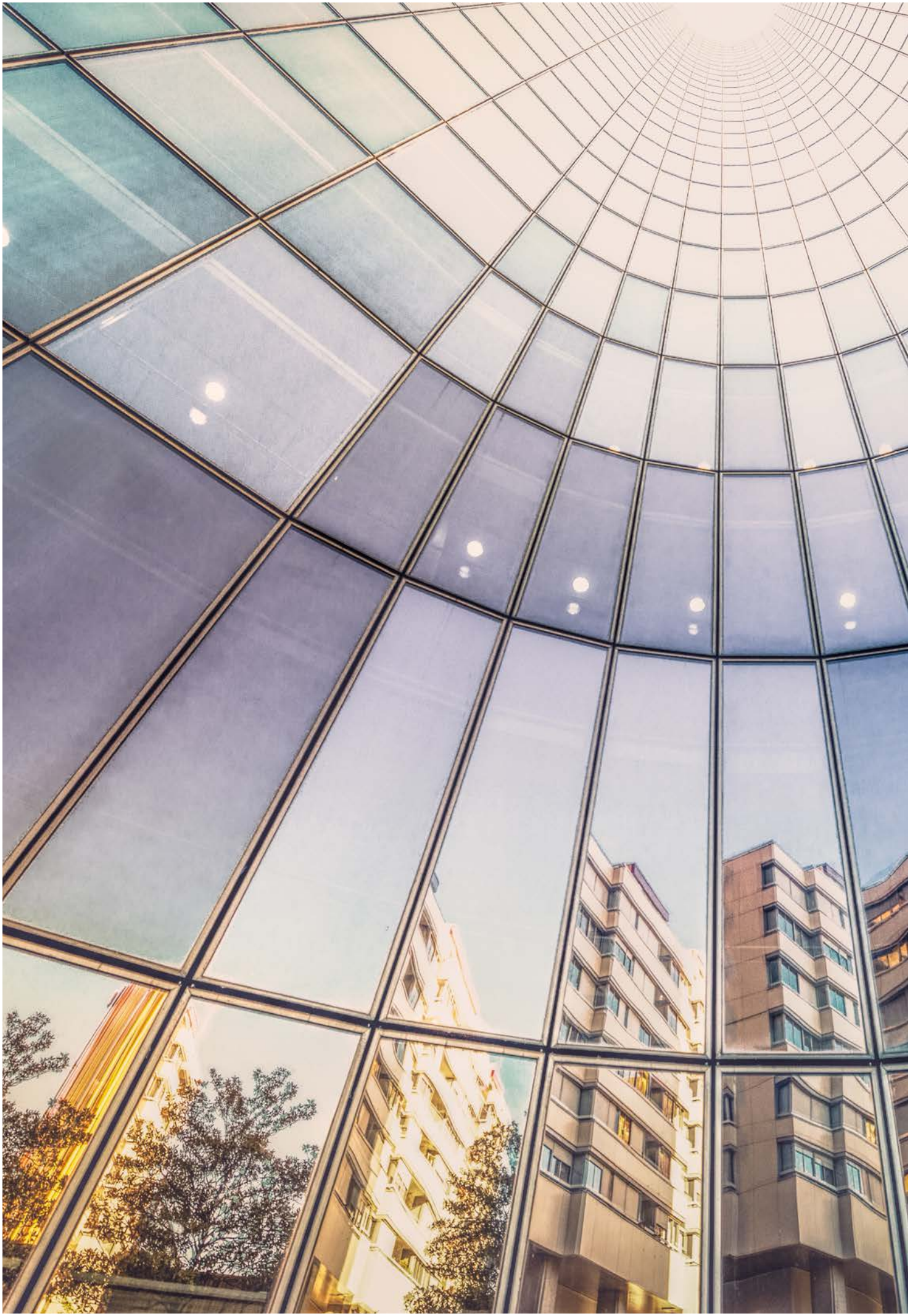
TMT China Brief

Summer 2018

Hogan Lovells



Editor's note

Welcome to our first issue of TMT China Brief in 2018!

This edition features a total of 14 articles which capture various significant TMT developments in Greater China. These 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.

