known that others are to use the personal information of citizens to commit crimes, but continuing to sell or provide such information.

d. Principal identity: Many information leakage cases are conducted by insiders. To crack down on such crime, the Interpretations lower the conviction criteria for information leakage from insiders. If people sell or provide others with citizens' personal information obtained in the performance of duties or the provision of services, it will be considered a "serious circumstance" if the number pieces or amount of information is greater than one half of the conviction criteria shown above.

e. Previous convictions: According to the Interpretations, if a person has ever received criminal punishment or has received administrative punishment within the last two years for the infringement of citizens' personal information, and again illegally acquires, sells or provides citizens' personal information, that person's conduct will be determined to be a "serious circumstance."

f. Special provisions: In practice, illegally purchased and accepted personal information is generally used for advertising promotions. Article 6 of the Interpretations sets forth conviction criteria under this circumstance. Under any of the following circumstances, illegally buying or accepting citizens' personal information (other than those mentioned in Items 3 and 4 of the first paragraph of Article 5 of the Interpretations) for lawful business activities shall be determined to

be a "serious circumstance":

iii. the profit from the illegally purchased or accepted personal information of citizens reaches RMB 50,000;

iv. those involved have ever been subject to criminal punishment or have received administrative punishment within the last two years for infringement of personal information of citizens, and are again illegally purchasing, selling or providing personal information of citizens; and

v. other serious circumstances.

What are "particularly serious circumstances"?

After defining "serious circumstances," the Interpretations set forth specific standards for "particularly serious circumstances" in both qualitative and quantitative ways:

a. Quantity standards: The Interpretations set forth different standards for "particularly serious circumstances" based on the importance of different types of personal information as detailed below:

No.	Information Type	Determining Standard
1	Information regarding whereabouts, communication, credit information, property information.	More than 500 pieces
2	Accommodation information, communication records, health and physiological information, transaction information and other personal information that may affect personal and property safety.	More than 5,000 pieces
3	Citizens' personal information other than that described above.	More than 50,000 pieces

b. Serious consequences: According to the Interpretations, acts which "cause serious consequences such as death, serious injury, mental disorder or kidnapping of the victims" or "cause significant economic losses or adverse social effects" are determined to be "particularly serious circumstances."

How is the quantity of information calculated?

In practice, a single case often involves citizens' personal information that is mixed or possibly contains many different types of information. Under this circumstance, the Interpretations specify that the quantity of information can be converted according to a corresponding ratio.

Consider the information type and quantity under the aforementioned "serious circumstances." If the quantity of information does not meet the standard of 50 pieces, 500 pieces or 5,000 pieces as shown in the table above, the quantities of information will be converted according in the ratio of 1,

10 or 100 times. The incident may be criminally investigated if the total quantity calculated according to the corresponding proportion meets the relevant standard. For example, when investigating a case, 20 pieces of type 1 information are found and 350 pieces of type 2 information are found, and the total pieces of the two types of information does not meet the respective standards of 50 pieces or 500 pieces. In this case, according to the Interpretations, the information quantity would be converted according to a ratio of 10. 350 pieces of type 2 information will be converted into 35 pieces of type 1 information and the total number will be 55 pieces, which meets the criminal standard. In other words, 20 pieces of type 1 information may also be converted into 200 pieces of type 2 information and the total number will be 550 pieces, which will also meet the standard of 500 pieces.

Article 11 of the Interpretations stipulates that the quantity of citizens' personal information is not to be counted multiple times when the same information is first illegally acquired and then sold or provided to another party. If the same citizen's personal information is sold or provided to different entities or individuals, however, the quantity of the citizen's personal information is to be aggregated based on each such transfer. The quantity of citizens' personal information found in batches will be directly determined according to the amount of such information, unless there is evidence that the information is not true or is duplicative.

What should enterprises pay attention to?

