Hogan Lovells

TMT developments in China

Contents

China's new national security law – new hurdles for technology companies? 4

China's draft cyber security law proposes more stringent regulation of cyberspace 7

E-commerce liberalization kicks off in China 9

Chinese court provides guidance on lawful use of cookies 13

A right to be forgotten in Hong Kong? 16

Supreme People's Court clarifies certain patent dispute rules 19

MIIT think-tank issues white papers on mobile internet industry 20

China opens up domestic bank card clearing market to foreign competition 23

Merger control in Hong Kong's telecom industry – emperor's new cloths? 25

Drive towards "more market" in China's standard-setting process 28

China's first antitrust regulation against IPR abuses 30

SUMMER 2015

Editor's note

The first half of 2015 has seen a number of landmark developments shaping China's TMT sector.

Since becoming the world's largest online retail market in 2013, China's e-commerce market has continued to expand at a much higher rate than the economy overall. China's online retail market reportedly totalled USD 450 billion in 2014, with the most rapid growth now being seen in outlying regions underserviced by traditional retail businesses.

This explosive growth has been well received by the Chinese authorities, and so the e-commerce sector saw a flurry of market liberalisation measures in the second quarter, with the availability of 100% foreign participation in online data processing and transaction processing services being a highlight of the State Council's Opinions on Vigorous Development of E-Commerce, which were implemented through MIIT's Circular 196. The State Council followed with further important measures in June directed at encouraging cross-border e-commerce.

At the same time, the State Council's liberalisation of the payment clearance market in May creates the possibility of further payment services liberalisation in China, supporting the accelerating movements in e-commerce.

These developments bode very well for multinational participation in China's e-commerce and payments markets, but have been tempered somewhat by equally ground-breaking developments in cyber security regulation. July saw the passage of China's new National Security Law, which casts an extremely wide net for regulation of national security matters in China. The same month saw the publication of a draft Cyber Security Law that show a China increasingly conflicted by the desire to integrate in the global economy through technology and at the same time preserve its unique understanding of national security and stability. These tensions will be closely watched in coming months as multinationals evaluate the implications for technology deployment in China.

Other key developments show a greater China coming to grips with more advanced regulatory concepts that are critical to the TMT sector, including important antitrust developments in China and Hong Kong, cookie regulation and the possibility of a recognition of a "right to be forgotten" in Hong Kong.

We hope that you enjoy this selection of articles, which we believe represent a good cross-section of the vibrant developments in Greater China's TMT sector.

Mark Parsons
Partner, Hong Kong
T +852 2840 5033
mark.parsons@hoganlovells.com

Sherry Gong
Counsel, Beijing
T +86 10 6582 9516
sherry.gong@hoganlovells.com

China's new national security law – new hurdles for technology companies?

On 1 July 2015, the National People's Congress passed the National Security Law ("**NSL**"). It took effect from the date of promulgation. The concept of national security under the NSL is very broad, covering matters ranging across politics, the military, the economy, finance, culture, technology, territorial sovereignty, cyber security, ideology and religion. The NSL specifically identifies high technology and cyber security as areas that implicate national security.

Not surprisingly, the NSL's broad scope of application has created a great sense of foreboding amongst the foreign business community, including technology companies concerned with the law's impact on investments and future opportunities in China.

Broad definition of national security

The NSL defines national security as "the status whereby there is a relative absence of international or domestic threats to the state's power to govern, sovereignty, unity and territorial integrity, the people's welfare, sustainable economic and social development, and other significant national interests, as well the ability to maintain security on a continuous basis."

From a business perspective, the key concern is in the reference to "economic development" as being seen as part of China's national security – i.e., in addition to the existing laws and regulations, commercial activities and investments will be considered separately in the light of the broad and amorphous perspective of national security.

Expanded national security review regime

The NSL provides that certain types of foreign investments, key technologies, network information technology products and services ("**IT Products and Services**", the term "network" may extend the application of the NSR requirement beyond IT Products and Services delivered via the internet, another example of the broad theme of the NSL), construction projects and other major activities that have national security implications will be subject to broad national security review ("**NSR**") requirements.

NSR in relation to foreign investments

Prior to the enactment of the NSL, the Chinese government imposed NSR requirements on mergers and acquisitions ("**M&A**") involving the acquisition of Chinese companies by foreign investors. Separately, earlier this year, the Chinese government issued a set of rules, which pilot run a NSR regime for foreign investments (including M&A and greenfield non-M&A establishments by foreign investors) in China's free trade zones (i.e. the Shanghai Pilot Free Trade Zone, the Guangdong Pilot Free Trade Zone, the Tianjin Pilot Free Trade Zone, the Fujian Pilot Free Trade Zone and other pilot free trade zones).

With the NSR requirement in the NSL, it is anticipated that the full-blown regime for foreign investment scrutiny applicable in the free trade zones will be rolled out nationwide, subject to more specific implementing rules to be enacted. There may be a potential overlap between the NSR requirements and the above mentioned security review processes. The lack of clarity on the processes and requirements as well as key determinants of the review process is of concern.

Further, with the broad definition of the national security concept in the NSL, the scope of industrial sectors that may be subject to NSR is likely to grow. In the past, the Ministry of Commerce – one of the main authorities responsible for implementing NSR – listed 57 industry sectors where M&A transactions by foreign investors may be subject to the NSR under the NSR Circular. With the NSL, additional sectors may be subject to NSR scrutiny given the lack of clarity and specificity in the NSL. For example, more technology products, particularly concerning network and cyber security, may potentially become subject to the NSR process.

NSR for IT Products and Services

The NSL calls for the establishment of a domestic internet and information security safeguarding mechanism. In particular, the new law requires, in very broad terms, that core network technology, critical infrastructure, information systems and data in important areas be stored and kept "safe" and "controllable." Importantly, the NSL further creates a NSR requirement for IT Products and Services, the scope and procedure of which are not defined in the NSL.

The new NSR requirement will have significant implications for providers of foreign IT Products and Services operating or selling in China, which may already, be 'feeling the heat' as a result of the draft Anti-Terrorism Law, the draft Cyber Security Law, and other recent industry-specific rules and drafts. Clearly, international suppliers of IT Products and Services are likely to face significantly higher entry barriers

to the China market than their Chinese competitors. The overlapping rules will give the Chinese government authorities plenty of avenues through which they can scrutinize foreign products/services more closely and require disclosure of key know-how (e.g.,encryption technologies).

Implications for merger control review

Although the NSR and the merger control review run in parallel, the NSL may also have an impact on some complex merger control cases.

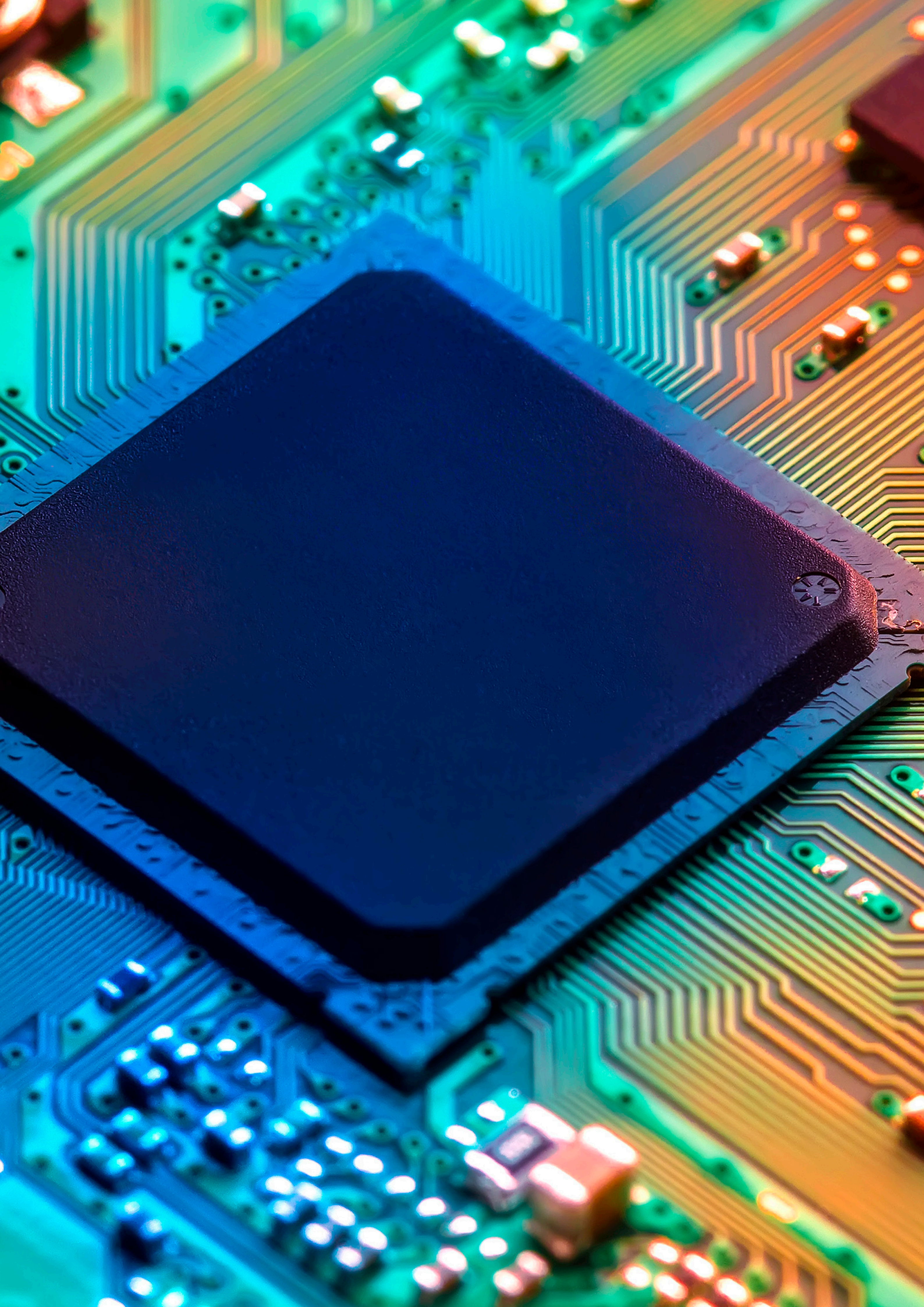
The Anti-Monopoly Law allows the Ministry of Commerce to consider in the merger control process "the impact of the concentration between business operators on the development of the national economy." Against this background, it is possible that the broad definition of national security in the NSL could further complicate the merger control review in China. For example, government departments that are more sensitized toward national security issues, such as the Ministry of National Security and the National Development and Reform Commission, may have additional incentives to get involved in the merger control process relating to specific transactions.