Cybersecurity in China remains a hot topic. The Cyber Security Law is already in place but the question is how this law is going to be interpreted and implemented. In this edition, we will look at various draft/trial measures which provide further insight on key topics such as critical information infrastructure and security review of network products. We will also look at closely related topics concerning data localisation and cryptography.

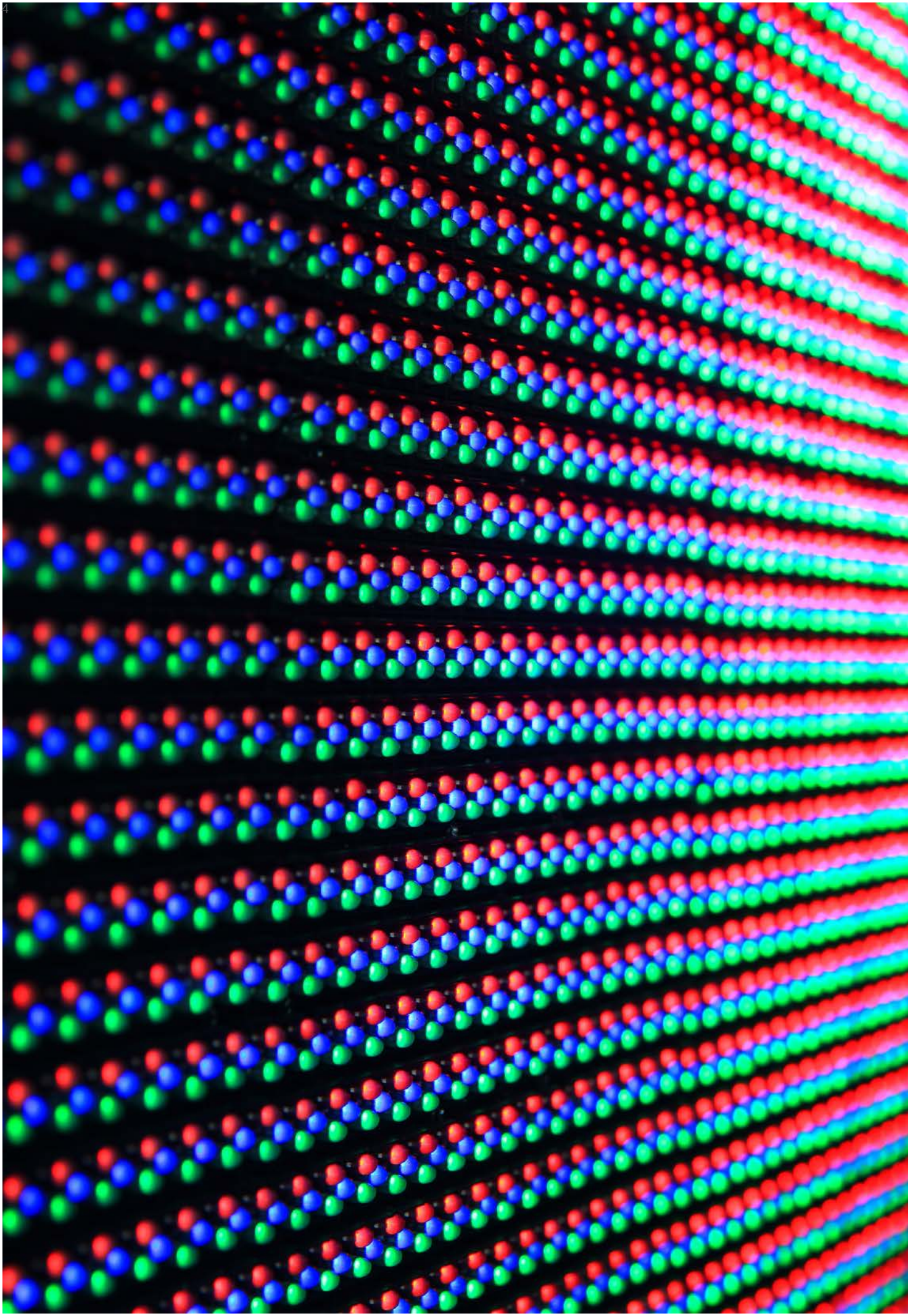
There is no doubt that China offers huge potential for technology businesses. The *Huawei v. Samsung* case is an excellent example of how China has become a new arena for global patent and FRAND disputes. The market is also opening up for areas such as cloud service providers and, more generally, the sharing economy. An important part to these developments is IP and e-commerce, and we will look at how China is establishing new laws and regulations (and courts) to brace itself for these challenges.