In general, the Interpretations set forth clearer conviction and sentencing criteria for the crime of infringement of citizens' personal information, which aims to strike at such crime by lowering the relevant criteria to some degree. We would therefore recommend that enterprises pay attention to the following issues:

a. Expansion of legal sources regarding protection for personal information

In accordance with Article 2 of the Interpretations, "violating relevant national provisions" mentioned in Article 253A of the Criminal Law means the violation of laws, administrative regulations, and departmental rules on the protection for personal information of citizens. What needs to be focused on is that the legal sources cited here are an extension of the laws and administrative regulations, which were common in previous legislative practice for departmental rules. In this manner, the Interpretations greatly expand the amount of applicable regulatory documents that cover personal information protection. In practice, the ministries and commissions of the State Council and their authorized agencies may issue departmental rules regarding the protection of personal information. Such authorities generally include: National Health and Family Planning Commission of the PRC, Ministry of Human Resources and Social Security of the PRC, Ministry of Industry and Information Technology of the PRC, Ministry of Science and Technology of the PRC, the People's Bank of China, China Banking Regulatory Commission, China Securities Regulatory Commission, China Insurance Regulatory Commission, State Ministry for Industry & Commerce of the PRC, China Food and Drug

Administration, Cyberspace Administration of China, and so on.

b. Enterprise management to face increased risk of criminal liability

In accordance with Article 7 of the Interpretations, entities that commit crimes specified in Article 253A of the Criminal Law will be subject to the conviction and sentencing criteria for natural persons in accordance with the Interpretations. Officers directly in charge and other persons directly responsible will be punished, and the entities will also be fined. As stated above, the Interpretations lower the conviction and sentencing criteria for the infringement of citizens' personal information. In addition, a noteworthy trend in current the departmental rulemaking by some authorities is that natural persons must be punished for their own illegal acts or the illegal acts of entities which they oversee or are responsible for. Therefore, it is no exaggeration that enterprise management personnel now face higher risks of criminal liability in relation to personal information and big data services.

c. Defense of lawful business activities

The Interpretations clearly stipulate that it is a "serious circumstance" potentially subject to criminal liability when a person illegally buys or accepts citizens' personal information for lawful business activities, and obtains profits of more than RMB 50,000 by virtue of such information (other than those specified in Items 3 and 4 of the first paragraph of Article 5 of the Interpretations). Therefore, as an enterprise whose business involves personal information, "lawful business activities" obviously cannot be a defense against criminal liability. Considering this, such enterprises should establish or improve their internal processes and controls regarding collecting personal information, while also reviewing contractual provisions regarding personal information in services agreement between themselves and their customers, thereby legally collecting and using personal information necessary for business.

d. Desensitizing personal information

In coordinating with provisions of the Cyberspace Law, the Interpretations stipulate that it shall be determined as an illegal act to provide others with lawfully collected personal information of citizens without the consent of those whose information is collected, unless such information has been processed to the degree where the particular person cannot be identified and such identifying information cannot be recovered. However, a large quantity of desensitized information and data can actually be recovered to some degree by virtue of technology. Therefore, it is a technological challenge to relevant enterprises to achieve true desensitization, to reach the degree where a particular person cannot be identified and such identifying information cannot be recovered. Failing to achieve desensitization will no longer merely result in civil or administrative liability.

e. Information leakage from insiders

Information leakage from insiders is an existing problem in industries with respect to the protection of personal information and big data. Considering this, the Interpretations lower the conviction

criteria for information leakage from insiders. If people sell or provide others with citizens' personal information obtained in the performance of duties or provision of services, and the number or amount of which has reached more than half of the conviction criteria mentioned above, the case will be determined a "serious circumstance." We would therefore recommend that relevant enterprises to improve employee management by

i. making specific guidance regarding how to legally obtain, use and protect personal information of citizens when performing their duties or providing services;

ii. improving internal control policies and compliance training, thereby protecting enterprises from harmful consequences caused by the acts of their employees.

==========

3. Internet News Information Service Industry Reshuffle? (Authors: Sheng LI, Xi YAN)

On May 2, 2017, the Cyberspace Administration of China promulgated the *Administrative Provisions for Internet News Information Services* ("**Provisions**"), which will come into effect on June 1, 2017 and replace the existing *Regulations for the Administration of Internet News Information Services* ("**Regulations**") which was promulgated in 2005.

