TMT China Brief

Winter/Spring 2017

Hogan Lovells

Contents

Editor's note

Welcome to this edition of our TMT China Brief!

This edition features a total of 15 articles which capture the significant TMT developments in Greater China since our last TMT China Brief. These latest developments cover an extraordinary breadth of topics and demonstrate a strong increase in the nuance and complexity of TMT law and practice in the region.

Cyber security and film made headlines with the passage of history-making top-level laws in Mainland China. Cyber security in particular has commanded the spotlight because of the Cyber Security Law's uncertain scope and because draft follow-on legislation on the cyber security review of network products and services has raised at least as many questions as it has answered. At a sector-specific level, cloud service providers need not only be in tune with new cyber security issues, but also new draft regulations setting out more precisely the licensing regime for offering cloud services in the Mainland, as well as the limits of foreign participation in this space.

Fintech is seeing doors open in Hong Kong, with stored value facilities licenses on the rise covering a greater diversity of business models, and potential pathways opening up for use of blockchain. In the Mainland, we see concerns about fair competition in the electronic payments space, as demonstrated by a case punishing cartel behaviour that is particularly interesting due to the fact that the cartel turned out to have been government organised!

Meanwhile, consumer protection and data privacy continue to be hot topics, with new draft regulations on consumer protection in the Mainland, and Hong Kong's Consumer Council publishing regulatory and best practices recommendations for online retail. Protection of minors in cyber space is also gaining greater regulatory momentum in both jurisdictions.

In the IP arena, ".cn" domain name complaints get a lift in a potential opening to the long-standing 2-year statute of limitations, and in this edition we also examine the complexities of utilising ISP blocking in Greater China to combat trademark and copyright infringement.

Lastly, don't miss our article on developments in China's foreign exchange controls, as the government seeks to curb capital flight and perceived abuses of outbound investment. This topic broadly impacts Chinese participation in global deals, not just within the TMT space. We dispel doomsday predictions, while at the same time giving insight into which deals are most likely to be affected.

We are pleased to present you this edition, which we hope will help you navigate through all these new developments.

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

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

China passes controversial Cyber Security Law

China's Cyber Security Law, which will take effect from 1 June 2017, was finally adopted on 7 November 2016. The net result is ongoing controversy coupled with uncertainty.

Multinational businesses in particular question the intent behind the law and criticising its vagueness, as the final draft contains a number of broadly framed defined terms that are critical to its interpretation but which continue to leave much to be resolved through detailed measures that may or may not follow. All in all, the direction of travel is towards a much more heavily regulated Chinese internet and technology sector. The question remains as to whether China's cyber space will be truly integrated with the rest of the world in the coming years.

Key issues

The Cyber Security Law's 79 articles address a wide range of issues, but we see particular focus on three main aspects:

- **Technology regulation:** The Cyber Security Law seeks to regulate what technology can or cannot be used in China's cyber space, including by: imposing requirements for pre-market certification of "critical network equipment" and "specialised security products"; and designating certain systems as "critical information infrastructure" that will be subject to national security reviews and detailed measures to be issued by the State Council. The concern here is whether there will be a protectionist slant to these measures that will make it difficult for foreign players to compete.
- **Cooperation with authorities:** The Cyber Security Law imposes duties on "network operators" to provide technical support and assistance in national security and criminal investigations and to retain weblogs for at least six months.
- **Data localisation:** The Cyber Security Law requires operators of "critical information infrastructure" to store personal information and "important data" within China, save where it is truly necessary to send this data offshore and the offshoring arrangements have cleared a security assessment process that is yet to be defined. Revisions in the final draft broaden the scope of personal data from "citizen's person data" to "personal data," suggesting that personal information of foreigners in China will also be subject to the localisation requirement. This does little to reassure foreign residents who may need to move data across borders for any number of good reasons.

Continuing uncertainty as to scope

Obligations under the Cyber Security Law attach to two main classes of business: "network operators" and operators of "critical information infrastructure." Neither of these terms are defined in any detail under the new law, leaving much room for speculation and interpretation.

"Network operators" are defined as an "owner or manager of any cyber network and network service providers," casting a potentially very wide net for the obligations to maintain weblogs and cooperate with authorities noted above.

"Critical information infrastructure" is ultimately left to be defined by the State Council, but is stated in the Cyber Security Law to be critical infrastructure relating to critical industries, being public communications and information services, energy, transportation, water conservancy, finance, public services, e-government affairs and other significant industries and sectors, as well as any other infrastructure that may jeopardise national security, the national economy, people's livelihoods or the public interest were it to be destroyed, lose functionality or experience data leakage. Ultimately it is a subjective test.

Following the recent inspection of critical information infrastructure (Cyberspace Inspection) carried out by the Office of the Central Leading Group for Cyberspace Affairs, (often referred to as the Cyberspace Administration of China, or CAC), the CAC moved to define "critical information infrastructure" by reference to a three step process, beginning with the identification of critical businesses, then identifying information systems and industrial control systems that ensure the functioning of those businesses, and then finally identifying the degree to which these businesses are vulnerable to attack in relation to specific items of infrastructure forming part of their systems.

In its press release on the Cyberspace Inspection, the CAC set out a non-exhaustive list of critical businesses within each of the critical industries identified. In relation to telecommunications and internet sector, a wide swathe of facilities and non-facilities-based services were identified, from voice, data, basic internet networks and hubs, through to domain name resolution systems, data centres and cloud services. A section headed "business platforms" referred to instant messaging, online shopping, online payments, search engines, e-mail, BBS, maps and audio/video services. To give context to the degree of materiality envisaged in the wake of the Cyberspace Inspection, if for example, they have over one million average daily visitors or if a cybersecurity breach would affect the life and work of over one million people, web sites are considered to be critical information infrastructure of critical businesses. Corresponding examples applicable to online platforms are RMB1m in direct economic loss due to a cyber security breach or the loss of personal data of one million people.

In addition to key definitions such as "network operator" and "critical information infrastructure," the scope of certain obligations under the Cyber Security Law lacks precision in many areas. It is not clear, for example, what extent of technical assistance that "network operators" will be obliged to provide in support of national security and criminal law investigations. Does this encompass, for example, directions to install "back doors" in technology that would enable uninterrupted access by law enforcement to data and communications? Similarly, what security assessment will need to be applied to proposals to offshore personal information and important business data collected or created by critical information infrastructure? These are fundamental issues for many of the foreign business and investors in this area.

Implications

China's Cyber Security Law has drawn significant criticism since the first draft was tabled. Multinational businesses have expressed grave concerns over the potential for discriminatory application of the law to foreign technologies and equipment, as well as over data localisation requirements that hamper efficiencies and may be counter-productive to information security. Human rights and free speech advocates see in the Cyber Security Law a further tightening of state control of China's media and communications infrastructure, especially against the broader background of new restrictions on internet publishing.

It is difficult to reconcile the Cyber Security Law with China's move to integrate with the global economy and gradually open the technology services sector to wider foreign participation. It is not clear, for example, whether or not foreign technologies will continue to meet the requirements for use in critical information infrastructure in China, and to what extent there will be official or unwritten requirements for "back doors" that may ultimately compromise security and intellectual property rights. There are also worrying parallels between the requirements under the Cyber Security Law and requirements for the use of state-approved "secure and controllable" technologies in the financial services sector. Here, the concern is that foreign technologies may be deemed incapable by their nature of being "secure and controllable" or that achieving certifications against such standards may involve the disclosure of source code and other trade secrets or standards that only domestic players can meet.

More broadly, the Cyber Security Law escalates concerns that China is pursuing a course where its domestic internet becomes something isolated and detached from the global internet. This is already true to a degree in relation to internet content, which is heavily censored in China. The thrust of the Cyber Security Law is to expand monitoring to the infrastructure level, with implications for technical standards and interoperability. If the result is that businesses in China are required to operate using technologies that meet China's security standards but do not meet international standards, there is a threat that networks in the rest of the world will be even more reluctant to interconnect due to security concerns. What this could mean for the international growth of China's fast-growing technology sector remains to be seen.

There is some evidence that China is alive to the need to react to the widespread international criticism. Chinese Premier Li Keqiang remarked during his August 2016 visit to the US that China will communicate with

foreign companies to seek to find effective approaches to cooperation in cyber security matters. Some progress on this front may be seen in the CAC's opening of its Technical Committee 260 to participation by foreign technology businesses. Amongst other responsibilities, Technical Committee 260 is tasked with developing standards that will be applied under the Cyber Security Law.

Practical next steps

It is clear that businesses operating in China must review their technology and data arrangements in the light of the implications of the Cyber Security Law coming into effect on 1 June 2017. Technology businesses will need to review their Chinese business strategies and evaluate whether or not their products and services fall within the scope of the new requirements and if so, for example, whether they will be subject to some form of certification or worse still, face exclusion from the market. They also need to consider matters such as the nature of personal data collected in China and how and where this data is stored.

Businesses in other sectors will need to evaluate their technology use in China across a range of fronts, including:

- the impact of the Cyber Security Law on the available options for technology procurement in China and what the range of options means in terms of performance, functionality, cyber security and other matters
- the interoperability of onshore systems with offshore networked systems
- options for data server locations, and
- potential knock-on effects of the Cyber Security Law for related areas of regulation, such as the encryption regulations and telecommunications licensing.

Businesses in the financial services sector, in particular, will need to consider the Cyber Security Law in the context of their specific technology risk management regulations, with an eye in particular on the move towards "secure and controllable" technology requirements, which to those in the know have set something of a worrying precedent.

Roy Zou
Partner, Beijing
T +86 10 6582 9488
roy.zou@hoganlovells.com

Andrew McGinty
Partner, Shanghai
T +86 21 6122 3866
andrew.mcginty@hoganlovells.com

Draft legislation to affect China cloud services market access

On 25 November 2016, the Ministry of Industry and Information Technology (MIIT), China's telecommunications and Internet regulator, issued a draft Circular on Regulating Business Activities in the Cloud Services Market (Draft Circular) for public comment. The stated aims of the Draft Circular are to improve the cloud services market environment and further regulate business activities in this sector.

In addition to introducing a number of minimum service, data protection and network security requirements that cloud operators must observe, the Draft Circular is of particular interest to the industry due to its focus on licensing requirements and the rules it sets out for market participation by foreign technology companies, including through cooperation with license holders in China. The period for public comments on the draft ended in December 2016.

Licensing requirements for providing cloud services

The Draft Circular clearly states that cloud services refer to the internet resource collaboration (IRC) services sub-category under the category of internet data centre (IDC) services, a "Category One" Value-Added Telecommunications Service (VATS) under the 2015 edition of Classification of Telecommunications Services Catalogue (2015 Catalogue). Such statement finally directly links IRC services to cloud and IDC services, a view that had been widely held since the IRC services category was introduced in the 2015 Catalogue, but up until now has lacked a specific legal basis.

As IRC services, cloud services will be subject to separate licensing requirements and technical assessments. As stated in the Draft Circular, cloud service business operators in China must comply with the requirements on funding, personnel, venues, facilities etc. under the various laws applicable to VATS, and are subject to passing technical assessments and obtaining VATS licenses. The applicable laws in question specifically include the Telecommunications Services Operating Permit Administrative Measures (MIIT Decree No. 5) and the Circular on Further Regulating Market Entry for Internet Data Centre Services and Internet Access Services (MIIT Telecom Administrative Letter No. 552) of 2012 (Letter No. 552).

When IRC services were originally introduced into the 2015 Catalogue, it was not clear whether they would give rise to licensing requirements above and beyond those applicable to IDC licensing, or whether the 2015 Catalogue allowed all IDC license holders to engage in cloud services. It was also not clear whether all non-licensed providers were meant to be excluded from offering cloud services.

The Draft Circular clarifies these points:

- additional licensing is required
- having a normal IDC license is not enough, and
- there must be no direct-to-customer offering of cloud services by unlicensed entities.

This is consistent with recent developments in MIIT practice, where we have already seen implementation of separate testing and application materials for IRC services as a distinct subset of IDC and with its own specific licensing (with the first IRC services license having been issued in 2016). It also appears from the Draft Circular and MIIT's recent practice that MIIT intends to stop any cloud services from being offered as "unregulated" services, likely bringing an end to regulated/unregulated split-services collaboration models in the cloud space (but see discussion below for what collaboration models will be allowed).

VATS licensing for entities with overseas investment

The Draft Circular emphasizes that overseas investors investing in and operating cloud services business in China must apply to establish a foreign-invested telecommunications enterprise (FITE) which has been issued (as part of its establishment process) a corresponding VATS operating permit in accordance with the Foreign Invested Telecommunications Enterprises Administrative Regulations, the Agreement on Trade in Services under the Mainland and Hong Kong/Macau Closer Economic Partnership Arrangement (CEPA) and other such policies concerning the liberalization of IDC services.

At present, FITEs in the VATS sector may only be established (with some exceptions such as call centres in the Shanghai Free Trade Zone) as a joint venture between a foreign investor and a domestic enterprise, with the foreign investor's maximum capital contribution capped at 50%. In practice, however, the ultimate question of liberalization goes back to MIIT's interpretation of China's World Trade Organisation (WTO) commitments: essentially the consistently held view has been that if a service is not included in the WTO list of liberalized VATS (neither IDC nor IRC were), then it is not open to foreign investment unless MIIT decides otherwise. Only the CEPA route has really been open to qualifying Hong Kong entities and even then it has proven difficult to obtain approval for FITE JVs in IDC services. What is not clear from the Draft Circular is whether foreign investors will be required to obtain an IDC permit in order to operate non-infrastructure type cloud services, such as Software-as-a-Service (SaaS) as opposed to Infrastructure-as-a-Service or Platform-as-a-Service, as there is no need for a SaaS operator to have its own infrastructure and the significant costs associated with this. Article 6 of the Draft Circular suggests not ("Operators of cloud services must use network infrastructure, IP addresses, bandwidth and other such access resources provided by a telecommunications provider having the appropriate permits and qualifications"), but the reference to Letter No. 552 and the fact that IRC is a sub-category under IDC services tend to suggest the contrary.