Turning to Hong Kong, the Securities and Futures Commission remains very much on the forefront in leading market discussions on cybersecurity standards and online advisory platforms in Hong Kong. We will take you through the details of those discussions, as well as the Hong Kong government's recent proposal to launch a statutory "do-not-call" register to put a tighter control on person-to-person telemarketing calls (cold calls or otherwise).

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

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



Content

Huawei v. Samsung – A new benchmark for standard essential patent litigation in China?

China has become a new battlefield in the global patent war amongst tech giants in the telecom industry. On 4 January 2018, the Shenzhen Intermediate People's Court (Court) rendered a landmark judgment in the *Huawei v. Samsung* standard essential patent (SEP) case that is expected to reshape dynamics between SEP licensors and licensees. On 21 March 2018, the Court released the non-confidential version of its judgment to the public.

The Court ruled in Huawei's favor – finding that Huawei had fulfilled its obligations under the fair, reasonable and non-discriminatory (FRAND) principle, but Samsung had not. Based on that finding, the Court granted an injunction against Samsung, forbidding any future infringement of Huawei's SEPs through the commercialization of Samsung's devices.

Case background

SEPs are patents which are meant to be indispensable for the proper working of a product implementing a standardized technology. The SEPs involved in the *Huawei v. Samsung* case concerned patents for telecommunication technologies, in particular what is known as 2G, 3G and 4G mobile communication standards.

Both Huawei and Samsung own extensive patent portfolios including numerous SEPs. This case was mainly about Huawei's SEPs – in particular, to what extent Samsung was allowed to use those SEPs in its communication devices like mobile phones, tablets etc. without having obtained a formal license from Huawei. Huawei brought its court action alleging that Samsung's devices infringed its SEPs, and asked the Court to grant an injunction against Samsung. Huawei argued that Samsung, by selling communication devices compliant with the 2G, 3G and 4G standards, had by definition implemented Huawei's SEPs. The Court accepted these arguments without much discussion.

The only aspect where the Court made an in-depth analysis was whether Huawei was entitled to seek an injunction based on its SEPs, as SEPs are subject to a set of specific conditions.

When a patent is incorporated into an industry standard and the patent holder believes it may become essential to the implementation of the standard, it will generally need to make a pledge to license the patent to all interested parties on FRAND terms.

Both Huawei and Samsung agreed to license their communication SEPs on FRAND terms. The question before the Court was whether in the negotiations to license their patent portfolios, each of the two companies had complied with their FRAND obligations. The Court found that Huawei had, while Samsung had not.

The Court re-phrased the FRAND analysis as an assessment of whether the SEP holder was "at fault" in terms of their procedural actions during the negotiation phase. It examined the extensive records of Huawei and Samsung's licensing negotiations and determined that Samsung deliberately "delayed the negotiations" that began in July 2011 and was "clearly at fault." Then, the Court also looked at the substance of the respective licensing offers — i.e. whether the royalty rates that each party offered were compliant with the FRAND principle.

Procedural aspects

The Court started its legal analysis by examining Samsung's conduct during the lengthy (cross)-licensing negotiations. When analyzing Samsung's compliance with the FRAND principle, the Court found the company "at fault" on several aspects, as Samsung was found to have:

- insisted on offering a portfolio license including both SEPs and non-SEPs (while Huawei insisted on only cross-licensing SEPs and later narrowed down the scope to LTE SEPs)
- failed to timely respond to Huawei's claim charts sent during technical discussion (alleging, in part, that its employees were too busy dealing with lawsuits with other competitors and licensors)
- failed to make a proper licensing offer or counter-offer until very late in the negotiations (and not in satisfactory form)
- rejected Huawei's proposal to submit the dispute on the FRAND royalty to arbitration
- continued its delaying tactics even during the Court-ordered mediation phase.