Conclusions

With the enactment of the NSL, foreign companies doing business in or with companies in China will need to brace themselves for further uncertainty until we have greater visibility on how the NSL will be implemented in practice. However the overall effect of this and other legislation currently going through the system is to make foreign investors increasingly nervous about the impact on their existing and future investments in China, and there is a worrying sense that China may be looking inwards rather than outwards for its future growth and prosperity.

Kurt Tiam
Counsel, Beijing
T +86 10 6582 9555
kurt.tiam@hoganlovells.com

Andy Huang
Associate, Beijing
T +86 10 6582 9533
andy.huang@hoganlovells.com



China's draft cyber security law proposes more stringent regulation of cyberspace

On 6 July 2015, the Legislative Affairs Commission of the Standing Committee of the National People's Congress issued a draft of the Cyber Security Law for public comment. The consultation period closed on 5 August 2015.

The draft Cyber Security Law incorporates many elements to be expected of a law aimed at mobilising a national cyber security strategy, including the identification of industry sectors of particular importance from a cyber security perspective and measures for cooperation in relation to standard-setting, development of protection systems, and the sharing of information about cyber incidents.

Interest and commentary on the draft law, however, have primarily come to focus on a number of specific measures dealing with more controversial issues such as technology regulation, access to systems and data by state authorities and data localisation, all of which are raised at a high level in the draft Cyber Security Law, with crucial details left to be determined in implementing regulations.

Technology regulation

The draft Cyber Security Law requires that "critical network equipment" and "specialised cyber security products" be inspected or certified by a qualified institution before they can be sold in China. An official catalogue principally authored by a yet-to-be-identified "national internet information department" is to decide which equipment and products will specifically be subject to this rule. While the point is not free from doubt, it appears likely that the Cyberspace Administration of the State Council Information Office will lead in establishing and maintaining the certification regime.

Security certification is an important area of focus for most multinationals dealing in China, in particular for technology companies that could be facing approval requirements. Inspections and certifications may delay a product's entry to the market. It also remains to be seen how invasive the proposed inspections of technology would be from the perspective of protecting valuable intellectual property.

Cooperation with authorities

The draft Cyber Security Law also requires "network operators" to provide necessary support and assistance if requested by investigating departments for reasons of national security or criminal investigation.

Network operators, a term of art used throughout the draft Cyber Security Law, is broadly defined and likely includes any businesses operating over networks and the internet, from basic carriers to companies operating websites.

The breadth of duties to cooperate with authorities in investigations is a concern for multinational technology service providers. There have been a number of well-publicised instances in which investigations by Chinese authorities have raised brand or public relations challenges for technology companies, and the network operator obligations – together with data localisation requirements under the draft Cyber Security Law – will be a critical area of focus for the sector.

Data localisation

The draft Cyber Security Law also imposes obligations upon "critical information infrastructure operators" to store personal information and other important data within China. Such information cannot be stored abroad or be provided to individuals or organisations outside China, unless it is "truly necessary" for the operation and the operator has conducted a security assessment in support of the offshore transfer. These security assessments would be carried out in accordance with measures to be jointly formulated by the state-level cyberspace administration authorities and the relevant departments under the State Council (such as presumably the Ministry of Industry and Information Technology).

"Critical information infrastructure," under the draft law, applies to a number of industries, including:

- basic information networks that supply public communications, radio and television transmission services
- important information systems in energy, transportation, water conservancy, finance and other key industries
- important information systems in power, water, gas supply, medical care, social security and other public service fields
- military networks

- government affairs networks of state organs at or above the level of cities divided into districts
- networks and systems owned or managed by network services providers with a large number of users.

At this stage, it is not clear which businesses (or which operational streams and functions) in the sectors mentioned above, or which of their specific networks, would be considered to be critical information infrastructure. It is clear, though, that the scope of industries and businesses covered will be broader than that covered in existing actual or draft regulations requiring data localization in the fields of e-banking, insurance, credit reporting, and network-based payment services.

The draft Cyber Security Law also gives no detail as to how broad the exemption for "truly necessary" international transfers will be or what the criteria for clearing the associated security assessment will be.

The typical aim of data localisation requirements is to support data security requirements and also to give regulators greater assurances of more immediate access to data relevant to the exercise of their authority. It remains to be seen, however, if the draft Cyber Security Law will be implemented with practical concessions to multinationals operating in China, or if this and other requirements will support suspicions that China is seeking to implement a more radical transformation of Chinese cyber space.

Conclusions
The draft Cyber Security Law stands as the latest in a series of new laws and draft laws that demonstrate a China increasingly focused on national security, stability, and the particular challenges that a digitally connected world pose for China's aims. Against a backdrop of geopolitical tensions over cyber security and Chinese concerns about the particular position that foreign technology companies hold in the global technology industry, there can be no doubt that there is a much bigger picture to this draft law.

In style, the draft Cyber Security Law continues a trend of broad legislation of expansive scope with a tendency to delegate critical points of detail to implementing rules and regulations to be issued by one or more separate regulators. This has been interpreted by some commentators to mean that there is room for engagement and negotiation, and some of the more challenging aspects of the draft law may be removed altogether. Of course, it will be the substance of the law – and its enforcement in practice – that count, and hence the output of the current consultation process will be closely watched as a barometer of China's openness to the global technology marketplace.

Mark Parsons
Partner, Hong Kong
T +852 2840 5033
mark.parsons@hoganlovells.com

Nolan Shaw
Junior Associate, Beijing
T +86 10 6582 9584
nolan.shaw@hoganlovells.com

E-commerce liberalization kicks off in China

China's regulatory framework for foreign investment in the e-commerce industry has undergone significant liberalization. Previous pilot programs on a local level have been extended nationwide, with directives from the highest political level to remove restrictions.

On 19 June 2015, the Ministry of Industry and Information Technology ("MIIT") issued a notice to lift foreign ownership restrictions in the e-commerce sector, subject to certain existing rules. A day later, the State Council issued guidance to encourage the development of cross-border e-commerce flows, a wider initiative to push China's e-commerce champions to expand overseas.

State Council orders liberalization steps

A few weeks before the recent developments on 19 and 20 June, the State Council actually laid out a general policy framework, allowing individual ministries and government agencies such as MIIT to formulate implementing rules for e-commerce liberalization.

On 4 May 2015, the State Council published a new policy document, the Opinions on Vigorous Development of E-Commerce to Accelerate the Cultivation of a New Driving Force in the Economy ("Opinions"), mandating government departments to develop policies to achieve a liberalized e-commerce market in China by the year 2020. The Opinions do not only address e-commerce operations, but also cover many aspects of the whole e-commerce business chain, from financial services to logistics, etc. As a broad high-level government policy statement, the Opinions signal the government's intention to promote e-commerce in order to reactivate a slowing economy.

The Opinions set forth a large number of directives to government agencies.

Re-ordering licensing procedures

The Opinions call on the State Administration for Industry and Commerce and the State Commission Office for Public Sector Reform to change the administrative policy of "first operational permit, then business license" to "first business license, then operational permit." The current practice to set up an e-commerce entity in China requires the applicant to first obtain an operating permit from the telecommunication authority – an internet content provider ("ICP") license, an online data processing and transaction processing services license, or both, depending on the local practice of the authority and the business scope of the company – as a pre-condition for obtaining a business license from the company registration authority. The Opinions now call for reform so that the business license is issued first, and then the operating permit. This change of order should in theory shorten the timeline for setting up an e-commerce company, allowing it to begin operations sooner.

Streamlining registration procedures

The Opinions call for a streamlining of registration procedures, the key ones being simplifying the capital registration process and lowering of the domicile/premises requirements for e-commerce businesses.