The Provisions preserve a part of the Regulations, while making significant changes with respect to both structure and content. This article will provide a brief analysis of the Provisions, primarily with respect to businesses subject to licensing requirements, entry requirements and the relevant responsibilities of license subjects.

Businesses required to obtain an Internet News Information Service License

The core requirements of the Provisions are identical to those of the Regulations, which are that operators engaging in Internet news information services must obtain an Internet News Information Service License, and be subject to the supervision and management of the Cyberspace Administration of China.

Compared to with the Regulations, the Provisions more clearly define Internet news information services, mainly from the following three aspects:

a. Content: The Provisions clearly explain that "news information" refers to reports and commentary related to political, economic, military, diplomatic and other social and public affairs and reports on social emergencies (which means that general sports, culture, science and technology news and news of a commercial nature would not be regarded as "news information" under the Provisions);

b. Communication channels: The Provisions clearly provide that news information services are provided to the public through channels based on the technology and developmentsof the times, including Internet sites, apps, forums, blogs, micro-blogs, public accounts, instant messaging tools and network-based broadcasts; and

c. Form of services: Depending on the service provider's specific work, the Provisions further classify Internet news information services into three categories: Internet news information editing and publishing services, Internet news information reposting services and Internet news information dissemination platform services.

Based on the definitions and understandings above, operators who engages in Internet news information editing and publishing services, reposting services or dissemination platform services such as Weibo, WeChat and network-based broadcasting platforms are required to obtain an Internet News Information Service License in accordance with the Provisions, although the existing Regulations would not currently require obtaining a license. Based upon our past experience, it would be quite difficult for some small service providers to obtain an Internet News Information Service License, if they have not yet done so. Failure to obtain a license could result in an order to cease operating.

Qualifications for Obtaining an Internet News Information Service License

With respect to the entry of foreign capital, the Provisions preserve the rules found in the Regulations which provide that an Internet news information service entity cannot be established in the form of a Sino-foreign joint venture, a Sino-foreign cooperative venture or a wholly foreign-invested enterprise. Where an Internet news information service entity intends to cooperate with a Sino-foreign joint venture, Sino-foreign cooperative venture or wholly foreign-invested enterprise, the entity should report to the competent authorities for a security assessment. In addition, the Provisions also require the person in charge and the editor-in-chief of Internet news information service entities to be PRC citizens. It is worth noting that the Provisions for the first time require Internet news information service providers to separate editing services from other business operations and clearly provide that non-public capital cannot be used to operate Internet news information editing services. Besides this, the Provisions also set forth that only news entities (including its controlled entities) or entities controlled by the news and publicity department are eligible to apply for an Internet News Information Editing and Publishing Service License. To some extent, these provisions reflect the government's strengthened management of the Internet news editing business and of the content of news information.

The Regulations have clear requirements regarding registered capital and the number of employees for applicants of the Internet News Information Service License. For example, Internet news information service units established by non-news entities must have registered capital of no less than RMB 10 million and more than 10 full-time news editors. The Provisions delete such

requirements and only generally require that applicants should have the premises, facilities and funds, full-time news editors, content reviewers and technical security personnel appropriate for the services, and should establish sound Internet news information service management systems, information security management systems and technical support measures. Based upon our experience, these general requirements are not easy to apply, and the authorities are very likely to put forward specific requirements in practice. In the short term, it is quite likely that the authorities will review applications according to requirements provided in the Regulations in the absence of enforcement rules for the Provisions that may be promulgated.