As a next step, the Court then examined Huawei's actions during the negotiation phase. It found that Huawei had not committed a material fault. In the Court's view, Huawei's actions during the negotiations did not violate the FRAND principle, as the company had:

- responded quickly to Samsung's declaration of its intention to negotiate a (cross)-licensing agreement
- insisted on cross-licensing only SEPs
- sent a list of its patents and claim charts, as well as an evaluation of Samsung's list of patents
- made six detailed and diverse cross-licensing offers to Samsung
- proposed to submit the dispute of the royalty rate to a third-party arbitrator (together with a detailed arbitration proposal)
- upon the Court's request during the mediation phase, quickly tabled a new cross-licensing offer
- promptly replied to Samsung's licensing offer.

Still, the Court also found a minor fault in Huawei's behavior during the licensing negotiations: the company was not clear enough about the amount of LTE SEP families acquired from Sharp, which were to be included in the cross-license. Nonetheless, since Huawei was found to have corrected its fault later on, the Court held the issue not to materially affect the overall negotiation process.

Substantive aspects

After the analysis on the procedural aspects, the Court also examined the substance of the parties' respective licensing offers. It examined the royalty rates that each party proposed, and held that the Samsung's offer was "clearly at fault," whereas Huawei's was not.

To reach this conclusion, the Court essentially made a two-step analysis: first, it assessed the relative strength of Huawei's and Samsung's SEP portfolios, and, second, it compared the licensing offers by the two companies with their respective SEP portfolio strength.

In the first step of the analysis – assessing Huawei's and Samsung's 3G and 4G SEP portfolio strength – the Court basically followed a "top-down" approach, although it did not use this precise term. In essence, the "top-down" approach looks first to the overall level of royalties associated with a standard and then allocates a portion of this total to an individual SEP holder based on the relative strength of its SEPs in that standard.

In its assessment, the Court used numerous pieces of evidence and testimonies (including by economics experts) put before it and conducted a multi-factor analysis. Among others, the Court looked at:

- the number of the parties' technology proposals accepted by the standard-setting organizations
- their relative estimates of confirmed SEPs (as compared to unilaterally declared SEPs)
- the eight SEP invalidity decisions before Chinese courts (as Huawei and Samsung each challenged the validity of their patents before the Patent Reevaluation Board and courts).

For many of the factors of this analysis, Huawei's number was higher than Samsung's. Hence, the Court held that the relative strength of Huawei's and Samsung's SEPs was at least similar (on a worldwide basis, with Huawei being stronger in China).

Then, the Court undertook the second step of its analysis, comparing the respective licensing offer to the relative strength of the SEP portfolio.

The Court examined Huawei's and Samsung's licensing offers in quite some detail and concluded that Huawei's proposed royalty was, and Samsung's was not, in compliance with the FRAND principle. This finding was made against the backdrop that the parties were discussing a SEP cross-license agreement and Samsung asked for a royalty three times as high as Huawei. Having concluded before that Huawei's SEP portfolio was at least as valuable as Samsung's, the Court decided that Samsung's demand was not reasonable and therefore not in line with the FRAND requirement.