Because of these historical market access issues, many foreign technology companies have focused their efforts on participating in the Chinese market via some form of non-equity holding technical services collaboration with a domestic Chinese partner (Cooperative Model). This form of collaboration is also addressed under the Draft Circular.

Collaboration between cloud service providers and other partners

In practice, Cooperative Models have taken various forms, with various structures being utilized by different industry participants with respect to contracting, client interfacing, service arrangements, billing, and issuance of tax invoices.

The Draft Circular proposes to unify this, setting strict rules in these areas and bringing the structuring of Cooperative Models officially under direct government regulatory scrutiny. Article 4 of the Draft Circular provides that cloud services operators engaging in technical collaborations with relevant organizations have an affirmative duty to report the details of their cloud services collaboration in writing to MIIT. By way of comparison, only in the media industry there is a similar level of regulatory scrutiny where cross-border collaborations are subject to approval.

Further, the following activities are not permitted during the course of collaboration:

- the leasing, lending or transfer of a telecommunications services operating permit to a partner in a disguised manner by any means, or providing to any partner the resources, venues, facilities or other conditions for unlawful operations
- a partner entering into contracts directly with users

– using only the trademark and brand of a partner to provide services to users, and

– unlawfully providing to any partner user personal information and network data, and

– other activities which violate laws and regulations.

Pursuant to the above provisions, the non-licensed party in a Cooperative Model is not permitted to enter into contracts with users directly or provide services to users by using its trademark and brand only. In other words, such unlicensed party must serve in a subordinate capacity without a direct relationship with the cloud customer, thus undermining the value proposition for many overseas providers. The 'sweep up' in the last bullet could be a veiled reference to Variable Interest Entity (VIE) structures, which have, in recent arbitration decisions at least, been found to violate mandatory provisions of Chinese laws by circumventing the obligation on the foreign 'operator' to obtain a VATS permit in China. The Draft Circular also specifically bans circumventing the great firewall of China by an operator linking its servers to an international network by using leased lines, virtual private networks or self-built international channels.

Some foreign technology providers operating under a Cooperative Model may already have operating structures that are aligned with the rules in the Draft Circular. Others, however, will need to review their current or contemplated collaboration arrangements with domestic cloud service providers in light of the implication of the Draft Circular, should it come into effect as currently written.

Conclusion

It was inevitable that cloud services were going to be regulated in China. However, the key issue raised by the Draft Circular for foreign investors is whether they are going to be partially or wholly shut out of this lucrative and fast-growing market. By aligning the category with IRC and IDC, which has traditionally been closed to all but the CEPA qualified Hong Kong investors, the Draft Circular suggests that this may well be the case – depending on whether the reference to CEPA should be read as excluding all those who do not fit within the CEPA tests and thereby potentially depriving China of the skills and technologies of some of the most advanced operating models and operators in the world. Cross-border collaboration remains possible, with some restructuring needed for existing models that do not conform. But, at the end of the day, the real question is whether in practice MIIT will create a true level playing field and will allow foreign investors to set up FITEs in this area, and for SaaS operators, whether this can be without imposing an unnecessary financial burden on them to invest in infrastructure.

Liang Xu
Partner, Beijing
T +86 10 6582 9577
liang.xu@hoganlovells.com

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

China's new foreign exchange controls create fresh concerns

Foreign investors and other parties transacting with Chinese counterparts are facing a new challenge: foreign exchange controls which affect all deals done involving currency outflows from China, notably outbound investments by Chinese buyers.

Current account versus capital account transactions

China divides transactions involving a cross-border element into:

- current account transactions which are liberalized and only require proof to be provided to the remitting and converting or receiving bank in China that there is a genuine and lawful underlying transaction, and
- capital account transactions which are still restricted and more strictly regulated.

Why has China imposed new controls?

There is currently a heightened sensitivity in China in relation to outflows of capital, with the authorities having very recently issued a series of policies to restrict these. This suggests that Chinese individuals and companies may have been trying to shift their money out of China in significant amounts in recent years as the growth curve and future growth prospects for the Chinese economy have weakened. Amongst other methods, it is known that one such route for shifting assets overseas involved fake transactions conducted via Hong Kong using dummy companies, e.g. setting up a shell company in Hong Kong and invoicing exports to China that were never delivered. It is not clear to what extent these structures were more motivated by individuals seeking to repatriate funds overseas as opposed to corporates.

Leaving aside the issue of the underlying fraud, these would constitute current account transactions. Eventually the Chinese authorities became aware of this through discrepancies in the relevant records, leading to increased scrutiny with regard to capital outflow transactions.

More recently concerns have been raised about questionable outbound transactions being used by Chinese companies and individuals to shift assets overseas. These, on the other hand, are capital account transactions. They are particularly sensitive and significant to China's regulators because of the potential to shift large amounts overseas in a single transaction.

What do the new policies say?

China issued a series of policies introducing the new procedures in the period running up to the end of 2016, through pronouncements by various government agencies, rather than hard law.

In November 2016, the central planning body and key outbound investment approval agency, the National Development and Reform Commission (NDRC), issued an internal note on restricting certain outbound capital account transactions. This restriction is scheduled to expire in September 2017. Based on such NDRC note, up to the end of September 2017, the following categories of outbound transactions will, in particular, be targeted by the Chinese authorities and will not be granted approvals to proceed in principle unless otherwise specifically permitted by the relevant authorities (based on criteria which are not in the public domain):

- outbound investments in real estate made by State-owned enterprises with a Chinese investment amount of US$1bn or more
- overseas investments involving an extra-large Chinese investment amount exceeding US$10bn
- outbound transactions outside the core business of the company involving an amount of US$1bn or more
- outbound investments directly made by limited partnerships

- foreign direct investment involving an acquisition of 10% or less of the shares in an overseas listed company
- investments in offshore targets that have an asset value that is larger than the Chinese acquirer
- investments in offshore targets where the investing entity is a newly-established vehicle, and
- transactions involving domestic capital participation in the delisting of overseas listed Chinese enterprises.

In addition, outbound investments made by Chinese enterprises with a high asset-liability ratio and low net assets yield will be monitored closely as well.

It was widely reported that on 28 November 2016, the Shanghai Branch of the State Administration of Foreign Exchange (SAFE) held an internal meeting with regard to the administration of cross-border receipts and payments. It was reported that, as a result of this meeting and the internal guidance to banks issued on its back, any single purchase or payment of foreign exchange and RMB/foreign currency disbursement in an amount equivalent to or greater than US$5m for capital account transactions must be first reported to the Beijing SAFE as a large transaction.

Such transactions may now only be carried out once the relevant authorities, including the People's Bank of China (PBOC), SAFE, NDRC, the Ministry of Commerce (MOFCOM) and others, have completed an authenticity and compliance review of the transaction and granted approval therefor. If the transaction amount exceeds US$50m (inclusive), a stricter level of scrutiny applies, involving direct monitoring by central SAFE in the system and a review. The Shanghai SAFE also emphasized that transactions must not be split up into smaller components in order to circumvent large amount transaction reporting.

On 6 December 2016, NDRC, MOFCOM, PBOC and SAFE jointly responded to a media inquiry regarding outbound investment administration, indicating that going forward the Chinese authorities pay particular attention to the following outbound investment transactions. This means the the following investments are subject to greater administrative scrutiny as compared to others:

- large investments in business outside the core business of the Chinese investor
- outbound investments made by limited partnerships
- investment in offshore targets that have asset values that are larger than the Chinese acquirers
- investments where the investing entity is a newly established vehicle [without any substantial operations], and
- "irrational" overseas investments in certain industries, specifically real estate, hotels, film, entertainment and sports clubs.

Conclusion

In general, what is clear from anecdotal evidence and our experience with actual client transactions is that payments out of China on outbound transactions are being subjected to far greater scrutiny as compared to say six months or a year ago. Summarising all the policy pronouncements so far, the levels of scrutiny on any outbound capital account transactions will depend on:

- the amount of money that is being transferred overseas
- the industry sector of the target
- the country to which the payment will be transferred, and
- the profile of the Chinese investor (e.g. newly established SPV and/or acting outside its core business).

The new procedures are somewhat opaque. Timing for completing the regulatory procedures for outbound direct investments is highly uncertain at present until we see the first few cases go through the new system, bearing in mind much of this is very recent in nature.

Extra time needs to be factored into payment deadlines for all transactions involving outbound payments from China, as the new approval process is likely to cause delays of up to several months in our estimation. Even the approval of the transfer of small amounts of money (less than US$ 10 million) may take up to one month.

In addition, based on our enquiries with local banks, currently PBOC grants an unofficial "quota" to each bank requiring the total capital outflow amount processed per month by the specific bank to be within the "quota" limits. This "quota" would apply to all capital outflows from China, even including payments under current account transactions (for example, cross border trading transactions) which, as noted above, are less highly regulated than capital account transactions. Transactions at month end are likely to be pushed into the next month due to quotas being used up. Good relationships with the relevant authorities and government officials will likely be crucial for getting larger transactions approved in a timely fashion, and we expect that many more interactions will be needed to explain the rationale of certain transactions to regulators.

Application documents for outbound approvals should include facts and evidence as to the genuine nature and business rationale for transactions (e.g. why the target is selling the asset and how the acquisition fits into the Chinese acquirer's strategy), so that any concerns in this regard from the regulatory stakeholders can be addressed at an early stage.

China will also be well aware of the cases where fraud was not involved but where Chinese companies going outbound (particularly but not exclusively State-owned Enterprises) overpaid or made overseas investments that

did not stack up commercially: it may also be using the new reviews and controls to "bring order" to the market and to weed out cases of fraud in the process, thereby preventing State-owned assets from being dissipated in ill-thought-through overseas forays.

This is clearly an area to watch as the new reviews are rolled out. We understand that the new policies create uncertainty and concerns for many transaction counterparties, particularly sellers to Chinese buyers. We remain, however, firmly of the view that this is not in any way the "end of the outbound trend" as some have predicted. Rather, we take the view that this is only a "bump in the road" and that where there is a genuine outbound deal that makes good business and strategic sense, it will still get approval/record filing and the deal will get done, even if the timetable stretches out somewhat.

Jun Wei
Partner, Beijing
T +86 10 6582 9501
jun.wei@hoganlovells.com

Andrew McGinty
Partner, Shanghai
T +86 21 6122 3866
andrew.mcginty@hoganlovells.com

Hong Kong's fintech surge: HKMA grants second round of stored value facilities licences

On 4 November 2016, the Hong Kong Monetary Authority (HKMA) announced a second round of eight successful stored value facilities (SVF) licensees under the Payment Systems and Stored Value Facilities Ordinance (Ordinance). Successful applicants in this round are 33 Financial Services, Autotoll, ePaylinks, K & R International, Optal Asia, PayPal, Transforex and UniCard Solutions.

With the issuance of the second round of SVF licenses, we now have 13 SVF licensees in Hong Kong, demonstrating the appetite for investment and growth in Hong Kong's emerging fintech ecosystem. Two licensed banks, Bank of Communications and Dah Sing Bank, are also SVF issuers, pursuant to section 8G of the Ordinance.

The gate opened in November 2015

The Ordinance commenced operation on 13 November 2015 with a one year transition period allowing existing SVF issuers to apply for a licence from the HKMA. From 13 November 2016 it became unlawful for any person to issue or facilitate the issuance of an SVF in Hong Kong without a licence (or the benefit of an exemption).

What's new for the second round of SVF licensees?

A diversity of business models

The players represented by the list of SVF licensees is impressive not only for its number, but also for its diversity.

The full complement of licensees now offering SVF services in Hong Kong includes technology giants such as Tencent and Paypal, telecommunications provider HKT, public transport fare operator Octopus and road toll system operator Autotoll. While these are all established and familiar names in the Hong Kong market, it is important to note that the successful licensees also include companies such as virtual card issuer Optal, China UnionPay card issuer K&R International, local e-wallet issuer TNG and traveller card issuer Transforex.

The clear implication is that the HKMA is encouraging a diversity of offerings in Hong Kong's fintech ecosystem,

with some players directed at retail payments and stored value, and others at business-to-business channels or collaboration under branded credit card schemes. Consumer choice for payment services in Hong Kong has received a significant boost, and we can expect the move to bring these players under HKMA regulation to continue to encourage wider change in the Hong Kong financial services market as these licensees expand their businesses into new channels.

A nuanced regulatory model

Shortly after the announcement of the first round of SVF licensees, the HKMA published a number of guidelines with which SVF licensees are expected to comply, including:

- Guidelines on Supervision of Stored Value Facility Licensees
- Practice Note on Supervision of Stored Value Facility Licensees
- Guideline on Anti-Money Laundering and Counter-Terrorist Financing (for Stored Value Facility Licensees).

These guidelines, and other guidance given by the HKMA during the licensing process, reflect the middle ground being sought in regulating SVF licensees to a different standard than is expected of banks. For example, the anti-money laundering and counter-terrorist financing (AML-CTF) guideline for SVF licensees, which we discuss in more detail below, are very similar in format to the guideline for financial institutions, incorporating different transaction thresholds for customer due diligence. This reflects different assumptions about typical transaction sizes for SVFs and the role played by SVFs in Hong Kong's financial system.

Float protection: a key concern

One of the challenges faced by SVF applicants completing the licensing process relates to measures required by the HKMA to ensure that stored value remains secure and available for use by SVF users. SVF licensees are required to have in place an effective and robust system to protect and manage the float and ensure that the funds are used only in accordance with SVF users' instructions, kept separate from the licensees working capital and protected against claims by the issuer's other creditors.