Access to capital/investment opportunities

The Opinions call on Chinese government agencies to streamline the approval process for the overseas listing of domestic e-commerce companies and encourage direct cross-border RMB investments in the e-commerce industry. Domestic listing of internet companies is also to be encouraged if certain conditions are fulfilled.

The highlight of the Opinions is the proposed removal of the foreign shareholding cap in e-commerce companies in China. The removal of the 50% foreign shareholding cap was first piloted in the Shanghai Free Trade Zone. The Opinions expand this liberalization nationwide, and can hopefully accelerate the implementation steps.

Preferences, incentives and venture capital funding

The Opinions stipulate that e-commerce businesses recognized as high-tech enterprises should enjoy related preferential policies. For example, qualified small and micro-businesses should enjoy preferential tax policies. According the Opinions, the National Development and Reform Commission is in charge of guiding venture capital funding and increasing support to newly established e-commerce companies.

Expanding the use of e-commerce

The Opinions call for the introduction and/or increased use of e-commerce in various sectors including energy, railway, and public utilities; the public service sector, for example, through the development of e-commerce platforms targeting residential communities by providing daily consumables, remote payment and health care services; traditional trading and distributing enterprises, including selling of food, health food, drug,

cosmetic and medical device on the internet, tourism, agriculture, and forestry, etc.

Additionally, the Opinions mention that the government is to enhance cooperation among financial institutions, telecommunications operators, bank card clearing institutions, payment institutions, and e-commerce companies in order to achieve large-scale application of mobile finance in e-commerce.

Logistics

The Opinions call for completion of the basic infrastructure of logistics, including establishment of logistics distribution terminals and warehousing facilities, which are critical to the e-commerce storage and delivery chain.

Building global brands

Another directive in the Opinions is to enhance the level of opening-up toward the international market. In particular, government agencies are requested to actively initiate multilateral and bilateral negotiations and communications on e-commerce rules. The Opinions call for promotion of e-commerce "going out" policies for China, by supporting e-commerce companies in establishing their own channels for overseas marketing and distinctive brands.

Improvement of support systems

The Opinions intend to enhance the regulators framework and standards, improve the establishment of credibility systems, strengthen technological and educational support (such as by enhancing the R&D of core technologies including cloud computing and big data), and coordinate regional e-commerce development, with each region addressing e-commerce as part of its plan for economic and social development.

Removal of foreign ownership restrictions

Following the issuance of the Opinions, on 19 June 2015, MIIT issued the Notice on Opening up the Limitation on Foreign Ownership in Online Data Processing and Transaction Processing Services (Operating E-commerce) ("**Circular 196**"). Circular 196 allows 100% foreign ownership in e-commerce services under the more general "online data processing and transaction processing services" category ("**E-commerce Services**") under the telecommunication services catalogue issued by MIIT in 2003. As mentioned above, Circular 196 removed the restriction nationwide after a pilot program launched in the Shanghai Free Trade Zone implemented in January this year.

According to Circular 196, foreign shareholding in E-commerce Services has been lifted from 50% (as part of the value-added telecommunications services ("**VATS**") category) to 100%. This means that foreign investors will be allowed to establish wholly foreign-owned e-commerce entities nationwide. However, under existing rules, such entities will need to be in the form of a foreign-invested telecommunications enterprise. In addition, the major investor of the foreign-invested telecommunications enterprise is required to have sound experience in operating VATS in order to be able to establish the enterprise and obtain the VATS permit to operate E-commerce Services.

Circular 196 also requires that a foreign-invested telecommunications enterprise apply for the online data processing and transaction processing services permit ("**OTP Services Permit**" which is a type of VATS permit). The key question is if the OTP Services Permit is the only VATS permit required or if the ICP permit is still required, to provide E-commerce Services. Our inquiries with central and Shanghai MIIT officials indicate that they believe an ICP permit may still be required depending on whether the business is "for profit." In reality, different MIIT offices may make different interpretations of the term "for profit." Nonetheless, against the backdrop of e-commerce liberalization, hopefully, the ICP permit requirement would eventually be loosened or replaced for the provision of OTP Services.

Cross-border e-commerce encouraged

On 20 June 2015, the State Council issued the Opinions on Guiding Healthy and Smooth Development of Cross-border E-commerce ("**Cross-Border Guiding Opinions**") which – when read together with the Opinions – further emphasize the push by the Chinese authorities for development in the cross-border e-commerce industry. With the Cross-Border Guiding Opinions, the State Council intends to promote the development of cross-border e-commerce by way of:

- offering positive financial support to traditional enterprises to explore the international market by using e-commerce platform
- improving the existing customs, inspection and quarantine and tax policies

- encouraging the development of cross-border e-commerce payment by domestic banks and payment institutions, and promoting RMB settlement of cross-border e-commerce activities.

Promoting the development of cross-border e-commerce acts as an important element in China's "internet plus" strategy, which is meant to upgrade China's economy and give it a more international presence. In addition, the Cross-Border Guiding Opinions show the government's interest in promoting transnational RMB settlement, which is an important step for the internationalization of the Chinese currency.

Conclusions

In 2015, we are seeing a ground-breaking policy change in the e-commerce sector in China.

Starting with the e-commerce liberalization in the Shanghai Free Trade Zone in January 2015, followed by the issuance of the amendment to the Foreign Investment Industry Guidance Catalogue in April 2015, the Chinese government has clearly signaled its willingness to open up the e-commerce sector to foreign investment.

The latest set of policies and rules issued in May and June 2015 bode well for further development of the e-commerce sector in China – including foreign investment – even though the end result will depend on whether the various government departments will implement the high-level policy directions. The government departmental policies requested in the State Council's Opinions should come out by year's end, and hence more clarity will soon be forthcoming

The recent liberalization of foreign investment in China's e-commerce industry and drive for cross-border e-commerce development are significant initiatives for China's e-commerce industry as a whole. The Opinions and the Cross-Border Guiding Opinions show the government's desire to facilitate the "going out" of Chinese e-commerce businesses – clearly a message to China's large e-commerce players to develop overseas.

Kurt Tiam
Counsel, Beijing
T +86 10 6582 9555
kurt.tiam@hoganlovells.com

Chinese court provides guidance on lawful use of cookies

On 6 May 2015, the Intermediate People's Court in Nanjing issued a judgment ruling that the search engine giant Baidu's use of cookies to personalize advertisements directed at consumers on partner third-party websites does not infringe consumer rights of privacy. The court based its decision on findings that the information collected by the Baidu cookies did not amount to "personal information" under Chinese law, the complainant did not suffer cognizable injury by receiving targeted ads on other sites, and Baidu afforded consumers mechanisms to opt out.

Although not binding on other courts, this judgment has significant implications. It provides insight into how other courts in China are likely to handle similar challenges to the use of cookies in the future. Its detailed analysis of Baidu's cookie policy sheds light on what policies and practices companies in China would be prudent to adopt in order to best balance industry and consumer interests in compliance with the law.

Regulation of cookies under Chinese law

Chinese law does not specifically regulate cookies. Instead, cookies are generally subject to laws and regulations on the internet, consumer privacy and data protection. Among these laws and regulations are:

- the 2010 Tort Liability Law
- the related 2014 Supreme People's Court's Provisions on Certain Issues Concerning the Application of Law in the Hearing of Cases of Civil Disputes over the Use of Information Networks to Infringe upon Personal Rights and Interests ("**SPC Provisions**")
- the 2013 Provisions by the Ministry of Industry and Information Technology on the Protection of Personal Information of Telecommunications and internet users ("**MIIT Provisions**")
- the 2015 Measures by the State Administration for Industry and Commerce on Penalties for Infringements of Consumer Rights and Interests

There is also a non-binding standard which gives helpful guidance for the industry, the China Standardization Administration's Information Security Technology Guidelines for Personal Information Protection within Public and Commercial Service Information Systems ("**Guidelines**") from 2013.

The issues

In this case, internet user Ms. Zhu Ye claimed that Baidu violated her privacy rights under the Tort Liability Law leading to damages in the form of emotional distress. Ms. Zhu had used Baidu's search engine to type in distinctive search terms such as "weight loss," "abortion" and "breast implants." Then, when visiting third-party websites, such as www.4816.com, www.paolove.com and www.500kan.com, she found that the advertisements displayed on these websites related to the search term she had input into Baidu's search engine before. These advertisements had a handprint-looking marking on the bottom left corner, which if clicked on, lead to the website http://wangmeng.baidu.com, Baidu's website for its cooperative advertising business. This allegedly caused Ms. Zhu to feel significant distress that Baidu engaged in commercial activity using her personal habits and preferences, in violation of her rights to privacy.

At first instance, the Gulou District People's Court in Nanjing had ruled in favor of the plaintiff. On appeal, the Nanjing Intermediate People's Court reversed, disagreeing with Ms. Zhu's privacy claim based on three key considerations.

No "personal information" collected by cookies

The first reason for the appellate court to reject Ms. Zhu's claim was that the information collected by the Baidu cookies did not amount to "personal information" as defined under the MIIT Provisions.

The court agreed that a record of a user's internet activity and internet preferences are matters of privacy, but also found that such items did not amount to "personal information" in the context of cookies because the information is separate from, and unable to lead to discovery of, the identity of the user. Baidu's cookies were not linked to the identity of a person, but only to the specific internet browser. Baidu did not know the identity of the user using the browser, nor did it know whether there were one or several people using the browser or what Ms. Zhu's preferences would be if she used a different browser.