Conclusions

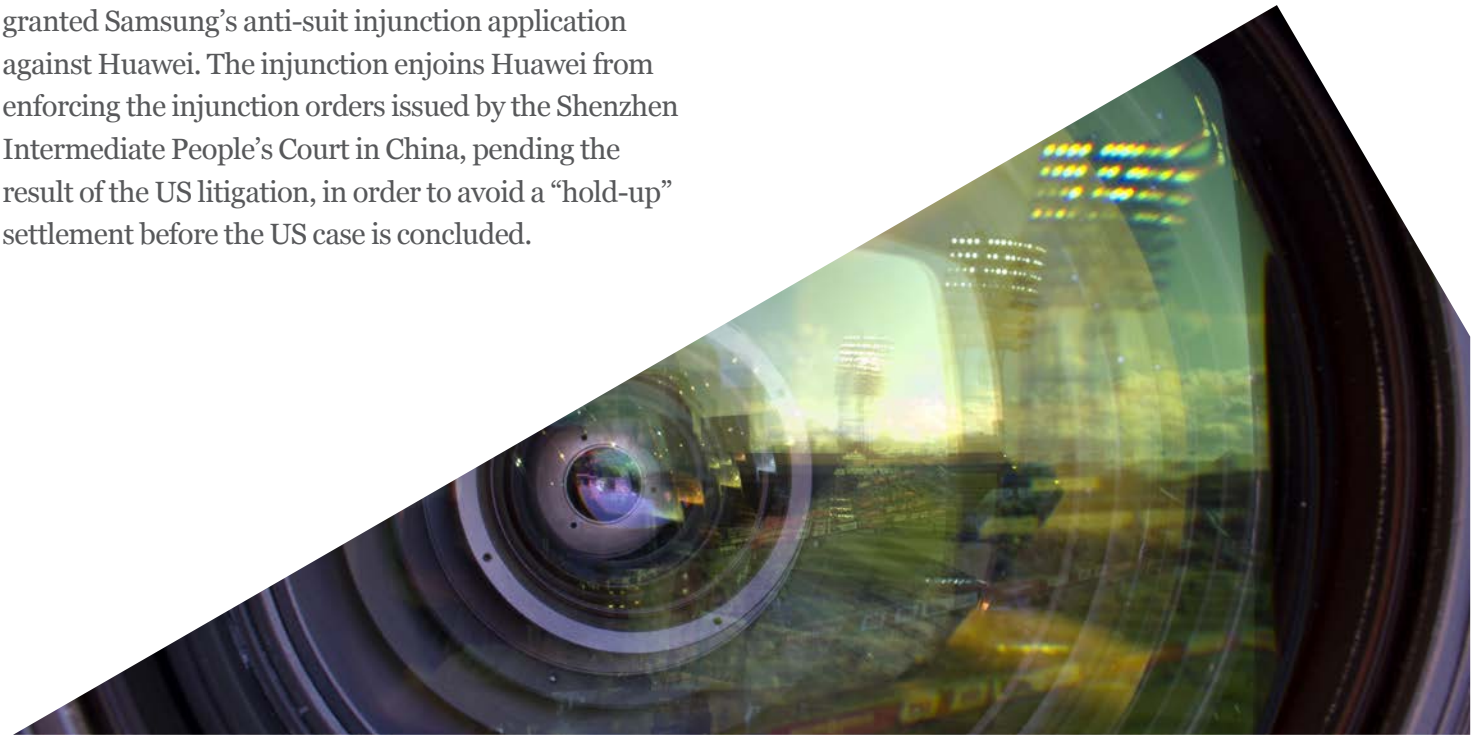
The Court's judgment in *Huawei v. Samsung* establishes a new approach for SEP licensing. The Court examined the conduct of both parties, both from a procedural and substantive perspective, to assess whether they behaved on FRAND terms.

The judgment is in line with the outcome in *Xi'an Iwncomm v. Sony*, where the Beijing High People's Court at second instance affirmed that the licensor (Iwncomm, a Chinese company) had complied with FRAND obligations when negotiating SEP licensing with Sony. At the same time, however, the *Huawei v. Samsung* judgment departs (both in terms of outcome and analysis) from a prior key judgment of the same court – the Shenzhen Intermediate People's Court – in *Huawei v. InterDigital*. As a couple of SEP cases are pending before Chinese courts at this point in time, it will be interesting to see whether the *Huawei v. Samsung* judgment indicates a shift to a more pro-licensor position more generally.

The Shenzhen Intermediate People's Court's judgment is clearly not the last word spoken in this case. Indeed, in addition to a potential appeal in China, on 13 April 2018, the District Court of the Northern District of California granted Samsung's anti-suit injunction application against Huawei. The injunction enjoins Huawei from enforcing the injunction orders issued by the Shenzhen Intermediate People's Court in China, pending the result of the US litigation, in order to avoid a "hold-up" settlement before the US case is concluded.