The specific requirements vary in each case based on the applicant's specific business model, but the HKMA has generally been requiring that a trust arrangement be put in place with a licensed bank, potentially with a bank guarantee or a custodian being appointed to monitor the flow of funds to and from a dedicated customer account holding the SVF float. The arrangements can be complex and will likely involve bespoke documentation. The HKMA has also been requiring an independent legal opinion validating the arrangements.

AML-CTF: a model for change?

The SVF regime has been implemented with significant focus on AML-CTF concerns. The balance being sought in the context of SVF is to enable fast and convenient payments and topping up of stored value through user-friendly digital interfaces, but at the same time recognize that an SVF could be used to facilitate payments for unlawful purposes.

As noted above, the specific AML-CTF guidelines approved for SVF licensees draw heavily from the guidelines applicable to licensed financial institutions, albeit recognising to a degree that SVF transactions are, in general, likely to be smaller in size than banking transactions. On this point, there is hope that the SVF regime will generate a regulatory experience that will

turn Hong Kong's AML-CTF regulation towards the potential of technology-driven customer verification solutions. The AML-CTF guidelines for SVF, for example, point to users' utility bills as being a benchmark for verification of a residential address (as do the banks' AML-CTF guidelines). The SVF regime surely presents an opportunity to reconsider the risk-based calculations delivering the conclusion that a paper utility bill is the best available evidence of its bearer's address. The potential for biometric verification of identity, for example, has gained traction in other jurisdictions and has been recognised by regulators in Hong Kong, albeit as a supplement to paper-based methods rather than a replacement for them. In order to avoid falling further behind, Hong Kong's SVF market, rich in technological aptitude, could be leveraged as a controlled environment in which to move forward.

Conclusion

In his press remarks at the announcement of the second round of SVF licensees, Howard Lee, Senior Executive Director of the HKMA, commented that the implementation of the SVF supervisory regime will strengthen public confidence in the use of SVF products and services which, in turn, will facilitate development and innovation in the local retail payment industry.

The increasing array of payments options being made available to consumers in Hong Kong through the SVF regime can only be good news. Ideally, the next step in progress will be to leverage the experience gained from the SVF regime towards a more technologically advanced financial services environment. Charting a course in this direction will enable Hong Kong to achieve its ambitions to be one of the world's leading fintech hubs.

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

Tommy Liu
Associate, Hong Kong
T +852 2840 5072
tommy.liu@hoganlovells.com

The shape of things to come –HKMA and ASTRI chart a course for blockchain in Hong Kong

On 11 November 2016, Hong Kong's Applied Science and Technology Research Institute (ASTRI) published its Whitepaper On Distributed Ledger Technology (DLT Whitepaper), a substantial research exercise commissioned by the Hong Kong Monetary Authority (HKMA).

The DLT Whitepaper is a useful and well-informed introduction to blockchain, or distributed ledger technology (DLT), as it is referred to throughout the paper, with a focus on how DLT may be used to enhance Hong Kong's banking system. Of particular interest is the discussion of a proof of concept project in mortgage loan applications that ASTRI has been developing with a number of Hong Kong's leading banks.

DLT has been widely touted for its potential to revolutionise financial services across a range of applications, from crypto-currencies to digital identity systems to smart contracts to fully automated clearing and settlements systems for payments and securities. The discussions are often expansive, ambitious and high level, making it difficult to bring a legal or regulatory assessment to any particular solution being proposed. The DLT Whitepaper is different. It does much to move forward discussion about Hong Kong's future in blockchain through its sharp focus on a specific proof of concept project, and at the same time recognises that there are legal and regulatory concerns that will need to be addressed in order to see this solution through to fruition.

DLT: a brief primer

DLT is a database technology having a structure that makes it particularly useful to the task of recording commercial transactions. Most databases in use today are centralised in the sense that there is a single set of transaction records (or a single "ledger") that is taken as the definitive record of all transactions that have taken place. Confidence in the completeness and accuracy of the ledger is established through trust in a central administrator having responsibility for maintaining the ledger, keeping it secure, vetting changes to it and otherwise keeping the ledger up to date.

DLT replaces the centralised transaction database with a multitude of separate but identical ledgers, each of which is maintained by a different participant in the database system. The "distributed" nature of ledgers in DLT systems gives the technology its name.

The word "blockchain" is often used interchangeably with DLT, and it is worth noting here what this word implies. Each distributed ledger contains a complete set of transaction records representing the entire history of transactions carried out on the system. Each transaction generates a separate transaction record (or "block"), which is added as a new entry to the end of the chain of blocks already making up the ledgers, as opposed to deleting and replacing the most recent entry. The addition of new transaction records to the existing set of records can be visualised as adding a new block to the end of a chain of pre-existing blocks, which in part explains the "blockchain" terminology often used to describe DLT.

Why is DLT an improvement over centralised systems? In actual fact, DLT will not always be an improvement. This is where a measure of hype concerning DLT meets careful consideration of system design. While there will be an important technical debate to be had about whether or not a DLT solution is the best technical solution for a particular transaction database, it is clear is that experts do see a significant number of cases where DLT brings advantages.

The principal benefit of DLT is that it eliminates the need for a trusted central administrator responsible for checking transaction records, ensuring the continued accuracy of the ledger and making error-free communication of the information requested by its users each and every time it is requested. The project of building a secure and trustworthy database is outsourced to the

participants. More fundamentally, the distributed ledger technology itself replaces the costly and time-consuming effort of verifying the authenticity of transactions and re-verifying transaction data each time an update is requested by a user.

Permissioned and unpermissioned ledgers

At this point it is useful to note the distinction the DLT Whitepaper draws between "permissioned" ledgers and "unpermissioned" ledgers. Permissioned or private ledgers are operated by a group of trusted or vetted participants who together agree rules on matters such as who gets access to the DLT, what data is stored in the ledgers, what security protocols apply and how a consensus is achieved on whether or not a new transaction record put forward by a participant for inclusion in the database is true and accurate or not. In some respects then, permissioned ledgers retain some of the characteristics of centralised database systems.

Unpermissioned ledgers, on the other hand, are completely open to the public without any central administration. Anyone can install the technology on their computers and connect into the system. The unrestricted openness of unpermissioned ledgers also means that anyone can contribute transaction records to the database, whether they are well-intentioned in doing so or not. Because users of unpermissioned ledgers cannot be trusted per se, a "technological fix" is required in order for the DLT itself to generate the same level of trust. The fix applied to this problem is that participants seeking to add a new transaction record must demonstrate to a majority of the others that a "proof of work mining" process has been completed as part of the preparation of the transaction record. The mining process involves the expense of significant amounts of computing resources and introduces some delay to the updating of the ledgers.

For the purpose of the proof of concept considered by ASTRI in the DLT Whitepaper, ASTRI concluded that permissioned ledgers have certain advantages over their unpermissioned counterparts, in particular that the former can make use of lower power computing facilities and make quicker updates. ASTRI also notes that securing access to a DLT system under a permissioned model also offers greater potential for the incorporation of personal data into the transaction records in a manner compliant with the Personal Data (Privacy) Ordinance (PDPO).

Data protection: a key regulatory consideration

The DLT Whitepaper is careful to note that PDPO compliance is one among many legal and regulatory issues that will need to be addressed as part of DLT adoption in Hong Kong.

The DLT Whitepaper concludes that permissioned DLT systems are likely to be preferable from a data protection compliance perspective to unpermissioned ones, given that permissioned systems are equipped with access controls. More broadly, permissioned DLT enables the encryption of personal data incorporated into the ledgers or, alternatively, allows this data to be linked from a separate secure source available only to the permissioned users.

ASTRI notes that unpermissioned DLT systems typically operate through anonymised DLT wallet addresses, which do not make individual identities visible on the blockchain. This does provide some privacy to users of these systems, but it is clear that anonymity is counter-productive to a system intended to support due diligence into specific individuals. A full analysis of unpermissioned DLT from a data protection compliance perspective needs to take into account the fact that anyone sufficiently motivated to seek to re-identify individuals from DLT transaction records would likely have the wherewithal to look beyond the DLT records and seek to re-identify individuals from other available databases. The fact of anonymity on the blockchain is not the whole story. In the "Big Data" era, powerful analytics technology can be applied to match databases that appear to be clear of personally identifiable information to those which are not, and this will be a critical compliance test for unpermissioned DLT systems that record personal data.

Other legal and regulatory issues

As well as the data protection challenges accounted for above, ASTRI also notes the following other legal issues as being potential obstacles for the proof of concept outlined in the DLT Whitepaper:

– **Electronic transactions**: The Electronic Transactions Ordinance (Cap. 553) (ETO) generally puts electronic signatures on equal footing with "wet ink" signatures under Hong Kong law. The ETO, however, excludes deeds from its scope of application, meaning that mortgage documentation would still need to be executed by hand in order to be legally binding. Still, we would note that the proof of concept as we understand it would not involve the implementation of any system that would actually charge or convey title. This being the case, the exclusions from the ETO should not be a constraint. However the ETO could foreseeably present challenges to more advanced DLT models, such as smart contracts, that envisage the DLT executing as well as recording the fact of the transaction. ASTRI notes that cheques were removed from schedule 1 of the ETO in 2014 to facilitate the use of e-cheques, and that a similar amendment could be made in respect of certain property transactions in the future if that were to be an extension of the scope of the mortgage loan application proof of concept.

– **Land registration**: Similarly, the Land Registry Ordinance (Cap. 128), which provides for the creation and maintenance of Hong Kong's Land Registry, only covers written conveyances. The Property Conveyance Ordinance (Cap. 219) requires related conveyancing documents to be signed, sealed and delivered. Again, we would note that we do not see these ordinances presenting a challenge for the proof of concept, which do not involve the creation of entries on the Land Register, but it is clear that legislative amendments would be needed in order to adopt a DLT model that enables execution of transactions.

Conclusion

The DLT Whitepaper represents a significant step forward in the thinking about DLT in Hong Kong. It is clear from the paper that DLT represents an opportunity to drive efficiency gains in the financial service sector, with a particular focus on mortgage loan application due diligence. There is an opportunity for Hong Kong to take a leadership role in DLT, and a firm push on a viable proof of concept would improve Hong Kong's chances of success in what is an increasingly hotly contested field of innovation. As a leading financial hub regionally and globally, Hong Kong has a large stake here and should take this opportunity to push forward as the new era of DLT-based financial services sees first light.

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

Louise Crawford
Registered Foreign Lawyer, Hong Kong
T +852 2840 5014
louise.crawford@hoganlovells.com

Chinese payment encryption device suppliers fined for participation in government-orchestrated cartel

On 4 November 2016, the State Administration for Industry and Commerce (SAIC) – one of China's antitrust authorities – published on its website three decisions, whereby three payment encryption device suppliers were fined by SAIC's branch in Anhui Province (Anhui AIC).

The Anhui AIC considered the companies' conduct to amount to market partitioning, prohibited under Article 13 of the Anti-Monopoly Law (AML). Interestingly, the market partitioning was orchestrated by the local branch in Anhui of the People's Bank of China (Anhui PBOC), one of the financial regulators in China.

Facts

On 20 October 2010, the Anhui PBOC selected three out of six companies as suppliers of payment encryption devices in Anhui: Sunyard System Engineering Co., Ltd., Sinosun Technology Co., Ltd., and Shanghai Haijiye Technology Co., Ltd. Payment encryption devices are used by bank customers to protect the security of payments from their bank accounts. These devices are typically distributed by the banks to their customers. In December 2010, the Anhui PBOC convened a meeting which was attended by the three companies and 20 local banks. In the meeting, the participants agreed, among other things, that

- the 20 banks were divided into three groups, and each group would distribute the payment encryption devices for one of the three suppliers, and
- the payment encryption devices would be distributed at a fixed price agreed in the meeting.

Following the meeting, the Anhui PBOC issued two circulars to embody the agreement above. In line with the two circulars, each of the three suppliers entered into agreements with the corresponding group of banks for the distribution of the payment encryption devices.

Ruling

Based on the findings above, the Anhui AIC held that the carving-up of customers among the three companies constituted a cartel practice prohibited under Article 13 of the AML, particularly because the three companies:

- attended the meetings organized by the Anhui PBOC, where they communicated their intentions with each other, and
- conducted themselves in accordance with the circulars issued by the Anhui PBOC, for example by not supplying devices to the banks allocated to the other suppliers; jointly fixing and adjusting the sales price; jointly paying commissions to the banks; and engaging in joint marketing and promotional activities.

For each of the three companies, the Anhui AIC imposed a fine and confiscated the illegal gains resulting from the practice in question. The penalties imposed on the three companies amounted to around RMB30m (US$4.3m) in total.

Takeaways

Unlike most cartel cases, this case involved a government body playing a significant role in the cartel practices – the Anhui PBOC took the initiative to select three suppliers for local banks, organize meetings to "assign" each of the three suppliers to a fixed group of banks and set the price for the payment encryption devices. From the decision it seems that the three companies would not have been able to supply their products if they had chosen not to obey the Anhui PBOC's directions. Indeed, the three suppliers cited this point as a defence in the investigation process. However, the Anhui AIC did not agree.

This is not the first case involving cartel conduct "supported" by government actors. On several occasions in the past, the Chinese antitrust authorities have attributed liability for cartel conduct to the companies involved, even where the cartel was "organized" by a government body. For example, in the *Fireworks* case, six fireworks suppliers divided up the sales territories in Chifeng, a city in Inner Mongolia, following regulatory requirements by the local government body responsible for work safety. In that case, the decision by SAIC's Inner Mongolia branch in May 2014 similarly found such conduct to be a market partitioning practice in violation of Article 13 of the AML.

The National Development and Reform Commission (NDRC) – another antitrust authority in China – took a similar position. In June 2015, NDRC's local branch in Yunnan Province found that four telecommunications carriers had entered into an anti-competitive agreement on their promotional activities. The four carriers were fined despite the fact that the local telecommunications regulator had taken the initiative in organizing the various discussions leading to the allegedly anti-competitive agreement.