No cognizable damage or public disclosure

The court's second argument for dismissal of the suit was that Baidu's online targeted advertising service did not result in cognizable damages to the user or involve public disclosure.

The SPC Provisions, which set down the parameters for courts to take on internet public disclosure cases, provides that courts are to uphold a finding for liability in tort for cases in which: (1) a network user or network service provider, (2) causes harm to an individual (3) by using the internet to make public the individual's genetic information, medical records, health examination data, criminal records, home address, personal activities or other private and personal information. The court found that Ms. Zhu's claims failed on the second element (damages) and the third element (public disclosure).

Concerning damages, the court held that Ms. Zhu's claims of emotional distress were subjective and not supported by specific evidence, and that the objective result of Baidu's personalized advertisements service, far from being harmful, actually provided a benefit to Ms. Zhu as the advertisements she saw on third-party websites were targeted towards her preferences, rather than being random and irrelevant.

Concerning public disclosure, the court found that no public disclosure had occurred. The only place where Ms. Zhu's internet preferences were disclosed was to Ms. Zhu's own internet browser, and not to the public.

No restriction to right of choice

The last reason the appellate court relied on to decide against the plaintiff was that Baidu had not denied her right to know and right to choose as a consumer regarding how Baidu collects and uses her search preference information.

The court found that Baidu had fulfilled its duty to Ms. Zhu as a consumer and user of its website by merit of its published and well-developed privacy policy. Baidu's privacy policy, which was accessible through a link at the bottom of its homepage entitled "*Must read before using Baidu,*" explained what cookies are, informed that Baidu uses cookies to personalize advertisements on partner websites, and provided two ways to opt out of cookies.

Although Baidu did not collect explicit consent for its use of cookies, the court found Baidu's policy functioned as a notice and opt-out mechanism consistent with the rules of the non-binding Guidelines, which state that when collecting "general personal information," consent may be obtained in an implicit way, as long as collection and use stops if a user objects.

In Baidu's case, there were not one, but two, opt-out mechanisms available to users. The first was Baidu's explanation of how to turn off cookies through adjusting the user's browser settings. The second was a button provided by Baidu on its own website that allows users to turn off the cookie function.

Conclusions

As noted, China has no specific rules on cookies, which can leave companies uncertain about whether the cookie policies they have formulated under general Chinese privacy rules and practice are sufficient to withstand claims in court. Indeed, Baidu itself could not be certain of the outcome of this particular case, and actually lost the case in the court of first instance.

The appellate judgment overruled the court of first instance and, in a detailed opinion, shed much needed light on the issue. Even though not directly binding on other courts as a precedent, given that China is not a common law jurisdiction, the Nanjing court's opinion is the final judgment for this case and its analysis reveals important takeaways to consider in addition to the main findings discussed above:

- Using cookies, at least in a targeted advertising context, can be compliant with Chinese privacy law. The legality of other uses of cookies, however, still remains unclear, and the court judgment did not address other uses outside the specific facts of Baidu's case. Baidu's case involved limited delivery of information as between Baidu's servers and the user's browser. Importantly, in that use, no personal information was displayed, provided or sold to external parties. If the opposite were true, then the use of cookies might be analyzed differently under Chinese law.
- Privacy policies are critical. They should be thorough in their explanation of cookie use and where applicable, explain how to opt out, or even better, directly provide a mechanism to users for opting out.
- A webpage privacy policy should be prominent and easy to find. In this case, the appellate court found it acceptable that Baidu's privacy policy was presented in a link at the bottom of the page. An argument was made challenging this presentation because the link was in a smaller font, was displayed in an inconspicuous color, and was sandwiched between other information. Although the court acknowledged

these points, it still found the link to be conspicuous enough given the simplicity of Baidu's webpage overall. This suggests a holistic approach to the notice analysis. A more conspicuous link may be advisable for more complicated webpages.

- The court cited the Guidelines. The Guidelines are non-binding, so their usefulness is sometimes questioned. Nevertheless, they are the most detailed statement of standards for privacy matters in China, and are often as benchmark to develop a company's best practices. In this case, the court explicitly found the Guidelines to be an important reference point for devising principles for what is acceptable, acknowledged the Guidelines' separate classification and consent requirements for sensitive personal information as opposed to general personal information, and recognized the Guidelines' purpose of striking a balance between preserving personal dignity and promoting technical innovation.

To conclude, while the judgment cannot directly be relied on as a precedent, it does provide some welcome guidance for technology companies across China.

Sherry Gong
Counsel, Beijing
T +86 10 6582 9516
sherry.gong@hoganlovells.com

Nolan Shaw
Junior Associate, Beijing
T +86 10 6582 9584
nolan.shaw@hoganlovells.com

A right to be forgotten in Hong Kong?

A recent appeal against an enforcement notice issued by the Privacy Commissioner for Personal Data of Hong Kong raised an interesting and highly controversial issue as to whether, and to what extent, individuals in Hong Kong have a "right to be forgotten" entitling them to deletion of personal data in the public domain.

This label of "right to be forgotten" gained significant publicity following a landmark ruling of the European Court of Justice ("**ECJ**") in May 2014 where the court held that under certain circumstances search engines are obliged to remove results if they link to webpages that contain information infringing the privacy of European Union ("**EU**") citizens. The rationale behind this right is to avoid indefinite stigmatisation or censure due to information available about a specific action performed in the past, or at least to avoid search engines producing results that aggravate the resulting harm to affected individuals.

David Webb's case in Hong Kong – a right to remove personal data available in the public domain?
David Webb is a former investment banker turned activist who runs a website at Webb-site.com offering investors information on corporate and economic governance in Hong Kong. The website contains a database which compiles information about the various roles certain individuals play in the financial and public sectors in Hong Kong, for example, directorships in listed companies or membership in governmental advisory bodies. The database also includes reports and links to public documents about that person, such as press articles and court judgments.

The personal data in question in this case are the full names of the parties set out in the court judgments of a matrimonial case heard in open court in Hong Kong. The judgments were published on the Hong Kong Judiciary's website during 2000 to 2002. Some ten years later, in 2010 and 2012, the Judiciary redacted the names in the files on its website and, acting on one of the data subject's complaint, the Privacy Commissioner ordered Webb to follow suit and remove the names from his reports on Webb-site.com.

Mr. Webb refused to follow suit, and in August, 2014 the Privacy Commissioner issued an enforcement notice under the Personal Data Privacy Ordinance ("**PDPO**") against Mr. Webb ordering him to remove the names of the data subjects in question. The ground on which the Privacy Commissioner issued his enforcement notice was apparently Data Protection Principle 3 ("**DPP3**") of the PDPO, which requires that processors of personal data only use personal data for the purposes for which it has been collected, or any directly related purpose. The Privacy Commissioner's position was that Mr. Webb, by maintaining the reports and hyperlinks in the Webb-site.com archives, breached DPP3 by using personal data for a purpose other than

the purpose for which it was to be used at the time of collection of the data. Under the PDPO, failure to comply with an enforcement notice constitutes an offence.

While taking down the reports in the interim, Mr. Webb filed an appeal against the enforcement notice, arguing that the personal data was collected at a time when it was publicly available, and so should continue to be accessible. Mr. Webb commented that the enforcement notice, if upheld, "would have a chilling effect on publishing within Hong Kong," with newspapers and websites potentially being ordered to take down articles about convictions, bankruptcies or divorces, information about which is already public.

Mr. Webb's appeal was heard by the Administrative Appeals Board ("**AAB**") in a public hearing on 13 July 2015. The AAB's decision is yet to be published.

Hong Kong law – is there a right to be forgotten?

The treatment of personal data in the public domain is a controversial subject, and has been the subject of enforcement under the PDPO in the past. The Privacy Commissioner issued an enforcement notice in July 2013 to the operator of a smartphone application known as "Do No Evil," which enabled searches for target individuals' litigation, bankruptcy and company directorship data obtained from public databases. Users reputedly made use of the smartphone application for due diligence and background check purposes. The Privacy Commissioner determined that the use of personal data obtained from the public domain for due diligence review and background checks was inconsistent with the original purpose of data collection by the Judiciary, the Official Receiver's Office and the Companies Registry, whether such purposes were expressly stated by the relevant registrar or were as determined by the Privacy Commissioner following his review of the functions of these registries. Use of data in such a way "obviously exceeded the reasonable expectation of the data subjects on public disclosure of their litigation and bankruptcy data." The Privacy Commissioner stated that "[t]his case highlights a common misunderstanding that personal data collected from the public domain, not from the data subjects direct, is open to unrestricted use."

As the law stands now then, there clearly is some basis in Hong Kong law, or at least in the Privacy Commissioner's enforcement policies, for a "right to be forgotten."

The position in Europe: a judicially sanctioned right to be forgotten

In the landmark May 2014 ruling, the ECJ held that under certain circumstances search engines may be required to remove search results if they link to webpages that contain information infringing the privacy of EU citizens.

The ECJ case concerned a Spanish national who requested a search engine to remove certain search links to newspaper announcements of 1998 regarding

the forced sale of properties arising from social security debts that contained his name.