In addition, similar to the *Administrative Provisions on Internet Publishing Services*, the Provisions also further require qualified Internet news information service providers to implement a special management share system, and specific implementing rules will be separately developed by the Cyberspace Administration of China. The following issues require special attention with respect to the special management share system:

a. Will the special management share system only apply to news editing and publishing service providers or will it apply to all three categories of service providers (i.e., news editing and publishing service providers, news reposting service providers and dissemination platform service providers)?

b. Is there a minimum limit for the shareholding ratio for state-owned special management entities (for example, at least 1%)? How will control rights of the state-owned special management entities be ensured (whether the state-owned investor will have a seat on the board of directors or whether the investor will have veto rights with respect to news content)?

There is no doubt that the special management share system, if implemented, will have a significant impact on the financing and listing of Chinese companies that use a VIE structure or on Chinese companies that intend to be listed overseas.

Responsibilities of Internet news information service providers

The Provisions classify Internet news information services into Internet news information editing and publishing services, reposting services and dissemination platform services. In addition to the general requirements applicable to all Internet news information service providers regarding editor and practitioner management, information security management, content dissemination management and the treatment of illegal information, the Provisions also provide certain special requirements related to the three categories of service providers mentioned above:

a. The Provisions provide that entities engaging Internet news information editing and publishing services should be a news entity (including its controlled units) or a unit controlled by the news and publicity department, which refers to news organizations in the conventional sense.

b. The Provisions require that providers of news reposting services should repost news published by central news entities or their direct local subordinates and should indicate the news source, the original author, the original title and the editor's real name. Providers must not distort or tamper with the meaning of the original title or the news content, and should ensure that the news information can be traced to its source.

c. The Provisions requires Internet news information platform service providers to require users to provide real identity information and cannot seek improper benefits by editing, publishing, reposting or deleting news information, or through interfering in the presentation of news information or search results. Providers should also sign agreements with registered users and audit the users' public accounts with respect to account information, service qualifications and service scope and file the same with the competent authorities based upon the category of the user.

Attachment: Comparison of Core Rules between the Provisions and Regulations

(Note: The English clauses are quoted from lexiscn.com.)

Items	Regulations	Provisions
Competent Authority	Article 4 The Information Office of the State Council is responsible for supervising and administering Internet news information services throughout China. The information offices of the people's government of the provinces, autonomous regions, or municipalities directly under the Central Government are responsible for supervising and administering the Internet news information services within their own jurisdiction.	Article 4 The Cyberspace Administration of China is in charge of the supervision, administration and law enforcement throughout China with regard to Internet news information services. Local cyberspace administrators are responsible for the supervision, administration and law enforcement regarding the Internet news information services within their own jurisdiction, depending on their respective functions and duties.
Applicable Scope	Article 2 Internet news information services as mentioned in the present Regulations include the services of publishing news information via Internet, providing electronic bulletin services on current affairs and politics, and transmitting communicative information on current affairs and politics to the public.	Article 5 Anyone who intends to provide the public with news information services on the Internet via Internet websites, applications, forums, blogs, micro-blogs, official accounts, instant message tools, network-based broadcast, etc. shall obtain a permit for Internet news information services, and is forbidden to carry out any activities concerning Internet news information services without the permit or beyond the permitted scope.
License Category	Article 5 Internet news information service providers are classified into the following three categories: 1. Internet news information service providers established by news entities to publish the news other than those that have not been published and broadcasted by the said entities, to provide electronic bulletin services relating to current affairs and politics, and to transmit communicative information of current affairs and politics to the public; 2. Internet news information service providers established by	Article 5 Internet news information services as mentioned in the preceding paragraph include services of collecting, editing and releasing Internet news information, reposting such news information and providing a platform to spread such news information.