These cases stand somewhat in contrast with the Vitamin C litigation in the United States, where an appellate court decided to exculpate Chinese vitamin exporters found to have engaged in cartel conduct due to regulatory intervention by government bodies in China.

In China, the government still plays an important role in both macro- and some micro-economic activities, even over 30 years after it introduced the market-oriented "reform and opening up" policy. In such an environment, the difficulty for businesses operating in China is that, on the one hand, they need to comply with the various regulatory requirements by government bodies and, on the other hand, they must ensure full compliance with the law, including antitrust law. The antitrust authorities' position, as illustrated in this case, may potentially put companies in a dilemma: face antitrust risks or lose business opportunities (if they choose not to work with a government body on a potentially anti-competitive project).

The difficulty is particularly significant for companies operating in regulated industries. For example, in the heavily regulated telecommunications and financial sectors, the government plays a major, if not predominant, role in economic activities. Companies from such sectors need to comply with various regulatory requirements on a daily basis. This case and prior cases show the importance of legal awareness and effective compliance systems – a mandate from a government body does not necessarily protect companies from potential antitrust liabilities.

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

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

Now playing: New film law impacts the Chinese silver screen

On 7 November 2016, China's highest legislative body, the Standing Committee of the National People's Congress, passed the Film Industry Promotion Law (Film Law). The Film Law took effect on 1 March 2017.

The Film Law is the first comprehensive "law" in China targeting the film industry specifically and was more than 13 years in the making. Up until now, the Chinese film industry was governed by a series of regulations and rules, but no top-level "law" in the Chinese legislative hierarchy providing an overall regime to govern the film industry. Passage of a top-level "law" now indicates that the highest levels of the Chinese government recognize the importance of guiding China's burgeoning film industry.

Broadly speaking, the Film Law is being well-received by a diverse set of business executives, Chinese film studios, academics and legislators. While no law is perfect from inception, and questions remain about how the Film Law will be interpreted and implemented, participants in the Chinese film industry are generally happy to see comprehensive legal guidance over the industry.

While the Film Law is a high-level statutory regime, the intention is for incremental change, not a radical overhaul, to China's film industry. The existing systems of most government approvals, censorship, and market access by foreign participants are still in place. However, the Film Law makes some tweaks to the existing rules and provides for some measures to further encourage growth in the film industry.

Does the Film Law apply to your film?

The Film Law's scope applies to the development, production, distribution and screening of films in China which are to be released in feature format, whether in fixed places like theaters and cinemas or on portable projection equipment.

In other words, the Film Law applies to the whole production and distribution cycle for domestically produced films intended for the big screen, whether released in China or to be exported.

As before, big screen films that will also be shown on the Internet or TV will continue to also be subject to specific regulations surrounding internet or TV broadcasting if they are to be shown via such media.

However, the Film Law apparently does not apply to made-for-internet and made-for-TV films, and instead only the relevant internet and/or TV specific regulations would apply.

Initial studio / per-film production permission to be abolished

Notably, the Film Law removes the initial permission step that Chinese companies previously had to satisfy before they could engage in film production. Before the Film Law, Chinese companies had to be approved as a "studio" or be permitted on a per-film basis before they could engage in making films.

By removing this initial qualification requirement, the government hopes that more Chinese companies will be able to enter the film production business, and faster. This change will primarily benefit Chinese companies, but may also help foreign companies looking to engage in Sino-foreign co-productions, as foreign companies may now have a greater range of Chinese partners to choose from.

Another potential effect will be increased use of special purpose vehicles for making films (for example, single-purpose corporations), now that an entity itself does not need special qualifications for market entry. We expect this to be a welcome development from the perspective of structuring film finance transactions, particularly for those parties wishing to follow corporate and financing structure models commonly used in Hollywood.

Potentially decreased market access to foreign companies and personnel in co-productions

The Film Law does not overhaul the existing regulatory regime on foreign participation in the Chinese film industry, but it may have the effect of raising the bar on which foreign companies and personnel have the right to cooperate with Chinese companies and produce films in China. Specifically, the Film Law states that foreign companies may not engage in local film production if they have ever "engaged in activities that damage China's national dignity, honor or interests; threaten social stability; or hurt the nation's people's feelings."

This new rule for foreign companies suggests that foreign studios, directors, and actors/actresses may have to be more careful in all their projects and public statements, not just in their China-specific projects, in order to ensure they have the opportunity to work on Chinese productions. This new rule shows an even greater sensitivity and desire by the Chinese government to control public expression about China, even outside the country's borders.

Domestic treatment of Sino-foreign co-produced films

The Film Law provides that Sino-foreign co-produced films (Co-Productions) are to be regarded as though they were domestically produced, provided that certain ratios for creative input, investment and profit distribution are met.

Requirements for creative input, investment and profit distribution by both the Chinese producer and foreign producer already existed before the Film Law, and it is already the case that Co-Productions are treated like domestic films in regards to import quotas and screen-time. In contrast, the Film Law indicates that Co-Productions will be treated equally with domestic productions in all regards now, including, for example, in censorship approval processes. What remains unclear, however, is whether this equal treatment of Co-Productions and domestic films requires a different ratio of creative input, investment and profit distribution than currently exists for Co-Productions. The Film Law's text is ambiguous in this regard, and it may contain an additional layer of meaning about ratios. Additional legislation is expected to follow in the near future which may clarify these points.

Review of scripts and of final products

Similar to rules already in place, under the Film Law, only the outline of a script needs to be placed on-file with the government prior to shooting, unless certain themes are raised. If the themes are "significant" or implicate national security, diplomacy, ethnicities, religion or the military, then a full script must be submitted to the government for approval. The main differences between the new Film Law and the current rules on scripts are minor language changes; however legislators and industry experts expect the implementation of the Film Law, in practice, to be the same as the existing process for reviewing scripts. If anything, the Film Law indicates a general trend for Chinese approval of film scripts: less government supervision and oversight at the early stages in the process in film making.

On the other hand, Chinese regulation of the film industry is also trending toward greater government supervision at the later stages of film production, particularly at the stage of final pre-release approvals. Under the Film Law, some significant changes exist regarding final pre-release approvals. First, final approval is being de-centralized, which means final approval will occur at the provincial level of the government film authority rather than at the central level. Second, the State Administration of Press, Publication, Radio, Film and Television (SAPPRFT) – China's film authority – is being charged with producing specific standards for granting approval, which will be released for public comment before being finalized and adopted. Third, a panel of at least five experts must be deployed to evaluate each film. Such experts will come from a pool of experts, together with any outside experts needed in relation to the specific content of a film. How these experts are chosen and the methods they should employ in evaluating films is to be decided in forthcoming regulations.

The introduction of written standards and expert participation is intended to balance the de-centralization of approvals, in order to ensure consistency and prevent forum shopping by producers. The written standards and expert involvement also likely exist to serve as an internal control function between different levels of government departments. Ultimately, producers may benefit from the increased transparency provided by written, published standards and rules for using experts.

Legislating against box-office fraud

The Film Law requires distributors and cinemas to record factually correct film sales revenue and provide truthful and accurate statistical data, forbidding them from fabricating false transactions. Failure to comply is subject to SAPPRFT levying new administrative penalties of confiscation of illegal gains and heavy fines of up to five times the amount of illegal gains.

The theatrical box office has greatly helped Chinese film industry by providing a needed source of revenue that is structurally less vulnerable to piracy. However, the centrality of the theatrical box office to the current Chinese

film industry has led to reported abuse on occasion. Further, foreign producers which distribute their films in China on revenue-sharing arrangements with Chinese companies have raised concerns before about falsified ticket sales figures.

Given the background of box office reporting concerns, both domestic and foreign companies are pleased with the Film Law's new rules requiring accurate reporting of box office revenue, and hope for steady and effective implementation of these rules.

Encouraging further development in the areas of finance, insurance and tax incentives

The Film Law expresses, in a number of places, how and in which direction the Chinese government would like to see the film industry develop further. The Film Law also suggests potential areas of development and possible incentives, including further development of regulations regarding film finance and insurance products to spread out risk in film production and distribution. The Film Law also addresses the central government's desire for local governments to provide film industry participants with access to resources, subsidies for making film accessible to rural audiences and the poor, and tax incentives.

Such provisions in the law suggest an overall favorable climate to the further promotion of the film industry, and new potential areas of opportunity within the industry.

More legislation expected

The Film Law took effect 1 March 2017. Following the law's entry into force, we expect further legislative activity, both to amend existing rules that now conflict with the Film Law and to elaborate some of the concepts that appear in the Film Law. For example, some of the areas slated for further development include:

- The specific standards applicable to film approvals
- The selection process for experts in final film approval, and the methods such experts should use for evaluating films
- Revision to the Sino-Foreign Co-Production Regulations
- Film industry-specific tax incentives, and
- Further rules on how government film authorities should enforce the Film Law and apply sanctions to violators.

Conclusion

Overall, as noted, initial reaction by industry experts, legislators and academics has been generally positive, understanding that certain changes will have to be made and further understanding that the Film Law will have to be implemented with more particularity, with much legislative activity expected to follow in relation to the Film Law for this reason.

If nothing else, the Film Law indicates China's intense focus on the continued development of the local film industry and local film demand. While the Film Law is not particularly oriented toward benefitting foreign players, there will be incidental benefits found in the general lift of the industry. Most notably, Sino-foreign co-produced films may see the most gains by being treated equally with domestic films in more respects.

Sheri Jeffrey
Partner, Los Angeles
T +1 310 785 4616
sheri.jeffrey@hoganlovells.com

Lu Zhou
Counsel, Beijing
T +86 10 6582 9578
lu.zhou@hoganlovells.com

Trending to the positive: New draft regulations for consumer protection in China

China's State Administration for Industry and Commerce (SAIC) recently released its draft Implementing Regulations on the Protection of the Rights and Interests of Consumers (Draft Regulations). The Draft Regulations seek to further strengthen consumer rights in China.

Proposed changes include setting mandatory returns and exchange arrangements, tackling aggressive selling behaviour, prohibiting cold calls, and imposing additional obligations and liabilities on e-commerce platform operators.

Who are consumers?

The Consumer Law provides that consumers who purchase or use goods or accept services are protected under the law. With the exception of consumers of financial products, the Draft Regulations specifically exclude from the scope of protection natural persons, legal entities and other organisations that purchase or use goods or accept services with the aim of making profits.

Defects and returns

The Draft Regulations introduce a suite of provisions governing defects in products and services and their quality, including those given to consumers as gifts or rewards. Where there are relevant national or industry standards, products/services will be deemed as defective if those standards are not met.

There are proposed detailed deadlines and requirements relating to returns, exchanges and repairs. For example, where goods are exchanged, the period for returns, exchanges and repairs is reset from the date the goods were exchanged.

In addition to the requirements under the Consumer Protection Law, business operators which are required to recall products must formulate recall plans, release recall information and keep records of the recall.

Where defects are found in "durable goods" and home decorations within six months of purchase, businesses are required to refund, exchange or repair the goods or show that the defects were not due to problems within the goods themselves. The Draft Regulations also expand the definition of "durable goods" and include specific consumer electronics such as phones, tablets and cameras.

Aggressive and misleading commercial behaviour

There is a new article prohibiting aggressive behaviour to force consumers to purchase or accept a service. Further, the Draft Regulations prohibit business operators from engaging in a list of types of misleading behaviour. These include selling goods which are counterfeits or past their expiry date, with incorrect information on place of origin, and using fictitious sales or reviews to falsely attract sales.

E-commerce platforms

The Draft Regulations introduce various requirements relating to e-commerce platforms:

- Platform providers must verify and register the identity of individual and legal entities selling products/services on its platforms, and display certain identification information
- Platform providers must use various technologies (e.g. electronic signatures) to ensure trade data are complete and accurate
- Platform providers must monitor and report illegal activities on the platforms. Failure to do so will attract fines of up to RMB 100,000 and correctional actions from the authorities
- Platform providers must establish a system of 'compensate-first' or consumer rights security deposits for compensating consumers using the platforms

– Where sellers infringe consumers' rights on the platforms and platform providers are unable to provide the real identity, address and contact of the sellers, platform providers shall become liable to the consumers directly.

Personal data of consumers

Companies must not collect or use unfair methods to collect personal data on consumers. Security systems must be established to ensure data collected are safe from leaks, damage etc.

The individuals concerned must have consented to the collection of the data. Business operators must keep for at least five years any supporting documentation showing performance of its obligations to inform and obtain the consent of consumers.

The definition of personal data is clarified and apart from the usual information such as name, sex, date of birth and ID number, it is expressly stated to include biometrics, health status and information on purchase.

Conclusion

The SAIC consultation period ended in September 2016. During the consultation period, Chinese media attention was centred on issues that have plagued Chinese consumers in recent years: leaking of personal data, loss of couriered packages and "professional" shoppers who purchase goods knowing they are counterfeits.

The Draft Regulations brings clarification to certain areas and provide greater protection to consumers, as well as new compliance requirements on businesses. Businesses should keep themselves apprised and review their business operations in China for compliance with the fast-developing consumer rights protection regime.

Philip Cheng
Partner, Shanghai
T +86 21 6122 3816
philip.cheng@hoganlovells.com

Access denied: ISP blocking injunctions in China and Hong Kong

Regulation for broadband internet service provider (ISP) blocking to combat trademark or copyright-infringing activities in China and Hong Kong is complex. This article focuses on whether ISP blocking remedies are available to trademark and copyright owners in China and Hong Kong.

China

Few IP actions are brought against ISPs in China compared with actions against (state-licensed) internet content providers. To date, no orders requiring ISPs to block websites in copyright or trademark infringement cases have come to light.

Despite the absence of any known ISP site-blocking orders, China's Tort Liability Law and the Regulations on the Protection of the Right of Dissemination via Information Networks may provide a route for rights holders.