The ECJ found that, in this particular situation, the processing of the personal data by the search engine was no longer relevant because the original publication was 16 years old and it could not be justified in the public interest or otherwise. An important point made by the ECJ was that, whilst the legal basis for a 'right to be forgotten' exists under the EU Data Protection Directive ("**Directive**"), its exercise needs to be considered on a case by case basis, by considering whether the public interest in accessing the information overrides the individual's right to privacy. In practical terms, an individual could argue that the processing of their data by a data controller is inadequate, irrelevant or excessive, such data is not kept up to date; or the data is being kept for longer than necessary.

It should be remembered that this "right to be forgotten" is a narrow one. The ECJ ruling concerns the de-listing of internet search results only. The original information continues to exist at the source and can be accessed online directly or by search using search terms other than the individual's name.

Beyond the Webb case: what next in Hong Kong?
It will be interesting to see how the AAB decides on the Webb case, which involves a fundamental conflict between the right to privacy, freedom of expression and the right to use personal data in the public domain.

It is clear that ECJ rulings do not bind Hong Kong courts or the AAB and, in any event, the basis of the Privacy Commissioner's enforcement notice differs significantly from basis for the European enforcement action. Commenting on the ECJ litigation on his blog, the Privacy Commissioner noted that "prima facie, the approach [the ECJ] has taken is not applicable under the Ordinance [PDPO]." In particular, the Privacy Commissioner expressed the view that a search engine would not be considered a "data user" in Hong Kong; in contrast, the ECJ considered the search engine operator a "data controller" (the EU equivalent of a "data user") subject to the Directive.

Furthermore, the ECJ case turned on a finding that the linking to prejudicial data in relation to the individual in questions was "excessive" use of that data rather than the use of personal data for a new, unrelated purpose than for which it was collected (the basis for the Hong Kong enforcement action against Mr. Webb). The ECJ held that the search engine had breached the principle that the personal data collected or processed "must be adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further processed." The gist of the ECJ ruling is that the processing of accurate personal data for the purposes for which it was lawfully collected may, in the course of time, become incompatible with the Directive. The Hong Kong enforcement action against Mr. Webb takes a different line of argument that the purpose of placing personal data into the public domain may over time be discharged, at least when the primary publisher of the personal data, in this case the judiciary, ceases to make the information public.

The issues under deliberation in Mr. Webb's case are perhaps narrower than those at issue in the "Do No Evil" case, where the personal data in question was ordered removed even though the data continued to be published by its primary sources. The forthcoming decision in Mr. Webb's appeal will necessarily, however, explore in much the same way the clashing of policy interests that arise when the interest in having a free flow of news and information poses challenges for privacy interests. Hong Kong's understanding of rights of privacy has expanded considerably in recent years. These issues are increasingly relevant in Hong Kong as elsewhere, and the decision in Mr. Webb's case will be an important one to watch.

Eugene Low
Partner, Hong Kong
T +852 2840 5907
eugene.low@hoganlovells.com

Dominic Edmondson
Registered Foreign Lawyer, Hong Kong
T +852 2840 5026
dominic.edmondson@hoganlovells.com

Supreme People's Court clarifies certain patent dispute rules

On 29 January 2015, the Supreme People's Court ("**SPC**") issued a new judicial interpretation on patent disputes, the Decision on Revising Provisions on Issues Concerning the Application of Law in Patent Disputes, ("**Judicial Interpretation**"). In this new Judicial Interpretation, the SPC seeks to bring its prior rules further in line with the Patent Law, and tweak some patent litigation rules. The Judicial Interpretation came into effect on 1 February 2015.

The Judicial Interpretation brings about some welcome changes, since the prior rules contained a range of provisions that were incompatible with the Patent Law after its major overhaul of 2008.

Submission of evaluation reports

Under the old rules, the submission of a "search report" (as it then was called) was a prerequisite to case acceptance in utility model and design patent cases. That prerequisite has now been abolished. The new Judicial Interpretation stipulates that a plaintiff *may* submit such a report, and that the court *may* request the submission of that report if it deems it useful. Still, the importance of the change is questionable. Even under the new Judicial Interpretation, a refusal to submit the report upon request can either lead to a stay or to a complete rejection of the case.

In addition, the report plays a vital role in cases where the defendant files a counterclaim for invalidity of the utility model or design patent. In such cases, the court may decide not to stay the case, but instead proceed with the infringement question if the evaluation report does not show any serious ground for invalidation of the asserted patent.

Doctrine of equivalents

For reasons of consistency, the revised Judicial Interpretation clarifies the Chinese doctrine of equivalents by stipulating that *all technical elements* rather than just the *essential technical elements* – as provided by the prior rules – should demarcate the protection scope of a claim. This is not a radical change in the interpretation of the doctrine of equivalents, since another SPC judicial interpretation dating back to 2009 already changed this.

Moreover, in the new Judicial Interpretation, the SPC clarifies for the first time from which point of view a disputed technical element should be assessed when applying the doctrine of equivalents. According to the Judicial Interpretation, this should be the standpoint of "the ordinary technical personnel in the relevant field *at the time when the contentious infringing activities occur.*" This last element – the time of assessment – is a new element in the test. While it may lead to greater clarity of the doctrine of equivalents, it may, at the same time, lead to a higher burden of proof on the plaintiff.

Wider jurisdiction over design patent cases

The new Judicial Interpretation confers jurisdiction over design patent cases to the courts of the place where the accused products are *offered for sale*. This means that it will now be easier for plaintiffs to determine and choose the best forum to bring their claims. This may in turn help them to avoid local protectionism or select courts with more experience in IP litigation (e.g., the newly-established IPR Courts in China).

Rules regarding damages updated

As to damages, the SPC mainly brought the Judicial Interpretation in line with the provisions of the Patent Law. As a consequence, the Judicial Interpretation now prohibits plaintiffs from freely selecting the method that awards them the highest amount of damages. Instead, they will have to follow the Patent Law's cascade system based on proof.

Moreover, the Judicial Interpretation now officially confirms the existing practice that reasonable expenses incurred by the plaintiff for stopping infringement may be separately calculated and may go above and beyond the amount of the statutory damages provided by the Patent Law.

To conclude, while the Judicial Interpretation does not bring about ground-breaking changes in Chinese patent law, it does clarify a few important points in practice.

Skip Fisher
Partner, Shanghai
T +86 21 6122 3850
william.fisher@hoganlovells.com

Rocky Wu
Associate, Shanghai
T +86 21 6122 3876
rocky.wu@hoganlovells.com

MIIT think-tank issues white papers on mobile internet industry

On 21 April 2015, the China Centre for Information Industry Development ("CCID") – a think-tank affiliated with the Ministry of Industry and Information Technology ("MIIT") – published two white papers, on mobile internet and on smart mobile devices respectively. The two white papers describe recent key developments in "mobile internet" – understood as access to the internet from a mobile device via the 3G/4G network – worldwide and in China, and put forward suggestions on how to devise an adequate policy framework to address the challenges and opportunities in this era of digital transformation.

When describing recent developments, the two white papers highlight the impressive growth of the Chinese mobile internet industry to around RMB 213.5 billion (approximately USD 33 billion) in 2014, representing a 115.5% increase compared to the previous year. The white papers identify the popularity of mobile smart devices and the development of internet services – such as e-commerce, internet finance and online education – as key drivers of growth.

After a comprehensive analysis of the most important developments and associated challenges, the white papers set out a few policy recommendations to promote the mobile internet in China. Some of these recommendations have already been incorporated into government policies.

Need for a coordinated overall mobile internet plan

The white papers suggest that coordination between the various competent government agencies is needed to prepare development plans and policies for the mobile internet.

In part, the contours of a coordinated overall plan for the mobile internet is already taking shape. In particular, the "internet plus" initiative – first mentioned by Premier Li Keqiang in March this year – is quickly becoming an important part of the Chinese government's overall policy layout for the internet sector. For instance, on 1 July 2015, the State Council unveiled a guideline for the "internet plus" initiative, aiming to integrate the internet with traditional industries and create a new engine for economic growth. The relevant ministries are now in the process of enacting their own "internet plus" plans to implement the State Council's guideline.

A cooperative eco-system

The white papers also recommend that the mobile internet ecosystem be further opened up in order to facilitate cooperation across companies of different areas, such as telecommunications operators, software and hardware companies, and mobile internet service providers.

The white papers propose that the government adopt a range of measures to boost the efficiency of the mobile internet industry, such as the formulation of internet service standards or rules to promote interoperability and data security. Notably, the white paper on smart mobile devices recommends introducing government policies to promote the vertical integration among mobile device companies to create integrated "chip-system-device-application" players and/or markets.

New business models

The white papers express a general concern about the seemingly low profitability of internet services (due to the low-price or "free" products typical in the internet industry) and the perceived "disconnect" with the high market capitalization/valuation of internet companies. Consequently, the white paper on mobile internet encourages the government to support mobile internet companies to devise new, more profitable business models.

Cross-industry regulatory regimes

The rise of the mobile internet industry has been radically transforming traditional ways of doing business and upsetting the competitive dynamics in the marketplace. Yet the white papers find that regulators' responses lag the economic integration of different industries driven by the mobile internet. Hence, the white papers call upon the government to identify regulatory responsibilities and formulate flexible and sustainable rules to regulate the new areas related to mobile internet and support innovation.