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

Qing Lyu
Associate, Shanghai
T +86 21 6138 1629
qing.lyu@hoganlovells.com



China tightens up overseas transfers of IPRs

On 29 March 2018, the State Council released the External Transfer of Intellectual Property Rights Measures (Trial Implementation) (IPR Overseas Transfer Measures) providing for further governmental scrutiny of overseas transfers of intellectual property rights (IPRs) from China, with a focus on the impact of such transfers on national security and/or the impact on the development capabilities for certain key industries in China. More specifically, the IPR Overseas Transfer Measures set forth procedures for various governmental departments, including those in charge of IPR, technology, agriculture, and forestry to become involved in reviews of such transfers conducted by the Ministry of Commerce (MOFCOM).

The IPR Overseas Transfer Measures became effective in March 2018. As is customary in China, there is no indication as to the length of the "trial implementation" period.

Though many of the details on how the IPR Overseas Transfer Measures will be implemented remain to be worked out, the message is clear that there will be a stepping up in the enforcement of Chinese technology export regulations. This development may affect companies that engage in research and development (R&D) activities in China or are parties to IPR licensing transactions wishing to export improvements made by Chinese licensees.

Scope of the IPR Overseas Transfer Measures

The IPR Overseas Transfer Measures apply to the review of any external transfer of IPR, which is defined to include patent rights, proprietary rights related to integrated circuit design, computer software copyrights, rights to new plant varieties and so forth, either by way of technology export or as a result of the acquisition of Chinese domestic capital enterprises by foreign investors. The language is open-ended enough to allow to be interpreted as encompassing other forms of transaction resulting in an overseas transfer of IPR. The IPR Overseas Transfer Measures further note that an external transfer may refer to the transfer of IPR by a Chinese entity or individual to a foreign company, individual or other form of entity including by way of changes to the IPR owner, changes in the actual controller of the IPR, and exclusive licenses to use the IPR (the latter may kick in contractually in practice when a Chinese counterpart makes 'improvements').

Evaluation standard

The IPR Overseas Transfer Measures stipulate that the subject matter of the review is both the impact of the external IPR transfer on China's national security and development capabilities of technological innovation in certain key sectors in China. None of these expressions is further elaborated on in the IPR Overseas Transfer Measures.

Review mechanisms

Involving exported technologies. For technology exports, the IPR Overseas Transfer Measures note that that any technologies that fall under the "restricted" category in the MOFCOM Restricted and Prohibited Technologies for Export Catalogue will be subject to review.

For the export of patent rights and rights related to integrated circuit designs, the local IP departments are consulted by the local MOFCOM office conducting the review for a written opinion. This opinion should be relied upon by the MOFCOM office in issuing its decision and provided to the national IP administration for record filing.

In the case of overseas transfers of copyright software, the competent local MOFCOM office and department in charge of science and technology jointly conduct the review. Where computer software copyright to be transferred overseas has already been registered with an appropriate software registration authority, the local MOFCOM office must notify that authority of the results of the review in a timely manner. The software registration authority must not carry out change of ownership procedures for the computer software copyright in question in the event it is found to be non-transferable.

Where the IPR to new plant varieties is transferred overseas, the agricultural and forestry departments carry out the review. Their emphasis is on the impact of the proposed transfer on China's agricultural security, in particular food security and seed industry safety.

Involving acquisitions by foreign inventors. The IPR Overseas Transfer Measures note that when conducting a security review in relation to mergers and acquisitions of domestic companies by foreign investors, the agency responsible for national security (i.e., MOFCOM) must transfer the materials to the competent departments in charge of the specific type of IPR for their comments.

Similar to the above scheme, where patent rights and exclusive rights for layout designs of integrated circuits are involved, the State Intellectual Property Office has responsibility; if computer software copyright is involved, the national department for copyrights has responsibility; if new plant variety rights are involved, the departments for agriculture and forestry are responsible. The relevant departments then need to promptly review and issue their written opinion to the national security agency, which then takes the final decision.

Supplemental rules to be issued

The IPR Overseas Transfer Measures call for the relevant governmental departments to formulate detailed rules on the review procedures and timeline, the required application documents, and the division of responsibilities between the various departments.

Conclusions

The IPR Overseas Transfer Measures cannot be divorced from the wider, somewhat tense political and trade-related climate which forms the backdrop to China tightening up the procedures on technology exports.