Potential basis for ISP site-blocking orders in China

Article 36 of the Tort Liability Law sets out that:

- Internet users and internet service providers must assume tort liability if they utilize the internet to infringe upon the rights and interests of others
- If an internet user commits tortious acts through internet services, the infringed party is entitled to inform the internet service provider to take necessary measures, including, inter alia, deletion, blocking and unlinking. If the internet service provider fails to take necessary measures in a timely manner upon notification, it is jointly and severally liable with the internet user for the extended damage, and
- If an internet service provider is aware that an internet user is infringing on the rights and interests of others through its internet services and fails to take necessary measures, it is jointly and severally liable with the internet user for such infringement.

Accordingly, an ISP may be held jointly and severally liable with a third-party IP infringer if it knowingly facilitates an infringement without taking necessary measures to stop it. This would form, at a high level, a legal basis for attempting to obtain a site-blocking order.

What needs to be proven?

If an aggravated party decides to pursue a site-blocking order, it bears the burden of proving that the ISP has knowledge of the infringement, is capable of detecting it and is obliged to stop it if notified of its existence and that the balance of interests between the rights holder, internet users and the ISP merits the grant of a site-blocking order.

The ISP's knowledge of the copyright or trademark infringement can be proven through a takedown notice issued to it. In this regard, the rights holder should follow Article 14 of the Regulations on the Protection of the Right of Dissemination via Information Networks, which requires a sufficient takedown notice to identify the rights holder and the infringing work, and the provisions of preliminary evidentiary materials proving the existence of infringement.

Whether ISPs are obliged to detect or stop copyright or trademark infringement on the internet is an arguable issue. ISPs provide internet infrastructure or connection services and are often deemed not to be content providers. Under the regulations, internet content providers are obliged to respond to valid takedown notices pertaining to copyright infringement, whereas ISPs have no such obligation. It would be difficult for a Chinese court to ignore this distinction in the regulations and impose a similar obligation on an ISP.

If an ISP blocking case is brought under the Tort Liability Law, balancing the various parties' interests will be an extremely delicate matter, especially given that no court has ever granted a site-blocking order in the past. Further, an ISP could argue that a site-blocking order, if misused, could jeopardise the public's access to the internet; this too is likely to make the courts hesitant to grant an unprecedented site-blocking order.

Outlook

While in theory ISP site-blocking orders may be possible under Chinese law, the path will be challenging to pursue given the legal hurdles outlined above. Moreover, from a practical standpoint, the fact that all ISPs in China are controlled or backed by state-owned companies is likely to discourage Chinese courts from issuing ISP blocking orders against ISPs. Add to that the technical and commercial issues around limiting IP infringement on networks in China, which handle about 624 million internet users each day, and one can see why the courts may be reluctant to burden ISPs with the task of doing so.

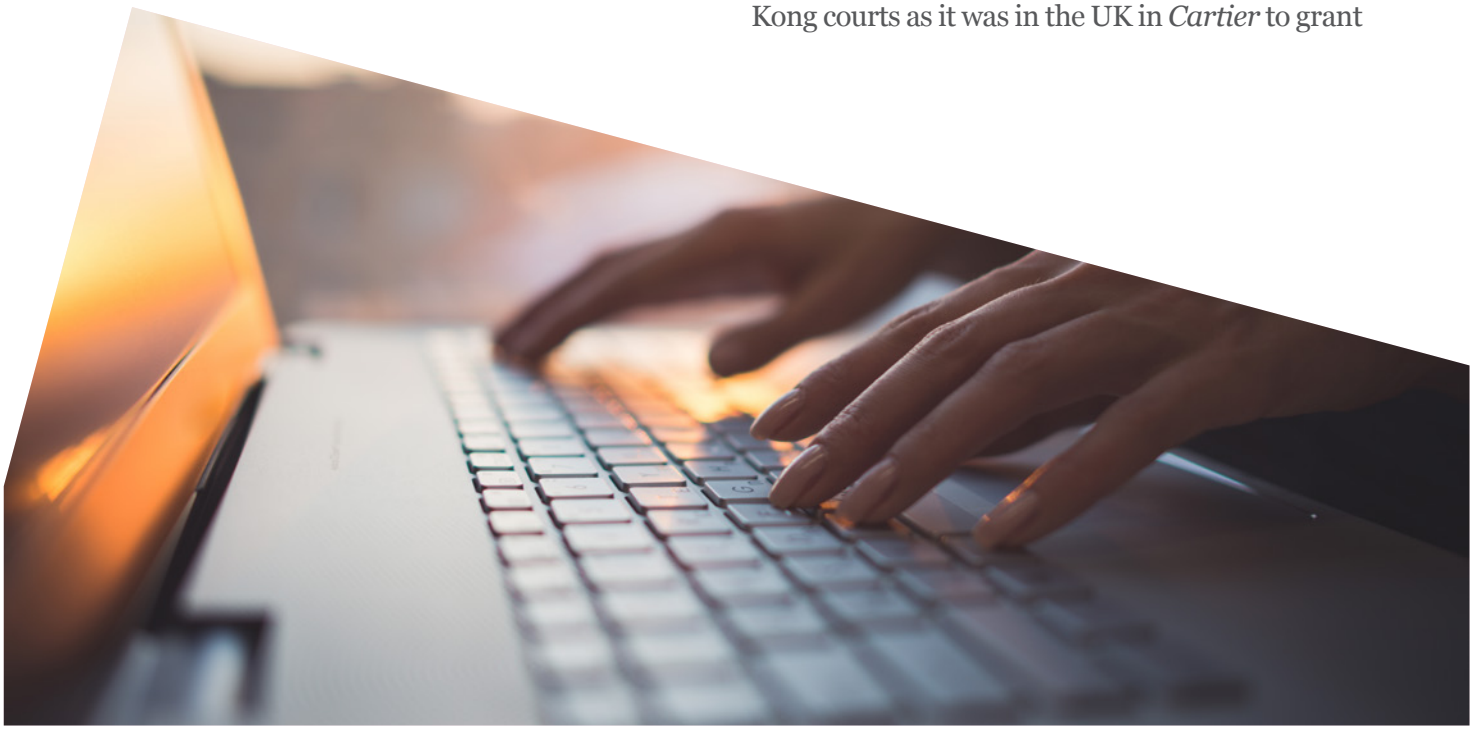
Hong Kong

To date, there have been no reported cases in which Hong Kong courts have ordered ISPs to block websites in trademark or copyright infringement cases, with IP actions against ISPs few and far between. Nevertheless, in the right circumstances, it would be open to a trademark or copyright owner to argue for such an order with at least a reasonable prospect of success.

Potential basis for ISP site-blocking orders

Despite the absence of cases in Hong Kong, it would appear that courts can in theory grant injunctions against ISPs, requiring them to block access to websites. Decisions issued by the UK courts are of persuasive value in Hong Kong and are frequently relied on when courts consider issues new to the jurisdiction. It is possible that Hong Kong courts will thus follow the approach in the *Cartier* case when it comes to issuing website-blocking injunctions.

First, Section 21L(1) of the High Court Ordinance gives the Hong Kong courts broad power to grant injunctions in "all cases in which it appears to the Court to be just or convenient." So, the same door is open for the Hong Kong courts as it was in the UK in *Cartier* to grant



blocking orders even where there is no specific legislation setting out a precise basis for them.

Second, courts in Hong Kong are not limited to making orders against wrongdoers. In one case, an ISP was ordered to disclose information about subscribers to its services – which were used for the illegal uploading and sharing of music files – under *Norwich Pharmacal* principles (which cover the duties of innocent parties who become mixed up in the wrongdoing of others). These principles were applied by analogy in *Cartier*.

Knowledge on the part of the ISP that its services are being used by others to infringe IP rights will likely be a prerequisite for a site-blocking order. This may be established, for example, by giving the ISP written notice. The requirements set out in *Cartier* for a site-blocking order are likely to be relevant for Hong Kong as well. In addition, it may be relevant to consider the proportion of infringing content on the website and how clear-cut the infringement is.

ISP liability for copyright or trademark infringement

It would appear that there is even more reason for Hong Kong courts to make site-blocking orders where ISPs themselves are found liable for copyright or trademark infringement.

For example, ISPs may incur civil liability for online piracy if they expressly or implicitly authorise another person to carry out an infringing act under the Copyright Ordinance or if they have deliberately collaborated with the infringer as part of a common design.

In the trademark context, Hong Kong courts may follow the same line as the European Court of Justice in *L'Oreal v eBay*, so that ISPs may be held liable for trademark infringement where they play an active role in promoting the infringing products, or where they were aware of the presence of infringing products on the website but failed to act promptly to remove the posts or to disable access.

Proposals

The Hong Kong government has acknowledged the adoption of judicial site blocking in other jurisdictions, but has no immediate plans to enact similar legislation, despite previously indicating that it would consider this issue in the next round of copyright review. As the passage of the copyright bill has been delayed several times, the issue of judicial site blocking is likely to be further put on hold.

In the meantime, there are options for rights holders. For instance, there are currently no such general safe harbours for ISPs in Hong Kong. Owing to this uncertainty, some ISPs respond positively (on a voluntary basis) to requests from rights holders to block access to infringing websites.

Katie Feng
Partner, Shanghai
T +86 21 6122 3826
zhen.feng@hoganlovells.com

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

Turning the clock back? Getting round the two-year time bar in a .cn domain name complaint

Unlike the Uniform Domain Name Dispute Resolution Policy (UDRP), the CNNIC ccTLD Dispute Resolution Policy (CNDRP) – the dispute resolution policy governing the ".cn" domain in China – sets a time bar which stipulates that no complaints concerning a ".cn" (or ". ") registration of over two years will be accepted. This time bar has in the past been criticised for imposing "unreasonable time limits" that would prevent the fair and equitable enforcement of intellectual property rights.

The history of this two-year time bar can be traced back to 2000 when CNNIC developed its very first set of domain name dispute resolution rules. It has been widely perceived as an absolute time bar which immunizes all ".cn" registrations of more than two years old from domain name complaints under CNDRP. In those situations the complainant would often have to resort to litigation or negotiations in order to recover the domain name.

However, in a case before the Hong Kong International Arbitration Centre (case number: DCN-1500641), the sole panelist considered that the transfer of a ".cn" domain name can amount to a new registration and thus re-set the two-year time bar. The domain name in question was first registered in 2006. The panel found in favour the complainant and ordered that the domain name be transferred to the complainant.

The complainant in this case, Leister Brands AG, was a Swiss company specializing in plastic welding, process heat and laser plastic welding technologies. The respondent was a Chinese individual by the name of "Chen Qiuheng." The disputed domain name <leister.net.cn> was first registered in 2006 by a Chinese company named Guangzhou Danlai Welding Machine Co., Ltd. (Guangzhou Danlai).

The complainant's case was that since registration the domain name had been used to mislead customers that Guangzhou Danlai was affiliated with the complainant. The complainant first commenced court proceedings in China against Guangdong Danlai in June 2015. In the course of the court proceedings, the complainant found out that the domain name was transferred to the respondent in this case in around mid-2016. The complainant contended that the respondent is closely related to Guangdong Danlai and the transfer should be regarded as a new registration in bad faith.

The panel of arbitrators made a preliminary ruling that the two-year time limit did not bar the filing of the complaint. The panel decided that the transfer of the disputed domain name did amount to a new registration, for the following reasons:

- Among the four circumstances of bad-faith registration or use of a domain name under Article 9 of CNDRP, the first and the third circumstance both include the reference to "acquiring" a domain name. Hence, the intention is that CNDRP should apply as long as the respondent was acting in bad faith, regardless of whether the respondent obtained the domain name by registration or by transfer
- The panel applied the consensus view of panelists of the World Intellectual Property [ ], which states that "transfer of a domain name to a third party does amount to a new registration. Registration in bad faith must occur at the time the current registrant took possession of the domain name"
- If the two-year time limit is considered an absolute bar, this would encourage illegitimate domain name registrations, and
- There would be no injustice to the respondent because the complainant would still have to prove its case on merits under the 3 elements of CNDRP (similar to UDRP) in order to succeed. Furthermore, the interpretation of the two-year time limit would not deprive either party from its rights to appeal the CNDRP decision to a competent court.

After making this preliminary ruling, the panel of arbitrators went on to discuss the substantive merits of the complaint and found in favour of the Complainant.

Conclusion

This is an interesting decision and offers a silver lining to trade mark owners who thought they might have been barred from submitting a domain name complaint under CNDRP when trying to recover a ".cn" domain name of more than two-years. We consider this decision to be a liberal reading of the two-year time bar under CNDRP and one which is commendable in following the spirit of UDRP. However, as mentioned, this two-year time bar has a very long history in CNDRP so we would suggest that this decision be read on its specific facts. It remains to be seen whether this decision would be followed in future CNDRP decisions and whether CNNIC will clarify the meaning of the two-year time bar.

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

Yvonne Fu
Paralegal, Beijing
T +86 10 6582 9410
yvonne.fu@hoganlovells.com

Protection of minors in cyberspace is on the agenda in China

On 30 September 2016, the Cyberspace Administration of China (CAC) issued a draft for comments of the Regulations on Cyberspace Protection of Minors (Draft). If the Draft becomes final in its current form, it may impose significant regulatory requirements upon "internet information service providers" that is, the organizations and individuals that provide information technology, information services, or information products via the internet, including providers of internet platform services and the providers of internet content and products.

Who is a minor?

"Minor" is not defined in the Draft, but the term is defined under the Minor Protection Law as any citizen under the age of 18. The term "citizen" is likely to be interpreted as a citizen of China. The non-binding (but perhaps persuasive) Guidelines for Personal Information Protection within Information Systems for Public and Commercial Services on Information Security Technology (Guidelines) define minority using a lower age of under 16. However, out of prudence, and due to the fact that the Minor Protection Law's definition would in all likelihood prevail over that in the Guidelines under Chinese rules of legislative hierarchy, we would recommend that it is best to proceed with under the age of 18 as the applicable definition.