One area where the government is setting up a new cross-industry regulatory regime is internet financing. On 18 July 2015, the People's Bank of China – together with other nine other ministries and commissions – released the Guiding Opinion to Promote the Healthy Development of Internet Finance, which divides regulatory responsibilities among the regulators and lays out the basic legal framework for this emerging industry. A few days after the issuance of this guiding opinion, on 27 July, the China Insurance Regulatory

Commission issued the first batch of rules to regulate internet finance – the Interim Measures for Regulating the Internet Insurance Business.

Key technologies and intellectual property strategies
According to the white papers, Chinese regulators should support R&D efforts in a number of key technology areas, such as multi-mode baseband and radio frequency chips, high performance multi-core application processors, BeiDou/GPS/GLONASS multi-mode satellite navigation receiver chips, MEMS (micro-electro-mechanical systems), LTPS (low temperature poly-silicon) and AMOLED (active-matrix organic light-emitting diode) displays.

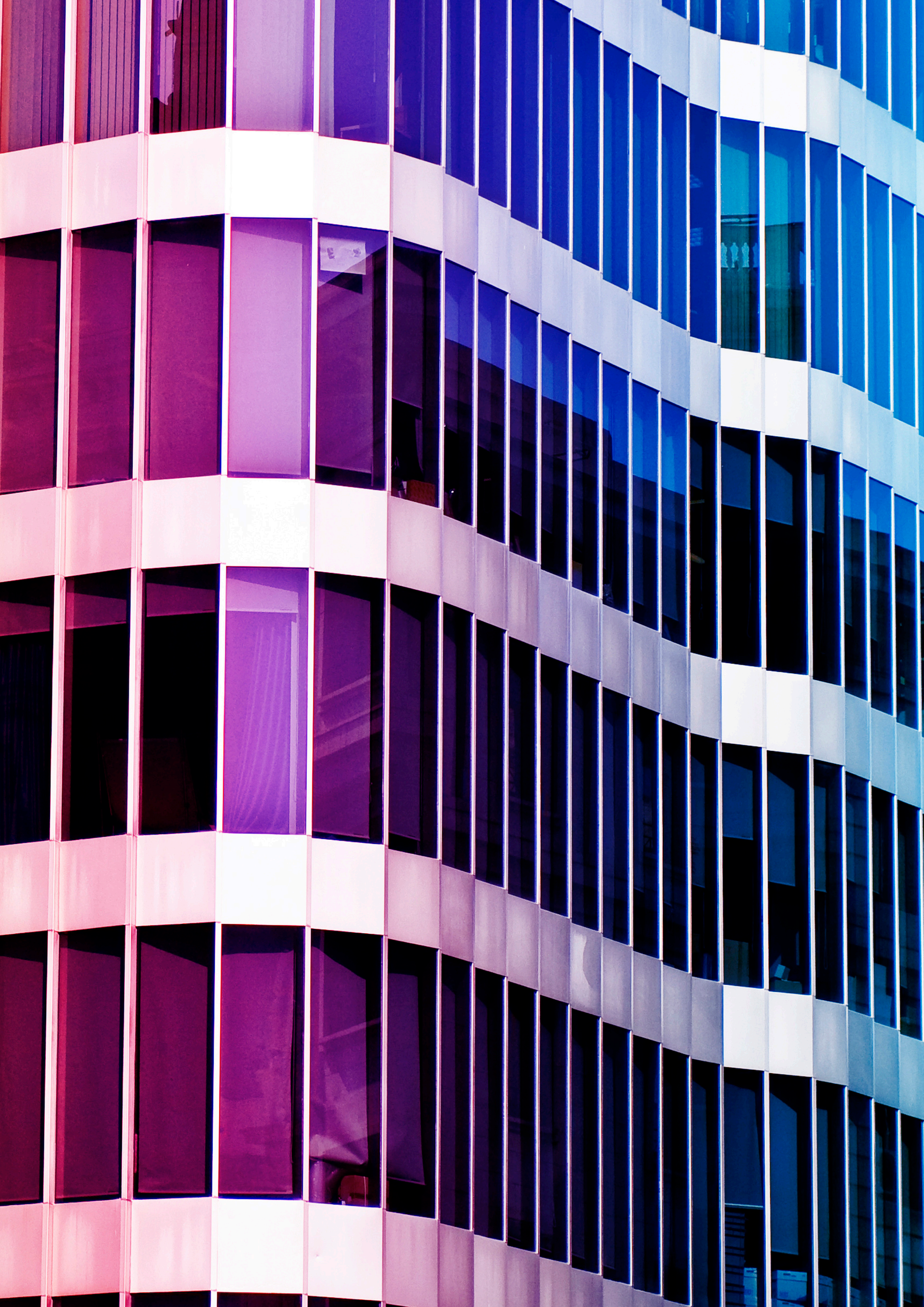
Further, in order to defend Chinese interests in the global patent wars in the smart phone area, the white papers recommend that the government promote patent pools and alliances among Chinese companies. The white papers also encourage Chinese companies to combine key technology resources and build up patent defence systems to fight off patent litigation. This recommendation is in line with what is happening in the marketplace. For example, on 28 April 2015, the State Intellectual Property Office issued the Guideline to Establish Industrial Intellectual Property Alliances to encourage the sharing and management of intellectual property rights.

Data security and promotion of domestic IT systems
The white papers further emphasize that the development of the mobile internet and mobile smart devices should not compromise data security. They stress the importance of having regulators issue rules to regulate the collection of personal information, to define responsibilities of internet operators, information service providers and device manufacturers, and to enhance the regulation of information networks.

The white paper on smart mobile devices also mentions the need to expand the use of domestic software and hardware in key industries and products. These comments are in sync with some of the directions of the draft Cyber Security Law and other initiatives, such as the attempt by the China Banking Regulatory Commission to reduce Chinese banks' reliance on foreign IT systems, which threatened to replace key IT products provided by foreign companies with home-grown products.

Conclusions
With the rise of the mobile internet, China is experiencing an impressive digital transformation, which is expected to make a lasting impact on its economy. Realizing the full potential of this transformation in part depends on the Chinese government's ability to create an adequate policy framework. As an affiliate of China's key internet regulator – MIIT – CCID's policy recommendations carry weight, and can give foreign and domestic market players additional background of some current policies and – perhaps – a glimpse of other policy initiatives still lying ahead.

Qing Lyu
Junior Associate, Beijing
T +486 10 6582 9401
qing.lyu@hoganlovells.com



China opens up domestic bank card clearing market to foreign competition

On 9 April 2015, the State Council issued the Decision on the Implementation of Market Access Administration in relation to Bank Card Clearing Institutions ("**Decision**"). The Decision became effective from 1 June 2015. Critically, the Decision is expected to end the current de facto monopoly on bank card clearing services in China and to pave the way for the opening up of this market segment to other entrants, including foreign investors.

Bank card clearing business in China

Currently, the processing and clearance of all RMB-denominated payments made via bank cards and credit cards in China is performed by China UnionPay ("**CUP**"). CUP is a bank card association in China established in 2002 with the consent of the State Council and the approval of the Chinese central bank, the People's Bank of China ("**PBOC**"). It is controlled by a consortium of mainly state-controlled banks. Given the requirement for all card issuers to process their RMB transactions through the CUP network, CUP has grown in parallel with the Chinese economy and the explosion in Chinese tourism outside its own borders in recent years to become the largest card issuer in the world, having issued more than 4.9 billion bank cards, which can be used in over 150 countries and regions.

Meanwhile, foreign companies such as American Express, MasterCard and VISA have been shut out of this segment of the Chinese market. They have hitherto only been able to process transactions by Chinese citizens while overseas, and have had to pay a network access fee when accepting RMB payments.

WTO intervention

This market shut-out caused the United States to file a complaint with the World Trade Organization ("**WTO**") that China was in violation of WTO rules requiring equal treatment for foreign credit-card and debit-card issuers in WTO member domestic electronic payments markets. The WTO ruling upheld the complaint and required China to open its bank card clearing market by August 2015.

China issued the Decision ahead of that deadline, although the Decision makes no mention of the WTO ruling. The Decision is important because it marks a significant step toward the end of the CUP de facto monopoly.

Market access criteria

Under the Decision, various market access criteria have been prescribed in terms of registered capital, the main investors in the bank card clearing institution, clearing systems, infrastructure, management personnel and internal risk controls.

Specifically, when applying to become a bank card clearing institution in China, the applicant must have:

- registered capital of not less than RMB 1 billion
- one or more "main capital contributors" (if only one, it must hold more than 20% of the shares; if more than one, together they must hold more than 25% of shares in aggregate, and additional rules apply)
- a standard bank card clearing system which is in line with Chinese national and industry standards
- infrastructure and a remote disaster recovery system within China, which meets specified requirements and is capable of independently completing bank card clearing business actions
- directors and senior management personnel with qualifications approved by the PBOC after having obtained the consent of the China Banking Regulatory Commission ("**CBRC**").

In addition, the applicant must satisfy other unspecified requirements, such as internal controls, risk prevention, information security and anti-money laundering. The concern with this "catch-all" clause is that given the open-ended nature of the (as yet unspecified) requirements, these might include gating items that would delay or, even worse, prevent market access by foreign or domestic applicants.