In a sense, nothing has changed, as the Technology Import and Export Administrative Regulations from 2002 imposed an approval requirement on the export of technology categories under the Restricted and Prohibited Technologies for Export Catalogue and a ban on prohibited category technologies being exported.

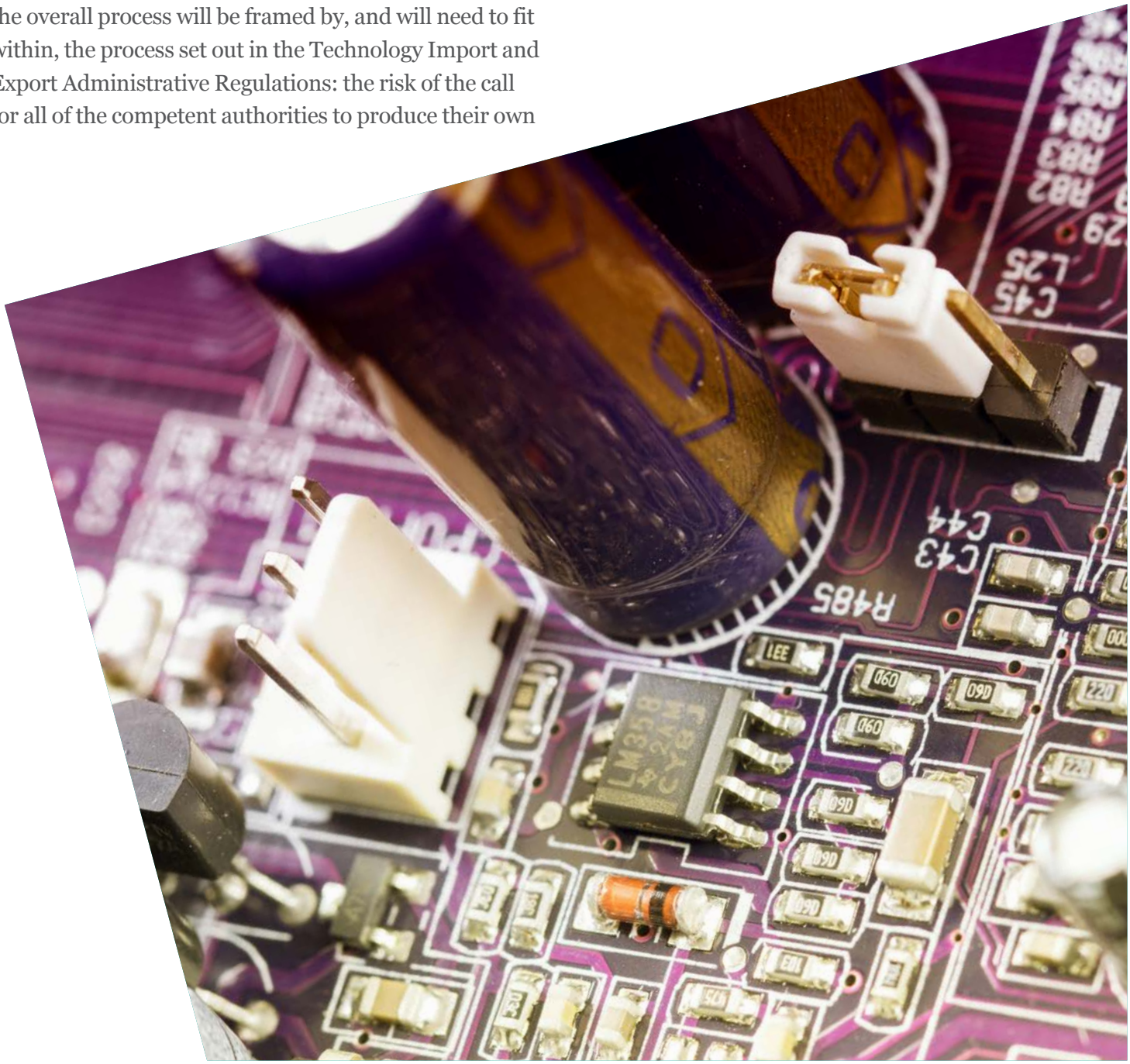
However what has changed is the requirement to involve the departments in the IPR space in a more formal, legally-defined manner. Presumably the idea is that they are more 'expert' in their respective fields and thus better able to assess the impact on national security and the development capabilities of sectors under their administration.