Warning of potentially harmful information

Any organization or individual that produces, publishes, or disseminates the following information unsuitable to minors in cyberspace is required to provide apparent warnings prior to such production, publishing, or dissemination:

- Information that may induce minors to undertake acts of misconduct such as violence, bullying, suicide, self-harm, sexual contact, vagrancy, begging, etc.
- Information that may induce minors to consume substances not suitable for their consumption, such as tobacco and alcohol
- Information that may induce minors to be wary of studying, to be cynical, or to feel self-inferiority, fear, or depression
- Other information that may negatively impact the physical or mental health of minors.

Internet information service providers that provide internet platform services have an obligation to review the information on their platforms. When the above categories of information are identified, measures must be taken to warn viewers prior to browsing. In addition, if an internet information service provider that provides internet platform services finds any information on its platform that is in breach of laws, regulations, and departmental rules, it should take measures to filter, delete, or block such information, and report the breach to the relevant government authority in charge of such matters.

Filter software

The Draft encourages the R&D, manufacturing and promotion of minor cyberspace protection software. Where internet access is provided in schools, libraries, cultural centers, and youth clubs, installation of such software is required. All network end products that may connect into the internet, have operational systems, and allow users to autonomously install applications by themselves – what the Draft calls "intelligent terminal products" (ITP), which to our understanding is roughly the equivalent of "smart devices," – should either install such software prior to being sold to end users (domestic ITP manufacturers pre-install it, and importers of ITPs install it before distributing in China), or they should facilitate the installation of minor protection software, and inform users about installation channels and methods in a conspicuous manner. Those who fail to install such software and also fail to facilitate installation and inform users in a remarkable manner may be fined between RMB 100,000 and 500,000.

The Draft does not address a key question raised by these provisions: whether the filter software must be designated by the Chinese government, or whether it can be developed or selected freely by hardware developers/distributors. Based on existing laws, regulations, and departmental rules, most information that may potentially harm minors is already required to be filtered out, such as contents containing pornography, gambling, and anti-government materials. As a result, the goals of these provisions may seem somewhat confusing to some stakeholders, including a large number smart device manufacturers and software developers in China.

In 2009, the Chinese government attempted to install Green Dam filter software to all new computers for minor protection. Green Dam became very controversial because its functions were not well defined, and because it could be used for censoring purposes. Later the mandatory requirement to install Green Dam was abandoned by the Chinese government. However, it must be pointed out that it was in the revisions of the Minor Protection Law that a related stipulation was introduced, namely: "The State encourages research and development of internet products that are conducive to the healthy growth of minors and promotes the use of new technologies for preventing minors from internet addiction." Though Green Dam was halted, this provision was added to the Minor Protection Law in 2006 (effective since 2007) and remains to this day. At the very least, tech companies dedicated to selling ITPs in China, domestic or foreign-invested alike, may opt to only facilitate and provide notices and instructions for installation rather than to preload ITP products with filter software themselves, which is sufficient for them to satisfy their obligations. However, what is deemed as "facilitate the installation of minor protection software," or "inform users about installation channels and methods in a conspicuous manner" is still open for interpretation.

Personal information protection

In terms of the protection of minors' personal information, the Draft requires those who collect and use minors' personal information to provide apparent warning notices, provide source, content, and usage of the information, and obtain consent from minors or their guardians. A specific set of collection and usage rules must be designed by internet information service providers to enhance the protection of minors in cyberspace. Internet information service providers which provide

search services must not violate this requirement and display search results containing personal information of minors. If a minor or his or her guardian demands that the internet information service provider delete or block any personal information in cyber space, the internet information service provider must take necessary measures to delete or block as requested.

Minors' personal information is defined under the Draft as each kind of information electronically or otherwise recorded which can be used alone or combined with other information to identify the identities of minors, including minors' name, location, address, date of birth, contact information, account name, identification card number, personal biological identification information, and portraits, etc. This open-ended definition does not differ significantly from the general definition of personal information under other Chinese laws, regulations, and guidelines, though the general definition also includes the following: password, status of income and assets, health status, consumption status, ethnicity, political opinions, religious beliefs, or any information that may reveal not only the location but also the time of data subjects.

Online gaming

Online game providers are required to register players' true identity, and identify those who are minors. They must also establish and improve game rules that prevent minors from being addicted to games, and must alter the technology if it may induce addictions. Between midnight to 8:00 am each day, online game providers must prohibit minors from playing. They must also limit the total and daily game time of minors.

Here it may be hard to define what can or cannot "indulge in network addictions." Similarly, potentially harmful information also lacks a standard. However, it is worth noting that this is not the first time this type of language appears. In the Minor Protection Law, Articles 19 and 33 have already required parents (guardians) and the State, respectively, to be responsible for taking measures to stop minors from "indulging in network addictions." The Advertising Law also prohibits advertisements on mass media about online games which are harmful to minors. What the Draft is trying to accomplish now may be considered trying to materializing the more abstract stipulations in the Minor Protection Law. The Draft sets out the following liabilities: if an online gaming operator fails to register a minor's identity or to take measures against addiction, it may first receive a warning to rectify within a period of time; if it still fails to rectify, it will face a fine between RMB50,000 and 500,000 potentially combined with suspension or termination of the online gaming services. Under severe circumstances, its license to operate in online gaming, the Online Cultural Operational License, may be suspended. The interpretation of these terms may need further clarification from the CAC (it may also come jointly from the Ministry of Industry and Information Technology), or better illustration from specific cases, after the final Draft's issuance.

The Draft's solicitation of opinions ended in October 2016. It is unknown when the Draft will be passed into law.

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

Jessie Xie
Senior Associate, Beijing
T +86 10 6582 9488
jessie.xie@hoganlovells.com

No child's play – protecting children's privacy in Hong Kong

Recent developments on children's online privacy in Hong Kong include the Privacy Commissioner for Personal Data (PCPD)'s; responses to data breach incidents involving minors' personal data, study on privacy practices of children websites and mobile apps, and newly published guidelines.

Data breach incidents

Back in December 2015, the PCPD commenced investigations into two data breach incidents involving minors' personal data. One case involved an international toymaker whose customer accounts were suspected to be hacked. The company notified the PCPD of the incident. According to the company's announcement, the incident involved leakage of data of over five million adult customers and six million children.

In the other case, the PCPD initiated an investigation into the suspected security vulnerability of a website targeting children users. The investigation follows the company's announcement that up to 3.3 million members' personal data could have been publicly accessible, including their name, email address, date of birth and password. According to the PCPD, the incident involved a large number of persons and might include children's personal data. The PCPD also commented that the potential harm to individuals as a result of the data breach would be more serious if children's personal data were involved.

In both investigations, the PCPD's key consideration was whether there had been a breach of Data Protection Principle 4 (Data Security Principle) of the Personal Data (Privacy) Ordinance (PDPO), which requires that data users must take reasonably practicable steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use.

Under the PDPO, there is no mandatory requirement to make a notification of a data breach incident. However, the PCPD issued a guideline encouraging data users to make a data breach notification.

2015 study report: online collection of children's personal data

In December 2015, the PCPD released a Study Report on Online Collection of Children's Personal Data (Study). This was part of the Global Privacy Enforcement Network Sweep exercise in which the PCPD collaborated with privacy enforcement authorities worldwide to examine the privacy practices of 45 local websites and mobile applications targeting children.

The Study found that most websites and mobile applications' privacy practices were not satisfactory, in particular:

- 36% asked for children's Hong Kong Identity Card numbers
- 49% indicated they may share collected children's personal data with third parties
- 73% asked for the children's phone numbers
- 60% asked for their home addresses
- 36% asked for information about third parties (such as the children's family and friends), and
- only 4% provided accessible means for a child to delete the account.

The Study showed that many websites and mobile applications seem to be collecting personal data from children without adequate protective measures limiting their use or disclosure, or providing accessible means to erase collected data. As a result, the PCPD issued new guidelines to urge website owners and mobile application developers to improve their privacy practices.

Practical guides to strengthen children's privacy protection

The PCPD has released two publications on the topic of children's online privacy: Collection and Use of Personal Data through the Internet – Points to Note for Data Users Targeting at Children; and Children Online Privacy – Practical Tips for Parents and Teachers. The first publication gives data users (such as website owners and mobile application developers) guidance on the use and handling of children's personal data; the second aims to increase parents' and teachers' awareness of privacy issues when supervising children's use of websites and mobile applications. Of critical importance, the PCPD recommends that data users should:

- **Avoid collection of children's personal data**. The best practice is not to collect any personal data from children at all (not just limiting personal data collection) as children may not fully understand all the privacy risks, particularly for sensitive personal data such as biometric data
- **Avoid open questions**. Ask closed (for example, yes-no questions) instead of open-type questions as those may lead children to over-supply information
- **Enable erasure**. Data users should offer easy means for children to remove their accounts, associated personal data and any contents they may have posted online
- **Obtain consent**. Before using or changing the use of collected personal data, data users should obtain consent from children. Particularly for young children, data users should ask them to consult their parents or adults before consenting or giving information about others
- **Safeguard personal data**. For example by encryption
- **Use appropriate language**. Privacy policies should be accessible to both children and their parents The language and presentation should be easy to understand, user-friendly and age-specific.

The PCPD further recommends that parents/ teachers should:

- **Actively participate**. Engage with children in their online activities, experiment and understand how those online platforms operate, explore available parental controls and privacy settings
- **Self-help/protect**. Safeguard computers, mobile devices as well as account information and passwords. Understand essential security measures and beware of digital footprints or disclosure of 'indirect' personal data such as photos, location trails and stored data on devices
- **Be good role models**. Adopt good privacy practices, teach children to respect others' personal data privacy and have frequent, frank discussions with children about their online practices.

Both data users and children's supervisors (parents, guardians and teachers) are responsible for ensuring adequate protection of children's privacy. The recent investigations show that PCPD takes privacy issues seriously, particularly those relating to children. It is important for data users, website/ mobile application developers, parents and teachers to stay informed and alert, consider the recommendations above and implement good privacy practices.

PJ Kaur
Associate, Hong Kong
T +852 2840 5634
pj.kaur@hoganlovells.com

China data privacy policy case: implications for "browse wrap" and implied consent

On 12 October 2016, West Lake District People's Court in Hangzhou issued its judgment on the enforceability of a data privacy policy forming part of Alibaba's Taobao user agreement.

Although the court issuing the judgment is relatively low in China's overall judicial hierarchy, the scarcity of cases in China addressing data privacy policies makes this judgment (in particular, what can be read between lines) well worth noting. As such, the decision can be seen as an implicit endorsement of the "browse wrap" approach to implied consent to contract terms and privacy policies that is widely used in the online and mobile contexts in China and elsewhere in the world.

Background

The plaintiff, Zhou Wangchun – a user of Alibaba's Taobao e-commerce app – filed a lawsuit against Alibaba in October 2015, alleging that the data privacy policy forming part of Alibaba's Taobao Cellphone Software Licensing Agreement (User Agreement) infringed users' privacy and impaired social and public interests. The court ruled in favour of Alibaba and rejected the plaintiff's claims.

Issue 1 – validity of user data licence

The first claim addressed by the Hangzhou court was whether Article 7(1) of the User Agreement was valid. That clause obliges the users to grant Alibaba and its affiliates an exclusive, worldwide, irrevocable, royalty-free license to use all materials and data provided by the user when using Taobao. Mr. Zhou claimed that this standard form clause infringed upon his rights to freedom of communication, to personality, and to privacy. Mr. Zhou further claimed that this clause harmed social and public interests by authorizing Alibaba to publish the data of over 200 million Chinese users on a worldwide basis. By way of background, under the Contract Law, a standard form clause can be invalidated if it exempts the party providing the standard clause from liability, or increases the liabilities or deprives the principal rights of the other party (although the Contract Law and certain Supreme People's Court interpretations outline ways to make such clauses fair and enforceable).

In its defence, Alibaba argued that Article 7(1) should be read together with the other provisions in the User Agreement, in particular Articles 6(2) and 6(3) which require Alibaba to keep users' private personal data confidential and not disclose it without notifying the users. Further, Alibaba argued that the use of standard form agreements is an accepted industry practice for online and mobile services. In the User Agreement "private personal data" is broadly defined as data which can be used to identify a specific user or data related to a user's contact details, such as ID number, cellphone number, IP address and UDID.

In its judgment, the Hangzhou court held Article 7(1) to be valid. The court agreed with Alibaba that, when Article 7(1) was read in conjunction with Articles 6(2) and 6(3), the scope of data that Alibaba was licensed to use under Article 7(1) did not include "private personal data" and as such, there was no infringement upon Mr. Zhou's right to freedom of communication, his rights of personality or his right to privacy. Further, the court rejected Mr. Zhou's request to invalidate Article 7(1) under the standard form clause plea as it did not exempt the party providing the standard clause from liability; did not increase the liabilities of the other party, or did not deprive the other party of its principal rights.

Issue 2 – perpetual data retention

The plaintiff's second and the third claims were interwoven. The second claim questioned the validity of Article 6(5) of the User Agreement, which confers on Alibaba the right to keep user data indefinitely

following termination. The third claim was that the User Agreement was deficient in not granting Mr. Zhou the right to have data generated during his usage of the app erased. By way of background, under Article 54 of the Contract Law, an agreement may be invalidated by the court under certain circumstances (namely, if the contract was entered into as the result of a major mistake, or was manifestly unconscionable at the time it was entered into, or was entered into contrary to a party's true intentions through fraud, coercion or taking advantage of the party's vulnerability). In its defence, Alibaba argued that this clause was not in breach of Article 54 of the Contract Law and should not be invalidated, and that Alibaba has no obligation to delete Mr. Zhou's data.