Approval procedures

The Decision divides the entire approval process into two phases, each with a concrete timeframe within which regulators must review and approve or reject the application. This division into phases is not new: it is the standard establishment procedure in relation to the formation of many CBRC-regulated financial industry entities like banks.

The first phase involves approval to begin the preparatory phase. The PBOC is the approval body, but it has to consult with and obtain the consent of the CBRC. This formulation is repeated throughout the Decision. The PBOC has 90 days' from acceptance of

the application to decide whether or not to approve the application. If approved, the applicant can start the preparatory phase. The Decision requires the preparatory work to be completed within one year from approval. During the preparatory phase, the applicant is not permitted to engage in bank card clearing activities.

The second phase involves approval to commence business operations. The application for approval can only be submitted after the preparatory phase has been completed. Similar to the first phase described above, the PBOC is the approval authority, but has to consult with and obtain consent from the CBRC. Again, the PBOC has 90 days from acceptance of the application to decide whether or not to grant approval. If the application is finally approved, the PBOC will issue a "bank card clearing business permit" to the applicant. Then, the approved applicant has six months to officially commence its bank card clearing business operations.

Conduct of business requirements
The Decision also sets out conduct of business requirements for approved bank card clearing institutions. For example, a bank card clearing institution must use its own, or its capital contributor's, bank card clearing brand when engaging in bank card clearing business activities. In addition, transactions between bank card clearing institutions and domestic card issuers or card acquirers must be handled through the domestic bank card clearing infrastructure, and fund settlement must be completed within China. This may prove problematic for some international card structures that have existing overseas processing hubs and infrastructure.

The Decision imposes certain restrictions on transfer of both business-related data and personal financial information. The imposed requirements are onerous, but are in line with recent developments in data protection law in China.

Regulations of foreign bank card clearing institutions
The Decision provides a dual regime for foreign bank card clearing institutions, depending on whether they operate domestic or cross-border clearing services.

Foreign companies that provide bank card clearing service to parties within China must establish a foreign-invested entity within China and obtain a bank card clearing business permit. In contrast, those that only provide bank card clearing services for cross-border transactions in foreign currency are not required to establish a bank card institution in China in principle, but instead must report their business developments/ circumstances to the PBOC and the CBRC. This last obligation is a concern in the sense that it seems to bring foreign bank card clearing institutions, which are only involved in clearing foreign currency cross-border transactions, within China's regulatory ambit.

Conclusions
This hard-won opening of the domestic bank card clearing market is clearly one of the most significant developments in the financial services sector in China in recent years. It would appear to be almost inevitable that the major global players will seek to establish themselves as competitors to CUP in the coming months or years.

Yet, it will be a steep hill to climb to get even close to the incumbent CUP, which has built a strong brand with overseas reach. As with all real or apparent regulatory breakthroughs in China, the proof of the pudding will be in the eating. In this case, the content of the rules to be issued in implementation of the Decision will be key to determining the success of the bank card clearing liberalization in China.

Roy Zou
Partner, Beijing
T +86 10 6582 9596
roy.zou@hoganlovells.com

Merger control in Hong Kong's telecom industry – emperor's new cloths?

In Hong Kong, holders of telecommunications carrier licenses have been subject to competition rules under the Telecommunications Ordinance since the 2000's. The competition rules include a merger control regime. Indeed, over the years, the Communications Authority – the regulator of the telecommunications and broadcasting sectors – has provided antitrust oversight over a number of significant mergers in Hong Kong's telecommunications sector.

The Hong Kong Competition Ordinance – enacted in 2012 and scheduled to fully enter into force on 14 December 2015 – is Hong Kong's first cross-sector competition law. However, the scope of the Competition Ordinance's merger control regime currently does not extend beyond the telecommunications sector, in line with the current regime. The Communications Authority will continue to have jurisdiction for antitrust enforcement over the telecommunications and broadcasting sectors, but will share that jurisdiction with the Competition Commission, the authority tasked with cross-sector enforcement of the Competition Ordinance.

On 27 July 2015, the two authorities jointly published the Guideline on the Merger Rule ("**Merger Guideline**"). The Merger Guideline sets out the authorities' policy, approach and procedure for the enforcement of the Merger Rule, and bears similarities with the prior guidelines published by the Telecommunications Authorities relating to mergers under the Telecommunications Ordinance.

Scope of the Merger Rule

The definition of a "merger" is broadly defined in the Competition Ordinance and the Merger Guideline. The definition of a merger covers not only the actual amalgamation of legal entities, but also de facto amalgamations where a permanent, single economic management between previously independent undertakings is established. In addition, taking direct or indirect "control" of the whole or part of another undertaking by any means, creating a joint venture on a lasting basis as an autonomous economic entity or the "take-over" of an undertaking through acquisition of all or part of its assets may fall within the definition of a merger for the purposes of the Merger Rule. Basically following European Union law, the Merger Guideline defines "control" as "decisive influence" to determine strategic commercial decisions of the undertaking such as the budget, the business plan, major investments or the appointment of senior management.

Under the current rules, the merger control regime only comes into operation if the merger crosses certain statutory thresholds for changes in voting rights (for example, if a person acquires 50% or more of the voting rights in a telecommunications carrier licensee). Therefore, the scope of the Merger Rule is potentially wider than the current telecommunications merger control regime.

Safe harbours

The Merger Guideline specifies two indicative safe harbours that act as screening mechanisms for mergers which are unlikely to substantially lessen competition. Where a merger falls below the relevant safe harbour thresholds, they will be considered unlikely to raise competition concerns.

The first such safe harbour concerns the level of market share and market concentration. The safe harbour kicks in where the market share of the merged entity is less than 40% and the combined market share of the four (or potentially fewer) largest firms in the relevant market subsequent to the merger (four-firm concentration ratio or "CR4") is less than 75%. In contrast, where a merger results in a combined market share of 40% or more, the authorities are likely to argue that the merger raises competition concerns.

The second safe harbour relates to the Herfindahl-Hirschman Index ("**HHI**"), which is also a measure of market concentration. The safe harbour applies where the relevant market shows post-merger (1) an HHI of less than 1,000; (2) an HHI between 1,000 and 1,800 and an HHI increase of less than 100; or (3) an HHI of 1,800 or above and an HHI increase of less than 50.

As noted, these safe harbours are merely indicative. Falling below the relevant thresholds does not preclude the authorities from taking action where they nonetheless consider the merger to raise competition concerns. Indeed, in the *HKT/CSL* case – examined under the Telecommunications Ordinance – the Communications Authority took the view that the merger would raise competition issues, even though the parties' combined post-merger market share was below the 40% threshold set out in the prior telecommunications merger guidelines.

Competition analysis

In terms of the benchmark for the substantive analysis, the Competition Ordinance follows a "substantially lessening competition" test. The Merger Guideline proposes a "with-and-without" test by comparing the likely post-merger level of competition against the likely level of competition without the merger (i.e., counterfactual).

Also important are, of course, the market shares and market concentration levels in the relevant market. Market shares are usually determined with reference to sales volumes or turnover and, in the telecommunications context, numbers of subscribers, call minutes and data volume, etc. This guidance in the Merger Guideline is, again, similar to the approach taken by the Communications Authority in the *HKT/CSL* case. High market share and market concentration levels may lead the authorities to raise competition concerns.

The Competition Ordinance also puts forward other factors to be considered such as the failing firm defense.

Exclusions and exemptions

The Competition Ordinance provides for a number of statutory exclusions and exemptions from the application of the ordinance, including the Merger Rule. Importantly, the Competition Ordinance provides for the exclusion of the Merger Rule for transactions which generate economic efficiencies that outweigh the transactions' adverse effects caused by the lessening of competition. Merging parties wishing to claim the benefit of this exclusion will bear the burden of clearly proving the efficiency gains resulting from the merger. This is potentially narrower than the "benefit to the public" justification in the current telecommunications merger regime.

This exclusion aside, the Competition Ordinance also provides for a number of exclusions and exemptions that may be granted by the Chief Executive in Council on public policy grounds. However, such exclusions and exemptions will ultimately still be subject to the scrutiny by the Legislative Council, Hong Kong's legislature, before taking effect.

Notification procedures

As in the current regime under the Telecommunications Ordinance, there is no mandatory requirement to notify a merger to the Competition Commission or the Communications Authority under the Competition Ordinance. However, the merging parties are encouraged to make a voluntary notification.

The parties can consult with the authorities informally on a confidential basis, and the authorities may then provide a preliminary, non-binding view on whether the merger is likely to raise competition concerns.

Merging parties may also request the authorities to take a formal decision as to whether one of the statutory exclusions or exemptions discussed above applies. However, the authorities are only required to process this request if it raises novel or unresolved questions of wider importance or public interest and if there is no clarification in existing case law.

As under the existing telecommunications merger control regime, the authorities may accept commitments by the merging parties. In return, the authorities would agree not to commence an investigation or initiate proceedings before the Competition Tribunal (or terminate them if already commenced).

Conclusions

The new merger control regime under the Competition Ordinance and the Merger Guideline should feel familiar to market players in the telecommunications sector in Hong Kong. In a way, the new merger regime under the Competition Ordinance is a continuation of the prior merger regime under the Telecommunications Ordinance. This circumstance will help telecommunications businesses get ready for full compliance from the moment of the Competition Ordinance's full entry into force on 14 December 2015.