	non-news entities to re-publish news information, to provide electronic bulletin services relating to current affairs and politics, and to transmit communicative information of current affairs and politics to the public; 3. Internet news information service providers established by news entities to publish the news information which has been published or broadcasted by the said news entities.	
Application Conditions	Article 7 The applicant shall satisfy the following conditions when applying for the establishment of an Internet news information service provider as stipulated in Item 1 of Paragraph 1 of Article 5 of the present Rules: 1. Having sound rules and regulations on the management of Internet news information services; 2. Having not less than 5 full-time news editors who have engaged in the news work in a news entity for more than 3 years; 3. Having the necessary location, equipment and funds, and the sources of the funds being legal. Article 8 When applying for establishing an Internet news information service provider as stipulated in Item (2) of Paragraph 1 of Article 5 of the present Rules, the applicant shall not only satisfy the conditions stipulated in Items 1 and 3 of Paragraph 1 of Article 7 of the present Rules, but also have not less than 10 full-time news editors, among whom there shall be not less than 5 news editors who have engaged in the news work in a news entity for more than 3 years. An organization that is allowed to apply for establishing an Internet news information service provider as stipulated in the	Article 6 Any party that plans to apply for a permit for Internet news information services shall satisfy all of the following requirements, 1. It is a legal person legally established within the territory of the People's Republic of China; 2. Its principal or chief editor is a Chinese citizen; 3. It is staffed by full-time news editors, content reviewers and technical support engineers who are suitable for its services; 4. It has thorough management systems for Internet news information services in place; 5. It has thorough management systems for information security in place and has taken safe and controllable measures for technical support; and 6. There are venues, facilities and capital that are appropriate for its services. The party applying for a permit for services of collecting and editing Internet news information shall be a news entity (including its controlled units) or a unit under the administration of the news propaganda department. The special management share system may be applicable to those Internet news information service providers that meet certain conditions.

	preceding paragraph shall be a legal person that has lawfully established for more than 2 years to provide Internet information services, and has not been given any administrative sanction within the latest 2 years due to violation of laws, regulations and rules for the administration of Internet information services. If the applicant organization is a legal person of enterprise, its registered capital may not be less than RMB 10 million Yuan.	Specific implementing measures will be enacted by the Cyberspace Administration of China separately.
Admission for News Collecting and Editing Services	**/**	(newly added) Article 8 Internet news information service providers shall separate their news collection and editing services from other operational businesses. Non-government-owned capitals shall not be used for services of collecting and editing Internet news information.
Personnel Qualifications	**/**	(newly added) Article 11 An Internet news information service provider shall establish a post of chief editor who will be responsible for the content of Internet news information. The candidate for the chief editor shall have relevant practice experience and satisfy relevant conditions. The candidate's name shall be submitted to the Cyberspace Administration of China or the local cyberspace administrator of a province, autonomous region or municipality directly under the Central Government for record-filing purposes. Relevant practitioners of Internet news information services shall obtain necessary qualifications and receive professional training and assessment in accordance with the law. If they would like to engage in activities to collect and edit news information, they shall also have the occupational qualifications for being news editors and reporters and hold the press card issued by the State Administration of Press, Publication, Radio, Film and Television in a unified manner.

Dissemination Platform Responsibility	**/**	(newly added) Article 13 An Internet news information service provider shall request its users to submit their real identification information in accordance with the provisions of the Cybersecurity Law of the People's Republic of China, provided that it provides such users with a platform to disseminate news information on the Internet. Where any user refuses to provide its real identification information, the Internet news information service provider is not allowed to provide it with relevant services. Any Internet news information service provider shall be obligated to maintain the confidentiality of information pertaining to its users' identification and logs, and shall neither divulge, falsify or destroy such confidential information, nor sell or illegally provide others with such confidential information. Any Internet news information service provider as well as its practitioners shall not seek unjustified profits by collecting and editing, releasing, reposting and deleting certain news information or otherwise for the purpose of interfering with the presentation or search results of news information. Article 14 Where an Internet news information service provider provides a platform for spreading Internet news information, it shall enter into an agreement with any user who registers for an account on its platform, so as to specify both parties' rights and obligations. In the event that a user sets up an official account, the Internet news information service provider shall verify its account information, service qualifications, scope of services and other information, and file a record of the same by category with the local cyberspace administrator of the province, autonomous region or municipality directly under the Central