In its judgment, the court held that Mr. Zhou had not brought a claim under Article 54 of the Contract Law. The court further held that there was no legal basis to support Mr. Zhou's request to have Alibaba delete the data generated during Mr. Zhou's usage of the app, as the retention of Mr. Zhou's data was not in violation of any laws or regulations, nor did it violate the parties' agreed method of collection and use of such data. It is interesting to note that the court did not take into account the non-binding standard in this area, the 2013 China Standardization Administration's Guidelines of Personal Information Protection within Information System for Public and Commercial Services on Information Security Technology (Guidelines). The Guidelines specifically state that personal information should be immediately deleted where the data subject has legitimate reasons to request that his or her personal information be deleted. This tends to show that the court did not find persuasive value in the Guidelines.

Reading between the lines – "browse wrap" and implicit consent

The ruling in this case is significant not just for the issues expressly considered in the court's reasoning, but also for the court's apparent endorsement of practices which are typical in the industry for achieving consumer acceptance of terms and conditions and taking data protection consent in the online and mobile contexts.

It appears from the judgment that the User Agreement did not require Mr. Zhou's explicit consent for the collection and use of his data, for example by presenting an empty tick-box by which he could explicitly acknowledge his agreement to the User Agreement at the time of downloading the app. Further, the User Agreement provides that once a user downloads and uses the software, the user is deemed to have accepted the terms and conditions of the User Agreement, including the privacy policy. The approach of deemed acceptance of terms by virtue of use is known as "browse wrap." The usage of "browse wrap" is widespread. Internet companies are generally reluctant to implement more rigorous contract formation procedures on the basis that members of the cyber space community lack any ability to interact and negotiate contractual terms with each other; hence more formal procedures would impede internet-user activity, disrupt the user experience and deter consumers from using the service.

The Hangzhou court did not raise any question or make any comment on this "browse wrap" approach to obtain users' consent. Reading between the lines then, the court appears to be acknowledging that the "browse wrap" approach to consumer acceptance of standard-form agreements is valid under Chinese law. It also shows that the court is in sync with China's agenda to develop a mature e-commerce environment.

Implications for businesses

The importance of online and mobile marketing and sales cannot be underestimated in the Chinese context, where e-commerce volumes now reportedly exceed RMB1tn every quarter.

Securing binding and enforceable terms and conditions is important from a risk management perspective, and in the "Big Data" era, information about consumers is an increasingly valuable asset and so data privacy policies must work.

The Hangzhou court's judgment is a helpful step forward in clarifying these issues.

Maggie Shen
Senior Associate, Shanghai
T +86 21 6122 3883
maggie.shen@hoganlovells.com

Briana Liu
Junior Associate, Beijing
T +86 10 6582 9559
briana.liu@hoganlovells.com

Hong Kong Consumer Council report: trends and pitfalls in online retailing

In November 2016, the Hong Kong Consumer Council published an in-depth study into online retail in Hong Kong, with a particular focus on the airlines & travel, food & beverage, clothing & beauty and computer & electronic products sectors. Although the Consumer Council is a private, not a public body, its study identifies a number of pitfalls in the commercial and legal environment in which online retail is conducted, and makes some important recommendations to the government to review the legal framework.

The study highlights the importance for online businesses to familiarise themselves with the interplay between the various laws applicable to various aspects of online retailing, including in particular data privacy, trade descriptions, online contracting, competition, and consumer rights in general.

Online shopping in Hong Kong

The study finds that the percentage of consumers who shop online in Hong Kong lags behind those in other countries. The figure was at only 23% in 2014, compared to around 70% for Mainland China, Japan, Europe and the US. However, the study recognises that online shopping in Hong Kong will continue to increase with globalisation.

When asked, consumers cited numerous concerns about the online environment as reasons for not shopping online in Hong Kong. For example, consumers complained about duplicate bookings due to the complexity of using online booking systems in the airlines sector. Another common complaint was that consumers were unable to redeem vouchers purchased on group buying sites.

More generally, the study highlights a number of pitfalls in online retailing. We elaborate on these below.

Privacy risk

There has been an upward trend in information and communications technology related complaints to the Privacy Commissioner. Consistent with this trend, the study flags that:

- Online businesses may be failing to observe the six data protection principles in the Personal Data (Privacy) Ordinance (PDPO) and are possibly, among other things, collecting excessive personal data and using personal data for direct marketing without consent
- When delivery is outsourced, not all platform operators restrict delivery agents by a confidentiality undertaking on handling customer data
- Digital security is identified as a particular concern for online platforms or shops, given the large amount of personal data collected and the multiple databases used to hold personal data. Online platforms may be an easy target of malware, hacking and phishing attacks.

Unfair trade practices

The study highlights that online shoppers are particularly vulnerable to misleading and deceptive practices as they may not be able to examine goods and have few avenues to seek clarifications.

Online shoppers are also more likely to be influenced by misleading or "paid" product reviews and discover unexpected surcharges towards the end of a transaction.

Allocation of responsibilities

The study also suggests that the matrix of commercial relationships in online retailing adds a further layer of complexity to the commercial and legal environment for online retail. Very often, one or more of the following parties may be involved: the customer, the supplier of the goods or services, search engines directing consumers to the online shop or platform, the platform for its

marketing service, payment gateways, bank and credit card companies for payment settlement and delivery companies.

Licensing concerns

The study reveals that ordering food & beverage online has become increasingly popular.

Licensing is a particular concern for the food & beverage sector, which is highly regulated with different licensing arrangements for food manufacture, importation, distribution and retailing to protect public health.

Competition concerns

In Hong Kong, the Second Conduct Rule of the Competition Ordinance prohibits a business with a substantial degree of market power from abusing that power. The study considers that online platforms derive significant market power from their large scale operations and the information they possess.

With such power comes the possibility of abuse. For example, in the airline and hotels sector, the study flags that online travel agencies with a large share of the travel booking market may be restricting the ability of smaller hotels to market rooms at lower prices by requiring the hotels to give them the best available rate.

Recommendations to the Hong Kong government

In view of the problems associated with online retail, the study recommends the government to consider adopting measures for the further regulation of online retail, including:

- **Legislate for consumers' right to withdraw**. In some jurisdictions (e.g. EU, UK and China), consumers can withdraw from online transactions within a specified period without a reason depending on the condition of the goods. Certain exclusions apply, such as for perishable and time-limited goods.
- **Legislate for a mandatory information provision**. This would cover all essential information, including the total price of the goods or services (inclusive of delivery charges, taxes and any other costs), the full identity and contact details of the trader, the duration of the contract, details about the right to withdraw, and the complaints handling policy.
- **Legislate to clarify consumer rights and remedies for digital content**. Presently, it is unclear whether digital content (e.g. software, music and video) is classified as a "good" or a "service" and accordingly whether the Sale of Goods Ordinance or the Supply of Services (Implied Terms) Ordinance are applicable to contracts for supply of digital content. Doubts therefore arise as to whether the rights and remedies under such ordinances are available to consumers of digital content. The UK has passed legislation to address this issue.
- **Monitor how online platforms exercise their market power**. The study flags that the business practices of large Internet platforms have raised the attention of antitrust authorities overseas, and their influence on competition in Hong Kong should be monitored.
- **Understand big data implications and how big data is being used**. This is particularly relevant for large platforms that collect a large amount of customer and transaction information, and have the ability to leverage such information for customer profile analysis.
- **Establish an online dispute resolution (ODR) mechanism**. As it may not be practical to bring legal action for online claims, an ODR mechanism can help consumers identify the party answerable and facilitate out-of-court settlement in a cost-effective manner. The EU has established a common ODR platform for EU members.

Best practices for online businesses

We set out below some of the best practices to help businesses avoid the pitfalls of operating in an online environment:

- **Provide full information relating to the transaction**. To enhance transparency and avoid subsequent disputes, online businesses should set out all relevant information, including about the product, price, delivery terms and the trader in a clear and conspicuous manner.
- **Maintain clear online business policies**. These include a privacy statement, personal information collection statement, user-friendly terms and conditions of sale and purchase (as well as a summary if helpful), return and refund policy and performance pledges.
- **Maintain a "goodwill" return and refunds policy**. This will instil confidence in consumers and encourage online shopping.
- **Display final prices and provide a summary review before concluding the transaction**. The prices displayed should be inclusive of delivery charges, taxes and other costs. This will reduce the number of cancellation requests and subsequent complaints from customers.
- **Handle data securely and comply with the PDPO.**
- **Steer clear of unfair trade practices**. In the online retail space, especially watch out for pricing claims/comparisons, product/photo discrepancies, bait advertising, false/misleading endorsements, etc.
- **Ensure compliance with all relevant safety and food regulations**. Any mandatory licenses should be displayed online.
- **Provide a customer support and complaints channel for online consumers**. This allows consumers to seek clarifications before making a decision to enter into a transaction, and allow timely settlement of disputes.
- **Retailer to retain overall responsibility**. The study recommends that overall responsibility for any problems should remain with the retailer.

Conclusion

Concerns about the online environment in Hong Kong are not surprising as consumer protection laws were designed for brick and mortar operations. There is also the added complexity of commercial relationships online which makes the scope for confusion, miscommunication, errors and delay potentially greater. It is of paramount importance for businesses operating online to be wary of the pitfalls in online retailing and the potential "hot spots" of customer complaints, and implement best practices to stay out of trouble.

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

PJ Kaur
Associate, Hong Kong
T +852 2840 5634
pj.kaur@hoganlovells.com

China's proposed cyber security review of network products and services leaves concerns of multinationals unanswered

On 4 February 2017, the Cyberspace Administration of China (CAC) issued a draft of the Network Products and Services Security Review Measures (Draft Measures) for public comment. The Draft Measures bring China one step closer to implementing a security review regime with respect to network products and services (and their providers), a process first set in motion by the Cyber Security Law.

How this regime will look has been one of several major areas of concern for foreign investors arising out of the implementation of the Cyber Security Law in China. Given the recent direction China has taken in this regard, and a previous campaign to introduce the "secure and controllable" (or "secure and reliable") concept in the banking, securities and insurance sectors, there were legitimate concerns that a new program of security review might be skewed in favour of "local" manufacturers and thus become a back door means of imposing essentially protectionist policies. In the case of the previous "secure and controllable" campaign, in some sectors, even though the campaign was eventually suspended, some such protectionist effects were felt, as it seemed that some businesses in China may have taken the view in light of impending requirements that buying local products was a better, lower risk purchasing strategy than buying products manufactured overseas or by foreign-invested enterprises (FIEs) in China, so these concerns are quite real.

The background to the Draft Measures is that the Cyber Security Law requires that network products and services purchased by operators of "critical information infrastructure" (the definition of which is somewhat vague and unsatisfactory) (CIOs) must undergo national security review (Security Review) if such network products and services "might potentially have an impact on national security." If the CIO fails to undergo the security review it risks being ordered to discontinue use and/or being subject to quite stiff fines (up to ten times the purchase price) and, in a formulation reminiscent of the Criminal Law, the persons directly in charge and other directly responsible persons will be liable to pay personal fines between RMB 10,000 and 100,000.

Thus, since the promulgation of the Cyber Security Law (which has yet to come into force), it has been known that a Security Review regime would be introduced for certain network products and services, potentially impacting both the businesses which are manufacturers of such products and providers of such services as well as the users (or prospective users) of those products and services.

The Draft Measures aim to give shape to such Security Review, but as drafted leave a number of critical questions unanswered.

Do the draft measures answer all the questions?

The Draft Measures fill in some of the details of the Security Review process, primarily by setting forth the broad content areas to be covered and by establishing its bureaucratic framework. However, the Draft Measures do little to settle some of the key areas of uncertainty that have arisen around the Security Review process, including:

- More precision around which products and services might be viewed as having an impact on national security and therefore potentially subject to Security Review
- More precision around which companies are considered to be CIOs and therefore potentially limited in their procurement options, and
- Whether there will be a protectionist slant in the Security Reviews, such that their practical implementation will make it difficult for foreign or FIE manufacturers to compete.

wPerhaps the biggest concern is that, even if passed in their current form, the Draft Measures also do not set out the specific standards and procedures applicable to the Security Review. On an optimistic view, the Draft Measures should only be an intermediate step closer to the launch of the Security Review regime, not the final step, and more legislation (perhaps in the form of further CAC implementing rules) should follow, bringing clarity. A more cynical view is that certain obvious gaps will persist in any event, and in practice will simply be filled in by opaque, subjective interpretation.

The Draft Measures also introduce some new potential areas of "scope creep" for rules that on their face are meant to be directed at cyber security concerns. For example (and as explained in more detail below), Security Reviews are to include an assessment of the risk that users could become so reliant on a technology that it gives rise to unfair competition, which is not a risk that would ordinarily be seen as part of a technology risk management exercise (and is a concern already addressed under other Chinese laws).

Scope of application

Article 2 of the Draft Measures provides that "important network products and services used by information systems which concern national security and the public interest are subject to network security review." Article 2 thus sets out an opaque and potentially broad scope of application for Security Review. However, it is the restrictions on procurement set out in the Draft Measures which really illustrate the "consequences" for failing to achieve certification:

- Party and government authorities and key industries must purchase network products and services which have passed Security Review on a priority basis, while refraining from purchasing any network products and services which have failed to pass Security Review
- CIOs may only purchase network products and services which have passed network Security Review if such network products and services may have an impact on national security (as determined by the government departments in charge of protecting the security of critical information infrastructure).

The second bullet point above is consistent with the text of the Cyber Security Law but, like the Cyber Security Law, carries with it some uncertainty as to the scope of its application, as "critical information infrastructure" has yet to be fully defined. The first bullet point above, by contrast, goes even further than the requirements under the Cyber Security Law and introduces further uncertainty, as the term "key industries" is not exhaustively defined but clearly allows the scope for sectors forced to buy only certified products and services to be expanded, based on subjective interpretation of what is a "key sector" going beyond those listed.