Adrian Emch
Partner, Beijing
T +86 10 6582 9510
adrian.emch@hoganlovells.com

Drive towards "more market" in China's standard-setting process

On 11 March 2015, the State Council issued the Reform Plan for Further Improving Standardization Work ("**Reform Plan**"), a master plan with specific measures to transform the current government-dominated standardization system into a (more) market-driven one.

The main theme in the Reform Plan is consistent with the Chinese government's broader initiative to de-regulate the market. During the Third Plenary Session of the 18th Central Committee, the Communist Party of China decided to let the market play a (more) "decisive" role.

Current situation

China's Standardization Law provides for four types of standards – i.e., national standards (which apply nationwide), industry standards (which apply to a particular industry), local standards (which apply to a particular province or municipality) and enterprise standards (which are set by companies). The first three types of standards are either mandatory or recommended (i.e., voluntary in nature).

At present, China maintains a "top-down" standardization system. This means that the government plays a dominant role in the standard-setting process, particularly when it comes to the first three types of standards mentioned above. Businesses may participate in the standard-setting process, but their role is more limited than typically in Western jurisdictions. Foreign businesses' involvement in standard-setting in China is even less prominent at this point in time.

Reform Plan highlights

According to the Reform Plan, the Chinese government intends to consolidate the existing mandatory national standards, industry standards and local standards into a new single category of mandatory national standards. Furthermore, the government aims to limit the scope of application of mandatory standards to areas which concern human health and property safety, national security, environment protection and basic requirements regarding social and economic administration. Those mandatory national standards will be made available to the public free of charge.

Currently, the Standardization Law does not recognize the key role of standard-setting organizations in setting standards as in many Western jurisdictions. Pursuant to the Reform Plan, the Chinese government plans to encourage organizations (e.g., industry associations) and technology alliances to drive the standardization process.

In addition, the Reform Plan sets out measures to ease restrictions on market-based standardization, including removing record-filing requirements for enterprise standards and potentially making it easier for foreign-invested enterprises to participate in standard-setting in China.

Antitrust implications

The Reform Plan, if implemented, will carry antitrust implications. In particular, as the government plans to withdraw (to a certain extent) from the standard-setting process, the responsibilities of the participating companies and the standard-setting organizations will increase. Many such organizations include competitors deciding to adopt a single standard among various alternatives, hence "reducing" the number of options in the market. Decisions between competitors – including exchanges of certain business information – are subject to scrutiny under antitrust rules, including in China. Furthermore, as the market players take the initiative in standard-setting, they may form alliances and consortia. Depending on their market position, antitrust risks increase if those alliances and consortia aim to be exclusive.

In short, the Reform Plan, if implemented, shifts responsibilities to market players, and their antitrust responsibilities and risks will grow in parallel.

Andy Huang
Associate, Beijing
T +86 10 6582 9533
andy.huang@hoganlovells.com

China's first antitrust regulation against IPR abuses

On 7 April 2015, the State Administration for Industry and Commerce ("**SAIC**") released the Regulation on the Prohibition of Conduct Eliminating or Restricting Competition by Abusing Intellectual Property Rights ("**SAIC IPR Abuse Regulation**"). The regulation came into force on 1 August 2015.

The SAIC IPR Abuse Regulation implements the high-level principle in the Anti-Monopoly Law ("**AML**") that the law does not apply to the lawful exercise of intellectual property rights ("**IPRs**"), but does apply to anti-competitive IPR abuses. The regulation is the first attempt by a Chinese authority to provide a comprehensive set of rules for the enforcement of the AML in the IPR field, and it gives some guidance on what conduct will violate the AML in the context of exercising one's IPR. However, the regulation does not bring about any ground-breaking changes as compared to the current state of law and practice.

Regulation's coverage
The SAIC IPR Abuse Regulation has 19 articles. The regulation's key guidance is on how the AML's abuse of dominance prohibition applies to the IPR field. Some of the guidance is generally applicable to the exercise of IPRs: refusal to license; exclusive dealing; tying; imposition of unreasonable conditions; and discriminatory treatment, none of which is surprising in the general context of the AML.

Another part of the regulation looks at certain types of IPRs and specific situations, such as patent pools and patent standard setting and implementation.

Licensing clauses
The SAIC IPR Abuse Regulation imposes a series of general restrictions on IPR holders – to the extent they have a dominant position – in their licensing activities.

Although the regulation confirms that the ownership of an IPR does not necessarily mean dominance, it also makes clear that an IPR's nature as a legally authorized "monopoly" over a technology or product is an important factor in determining dominance. As a result, companies should either make a detailed analysis of whether their respective IPR confers market power leading to dominance or proceed on the assumption they have a dominant position.

If the risk of dominance cannot be excluded, certain conduct in the licensing context will become more risky in view of the regulations and more aggressive antitrust enforcement by the authorities. Beyond the more general principles such as the prohibitions of tying or discriminatory treatment contained in other articles, the SAIC IPR Abuse Regulation lists a number of types of licensing conditions that dominant licensors cannot insert in agreements absent valid reasons – for example, exclusive grant-backs to improved technology, no-challenge clauses, non-compete clauses, etc.

Refusal to license
One article of the SAIC IPR Abuse Regulation that has been subject to intense discussions is the "refusal to license" clause. According to that clause, the holder of an IPR that is an "essential facility" must agree to license under reasonable conditions.

The regulation also lists a few "factors" to be considered in a refusal to license assessment, which may limit the scope of application of the clause:

- the IPR must be indispensable for the licensee to compete in the market
- the refusal to license must have a negative impact on competition or innovation
- the license does not cause unreasonable harm to the licensor

It appears that, on this point, the SAIC IPR Abuse Regulation follows European Union antitrust law, without however taking on board an additional qualifying factor usually present there – namely, that the licensee use the licensed IPR to bring a "new product" to the market, rather than copying the licensor's existing product.

Patent standard setting and implementation
Another of the most controversial provisions in the SAIC IPR Abuse Regulation attempts to regulate patent standard setting and implementation. This provision starts with the general principle that IPRs should not be used to anti-competitive ends during the setting and implementation of standards. Then, the provision continues with more detailed prohibitions of (1) patent assertions after failing to disclose patents in the standard-setting phase and (2) violations of the fair, reasonable and non-discriminatory ("**FRAND**")

principle during licensing activities in the standard implementation phase.

The first prohibition must be analyzed against the background of the recent announcements by the State Council to transition standard setting from an essentially government-driven to a more market-driven process. With this provision in the SAIC IPR Abuse Regulation, SAIC has signaled that it intends to play a role in the antitrust scrutiny of the standard-setting process.

The second prohibition throws SAIC right into the middle of one of the most contentious issues surrounding the antitrust and IPR debate – namely, the obligation to license standard essential patents under FRAND terms.

Conclusions

The SAIC IPR Abuse Regulation is the first comprehensive antitrust regulation in the IPR field in China. Nonetheless, some of its rules are already featured in existing laws and regulations in a less systematic way – in particular, the implementing provisions of the Contract Law and the Foreign Trade Law – or have been developed through court judgments and authority case practice – such as the *Huawei v. InterDigital* judgments or the decision by the National Development and Reform Commission ("**NDRC**") in the *Qualcomm* case.

Perhaps the biggest impact of the SAIC IPR Abuse Regulation is that, through it, SAIC signals that it is "up for business," ready to take on alleged IPR abuse cases, in addition to NDRC, the Ministry of Commerce ("**MOFCOM**") and the courts.

NDRC has already responded to the issuance of the SAIC IPR Abuse Regulation by launching its own effort to draft guidelines on the same subject – antitrust enforcement against IPR abuses – which, if enacted, would be applicable to all three Chinese antitrust agencies, NDRC, SAIC and MOFCOM.

Adrian Emch
Partner, Beijing
T +86 10 6582 9510
adrian.emch@hoganlovells.com

www.hoganlovells.com

Hogan Lovells has offices in:

Alicante
Amsterdam
Baltimore
Beijing
Brussels
Budapest*
Caracas
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta*
Jeddah*
Johannesburg
London
Los Angeles
Luxembourg
Madrid
Mexico City
Miami
Milan
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Rio de Janeiro
Riyadh*
Rome
San Francisco
São Paulo
Shanghai
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar
Warsaw
Washington, DC
Zagreb*

"Hogan Lovells" or the "firm" is an international legal practice that includes Hogan Lovells International LLP, Hogan Lovells US LLP and their affiliated businesses.
The word "partner" is used to describe a partner or member of Hogan Lovells International LLP, Hogan Lovells US LLP or any of their affiliated entities or any employee or consultant with equivalent standing. Certain individuals, who are designated as partners, but who are not members of Hogan Lovells International LLP, do not hold qualifications equivalent to members.
For more information about Hogan Lovells, the partners and their qualifications, see www.hoganlovells.com.
Where case studies are included, results achieved do not guarantee similar outcomes for other clients. Attorney advertising.

Images of people may feature current or former lawyers and employees at Hogan Lovells or models not connected with the firm.

© Hogan Lovells 2015. All rights reserved. 10407_Aa_0815

* Associated offices