		Government at its locality.
Reposting Cooperation	Article 16 In case an Internet news information service provider as stipulated in Item 1 or Item 2 of Paragraph 1 of Article 5 of the present Rules publishes any news information or transmits any communicative information on current affairs and politics to the public, it shall do so by either news entities of the Central Government or news entities directly under the people's government of a province, autonomous region, or municipality directly under the Central Government, give a clear indication of the sources of the news information, and may not misrepresent the contents of the original news information. An Internet news information service provider as stipulated in Item 2 of Paragraph 1 of Article 5 of the present Rules may not publish the news information gathered and edited by it. Article 17 In case an Internet news information service provider as stipulated in Item 1 or Item 2 of Paragraph 1 of Article 5 of the present Rules publishes any news information, it shall conclude a written agreement with the news entity of the Central Government or the news entity directly under the people's government of a province, autonomous region, or municipality directly under the Central Government. The Internet news information service provider established by a news entity of the Central Government shall submit a copy of the agreement to the Information Office of the State Council for record; while any other Internet news information service provider shall submit a copy of the agreement to the relevant local information office of	Article 15 An Internet news information service provider, if to repost any news information, shall repost the news information released by the range of units enumerated by the State, such as the central news entity or the news entity directly affiliated to a province, autonomous region, and municipality directly under the Central Government, and specify the source of the news information, its original author, the previous title, and the real name of the editor. It shall not distort or tamper with the original meaning of the title or content of the news information, and is required to guarantee the possibility to trace the origin of the news information. Any Internet news information service provider shall abide by the provisions of copyright-related laws and regulations when reposting any news information, and protect the legitimate rights and interests of the copyright holders.

	the people's government for record. A news entity of the Central Government or a news entity directly under the people's government of a province, autonomous region, or municipality directly under the Central Government shall check the other party's license for Internet news information services when concluding the agreement as stipulated in the preceding paragraph. And it may not provide any news information to an entity that has no license for Internet news information services. Article 18 In case a news entity of the Central Government plans to cooperate with an Internet news information service provider as stipulated in Item 2 of Paragraph 1 of Article 5 of the present Rules in Internet news services other than making contributions, it shall, 10 days before engaging in business cooperation, report of such intention, to the Information Office of the State Council; in case any other news entity plans to cooperate with an Internet news information service provider as stipulated in Item 2 of Paragraph 1 of Article 5 of the present Rules in Internet news services other than making contributions, it shall, 10 days before engaging in business cooperation, report of such intention to the relevant local information office of the people's government of the province, autonomous region, or municipality directly under the Central Government.	

Important Announcement

This Newsletter has been prepared for clients and professional associates of Han Kun Law Offices. Whilst every effort has been made to ensure accuracy, no responsibility can be accepted for errors and This Newsletter has been prepared for clients and professional associates of Han Kun Law Offices. 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.

If you have any questions regarding this publication, please contact:

Contact Us

Beijing Office
Tel.: +86-10-8525 5500
9/F, Office Tower C1, Oriental Plaza
No. 1 East Chang An Ave.
Beijing 100738, P. R. China

Estella CHEN Attorney-at-law
Tel.: +86-10-8525 5541
Email: estella.chen@hankunlaw.com

Shanghai Office
Tel.: +86-21-6080 0909
Suite 5709, Tower 1, Plaza 66, 1266 Nanjing West Road,
Shanghai 200040, P. R. China

Yinshi CAO Attorney-at-law
Tel.: +86-21-6080 0980
Email: yinshi.cao@hankunlaw.com

Shenzhen Office
Tel.: +86-755-3680 6500
Room 2103, 21/F, Kerry Plaza Tower 3, 1-1 Zhongxinsi Road, Futian District, Shenzhen 518048, Guangdong, P. R. China

Jason WANG Attorney at-law
Tel.: +86-755-3680 6518
Email: jason.wang@hankunlaw.com

Hong Kong Office
Tel.: +00852-2820 5600
Suite Rooms 2001-02, 20/F, Hutchison House, 10 Harcourt Road, Central,
Hong Kong, P. R. China

Dafei CHEN Attorney at-law
Tel.: +852-2820 5616
Email: dafei.chen@hankunlaw.com