The foregoing provisions on procurement might suggest limited impact for product and service providers whose target markets do not include party and government authorities, key industries, and CIOs in segments touching upon national security. Absent any amendment or clarification to the Draft Measures, however, we do not expect a limited impact, given that "key industries" and "operators of critical information infrastructure" may be interpreted to apply to a broad swath of companies, and given the likelihood that some companies, for example state-owned enterprises outside these defined categories, may also voluntarily chose to (or come under pressure to) give priority to purchasing products that have passed the Security Review and are readily available on commercial terms. The teeth in the imposition of the "secure and controllable" policy in the banking sector was not so much the threat of punishment for violating the legislation, but more in the commercial pressure brought to bear in the tendering and procurement of equipment processes by state-owned banks, where in practice any bidder that failed to meet the given "secure and controllable" criteria

would essentially find its bid marked down to the point where the bid was virtually or literally disqualified.

What does the Security Review involve?

The Draft Measures implicitly require that network products and services be "secure" and "controllable", and in this regard require the assessment of the following potential risks:

- The risk that such products or services might be subject to unlawful control, interference or operational shutdowns
- Risks occurring during the course of research, development, delivery and technical support in relation to the products and key components thereof
- The risk that the product or service provider might be able to use the provision of such product or service as a means to unlawfully collect, store, process or use related user information
- The risk that the product or service provider might be able to take advantage of users' reliance on such product or service to engage in unfair competition or activities detrimental to user interests, and
- Other risks which may jeopardize national security or harm the public interest.

The first bullet point seems to be taking aim at whether the products are at risk of being hacked, infected by viruses, and/or controlled or turned off remotely.

The second bullet point is more oblique and likely contemplates a number of risks. Risks concerning the development of the products and its components points could include software "back doors," "logic bombs" and other code that would have been deliberately installed as part of the development with a view to allowing data extraction or remote operation. It could also involve

an assessment of how secure the course of development of the technology was and, for example, assessing the risk that knowledge of the security features of the technology such as encryption/decryption keys has "leaked" or has otherwise become known outside the developer's organization, or that software or firmware, whether open source or sourced from a third party, has not been properly screened prior to its use in the product. Risks concerning technical support of a product could point to the product's reliance on remote support, whether within or outside of China, or to the customer's access to source code, and so may be a further point of concern about the Security Review for foreign technology providers in particular.

The third bullet point takes aim at data protection concerns around user information, in particular the risk that products collect and process information without the user's knowledge. Unlike in the first bullet point, the focus here is on misconduct by product and service providers and not third parties that may hack into the product.

The fourth bullet point seems to be something of a mixed concept, whereby it hints at issues like abuse of a dominant market position with the words "might be able to take advantage of users reliance on such product or service to engage in unfair competition" but also brings up more generalized and vague notions of the provider or manufacturer engaging in behavior prejudicial to users which points to consumer protection-type laws. The risk highlighted here is not one which would ordinarily be seen as a direct concern from a network security perspective.

What is interesting or you could say unfortunate about this is how China appears to have conflated what some might argue are non-national security-related issues like data protection and acts of unfair competition in what is supposed to be a national security test. These areas are already extensively addressed in other parts of Chinese law, so it is difficult to see why they should form part of a national security test.

The unfair competition/prejudicial conduct to users part is not just vague, it is also largely subjective and could be used to fail a product manufactured overseas or by an FIE for the wrong reasons: any service or product provider regardless of origin has the potential for abusing its position as vendor or supplier in a manner that goes against the interests of the consumer, depending on how you define "abuse," so the question becomes how do you make an objective, non-political decision whether or not to pass based on the potential for abuse?

As for the sweep up at the end: as drafted, this is basically a purely subjective test of anything else that may have been omitted from the legislation or which may be determined as harming the public interest as determined by the CAC or the institutions or experts making the determination. It is so broad as to make the other criteria basically redundant, as virtually anything could be fitted within this category.

Security review process framework

The Draft Measures set out a multi-layered, multi-institutional approach to Security Review, which we have illustrated in chart form in the Appendix.

The top layer is the CAC, which will promulgate the legislation in its final form and will be responsible for its interpretation.

The next layer down is a Network Security Review Committee (NSR Committee). The NSR Committee will be established by the CAC, together with other departments in charge (perhaps the Ministry of Industry and Information Technology (MIIT) and/or others), and will be responsible for deliberating on major Security Review policies, uniformly organizing network security review efforts, and coordinating major Security Review issues.

The next layer down is a Network Security Review Office (NSR Office). Though not specifically defined, the NSR Office might presumably be a local office under the CAC.

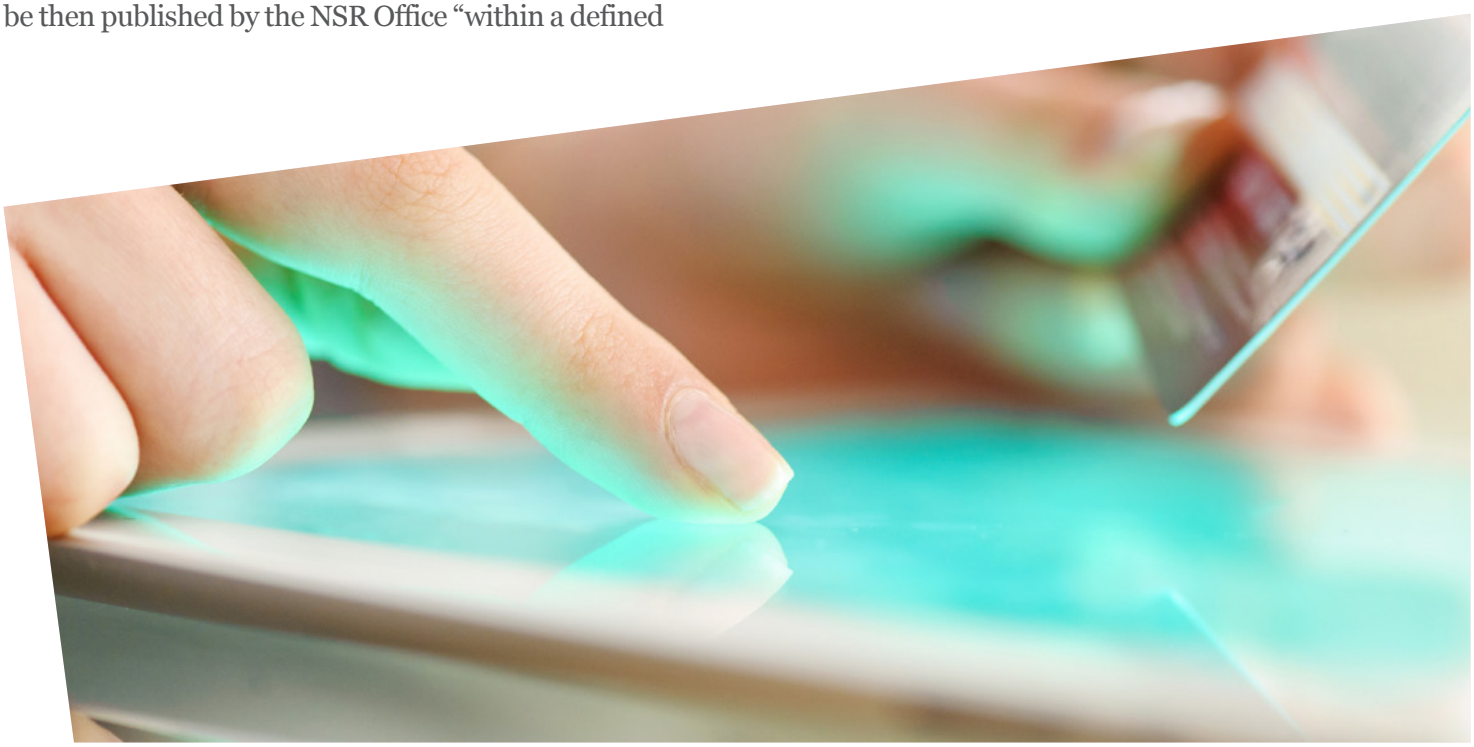
Each NSR Office is in charge of the specific organization and implementation of Security Reviews.

The NSR Office will arrange for two other groups of actors – third-party institutions, and experts – to actually conduct Security Reviews, where and as required based on the requirements of the state, the advice of national trade associations, market reactions, applications by enterprises and so forth. One of the dangers of such broadly consultative approach is how the NSR Office will balance comments or recommendations and, for example, filter out those driven by protectionist motives.

Third-party institution review apparently comes first. Such third-party institutions are to be designated by an as-yet unspecified organ of the state (so are not independent in any sense) and clearly there is a risk of decisions being driven by undue influence. The third-party institution will conduct a third-party evaluation. After that, a committee of experts (formed by the NSR Committee), taking the third-party evaluation as a basis, will conduct an overall assessment of (1) the security risks of a given network product or service, as well as (2) the security and reliability of the provider of such product or services. In a partial nod to greater transparency, security review results will be then published by the NSR Office "within a defined scope," so presumably with the parts relating to national security redacted.

Government authorities in "key industries" such as finance, telecommunications, energy and so forth (and therefore potentially others) are responsible for Security Reviews in their respective industries and sectors. It is not entirely clear, though, whether involvement of sector-specific authorities in Security Reviews puts those reviews on a separate track from other industries, or whether their participation is an additional layer, and how products and services that are used across multiple industries will be treated.

This does not augur well for overseas or FIE manufacturers which may, in the industry-organised reviews, come up against some of the government and regulatory bodies that historically have been less open to foreign investment. Many of the officials in those bodies and/or in the ranks of review institutions or experts will have worked in, or spent time with domestic players (those who have worked overseas or for FIEs or overseas manufacturers are likely to be in the minority) who will be seeking Security Review for their products, leading to obvious conflicts of interest. Other risks are exactly the same as those that



have plagued invitation to tender bid panels in China: manufacturers and other interested parties will try to pre-determine the outcome by identifying and seeking to influence the members of the group who make the final decision. Article 12 alludes to this risk by requiring these third party institutions to conduct an "objective, impartial and fair evaluation of the product, services and the provider," but this is really only a counsel of perfection and the potential for gaming the system through undue influence is undeniable. Article 13 alludes to another major issue: how to ensure the reviewers do not disclose confidential information revealed during the review process. This is discussed in detail below.

Security of proprietary information

Article 13 makes the position of the equipment or service provider with respect to compliance abundantly clear when it says: "Network product and service providers must cooperate with network security reviews." These will undoubtedly include disclosure of certain product/service information, some of which may be sensitive and/or proprietary and constitute valuable IP rights. This raises concerns about the security of such disclosed information and potential theft or loss of IP rights as a pre-condition to gaining market access.

The Draft Measures attempt to provide some comfort in this regard by providing that third party institutions and other relevant entities and personnel (such as experts) are obligated to maintain the security and confidentiality of any information to which they have access during the course of a security review, and must not use such information for purposes other than performing network security review.

However, we expect this will provide little real comfort, as no punishments are specified for the contravention of these measures and leaks and misappropriation can be virtually impossible to trace; obtaining adequate redress in the Chinese courts may not be realistic or achievable in the absence of overwhelming evidence. Understandably, some multinational companies providing network products and services may prefer to only provide non-front-line or a limited range of products in China to mitigate the risk of disclosures of "crown jewels" IP rights. And, of course, the "elephant in the room" (on which the Draft Measures are predictably silent) is whether passing certification means disclosing source code in part or in whole. Given the fact that the Draft Measures potentially allow and essentially require a wide range of government and Party bodies and other key industry participants to shun non-certified products, the commercial pressure on those overseas or FIE manufacturers who service those markets and industries to obtain certification is likely to be intense if they want to continue to service those markets; hence the pressure to produce source code once a request is made is also likely to be intense, bearing in mind, as noted above, that "cooperation" is mandatory.

Conclusion

National security is by definition a rather murky area of law and so it could not have realistically been expected that the Draft Measures would bring laser-like precision to the new Security Review process.

However, even the minimalist expectations of the foreign investor/manufacturer community are likely to have been disappointed by the Draft Measures, which do not appear to address some obvious and essential areas, to name but a few:

- No further clarity on which products and services are subject to Security Review: essentially an unsatisfactory and ultimately subjective test of "important network products and services used by information systems which concern national security and the public interest" will determine this
- No further clarity on which companies will be considered CIOs
- A national security review test that conflates areas already addressed elsewhere in Chinese law and which do not obviously belong in the national security review context
- A multi-layer government-driven bureaucracy organizes the review process and chooses all the participants with no safeguards on independence built in at any stage
- No obvious filtering mechanisms to prevent protectionist data and recommendations being put forward by trade associations or market players
- No clear machinery to prevent government officials with conflicts of interest (for example, ties to industry participants whose equipment or services is under review) from participating in the review process
- Many industries which have historically tended to be most closed to foreign investment will organize and carry out their own sector-based review processes
- No definitive list of the "key industries" which will be under an obligation to purchase certified equipment and services, so the list can be extended based on subjective interpretation
- No provision imposing accountability or specific punishments on participants who fail to conduct an "objective, impartial and fair evaluation" other than "being held responsible for the results of their evaluations"
- No mention of whether source code can be requested, but an obligation to cooperate means that if requested, network product and service providers have an obligation to provide it
- No safeguards built in to prevent corruption in the process or gaming the system through undue influence (although arguably partially covered by existing legislation)
- No mention of any review or appeal procedure for an interested party who feels the outcome of a Security Review was seriously flawed.

All in all, the Draft Measures do little to address or alleviate foreign investor or manufacturer concerns that came out of the passing of the Cyber Security Law in relation to Security Review. At most the Security Review process is now a little clearer. All that can be hoped for is that subsequent drafts can address at least some of the key issues raised above.

Please continue to the next page to see our Appendix showing the Security Review process in chart form.

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

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

Appendix

Security review process tree

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

Our offices
Associated offices

www.hoganlovells.com