The IPR Overseas Transfer Measures also link to the national security review process for certain acquisitions by foreign investors of domestic companies where IPR transfers is considered as part of the national security review process. The IPR departments in charge are given responsibility for their sectors under administration, thus making IPR a prominent feature of the otherwise 'black box' process for national security review. This appears to be designed to ensure that MOFCOM does not overlook this angle when making the final decision on the national security review.

Going forward, it may become even harder for foreign investors to export the results of their R&D and other IPR-generating activities in China where they fall within "restricted" sectors (a well-advised foreign investor would presumably have started out with no expectation of overseas transfer in the case of a "prohibited" sector).

Further delays can also be expected, as nowhere in the IPR Overseas Transfer Measures is there any mention of time limits for the review process, although presumably the overall process will be framed by, and will need to fit within, the process set out in the Technology Import and Export Administrative Regulations: the risk of the call for all of the competent authorities to produce their own detailed implementing rules is ending up with multiple inconsistent processes where it becomes a timing lottery, based on the category of IPR in question.

Yu-An Chang
Counsel, Shanghai
T +86 21 6122 3802
yu-an.chang@hoganlovells.com



Push for joint ventures among international cloud providers in China

Foreign investment in cloud services is heavily restricted in China. For years, international cloud operators have been struggling to identify structures that address regulatory concerns, but at the same time enable a service delivery model that is consistent with international offerings. Teaming up with Chinese companies is not something new, but has become a more prominent feature in the cloud space following certain regulatory developments in 2017, notably new licensing requirements issued by the Ministry of Industry and Information Technology (MIIT), China's telecommunications industry and internet regulator, as well as the implementation of the Cyber Security Law.

Over the past year or so, multiple US technology companies have announced their partnerships with Chinese cloud license holders, naming such Chinese partners as "operators" of their cloud services in China. These cross-border partnerships represent the latest trend in China's cloud industry.

Licensing requirements for cloud operators

To understand this somewhat challenging area and to put it into context, you have to go back to China's liberalisation commitments when it joined the World Trade Organisation (WTO). The commitments allowed foreign investment of up to 50% in value-added telecoms services (VATS) and up to 49% in basic telecoms services (BTS). However, what is less well understood is that when the section in the WTO accession schedule setting out China's sector-by-sector commitments on VATS (which reads "Value-added telecoms services, including the following [...]" and then lists certain VATS services) was being negotiated, those on the other side of the negotiating table to China interpreted "including" to be the lawyer's "including, without limitation," while MIIT has consistently taken the view that "including" means "namely," so China has no obligation to liberalise any sector not expressly included in the WTO text. Internet data centers (IDC) are classified as a VATS, but are notably absent from the WTO schedule. Hence as far as MIIT is concerned, there is no commitment to open up this sector to foreign investment. The classification of services into VATS and BTS is set out in the Catalogue for the Classification of Telecoms Services, the latest iteration of which took effect in March 2016 (Telecom Catalogue).

Operating cloud services in China generally requires a VATS business operating permit (Permit) issued by MIIT, although there is some debate over whether certain elements of Software-as-a-Service (SaaS) models require a VATS Permit. A Permit is clearly required for IDC services, a category more meant to cover the hardware aspects of cloud services, in particular the operation of Internet data centers. Beginning 1 March 2016, a separate license was de facto required for Internet resource collaboration (IRC) services, which are set out as a subset of IDC in the Telecoms Catalogue. MIIT confirmed that this sub¬category under IDC covers "cloud services" in the draft Circular on Regulating Business Activities in the Cloud Services Market, issued for public comment in November 2016 (Draft Cloud Circular).

"Cloud services" were not defined in the Draft Cloud Circular, and may, based on recent market practices, be broadly interpreted to cover three types of services: Infrastructure-as-a–Service (IaaS), Platform-as-a-Service (PaaS) and SaaS. Based on a circular issued by MIIT in January 2017, cloud businesses established after 1 March 2016 must now obtain an IRC Permit as well as an IDC Permit before going into operation. Cloud businesses with IDC Permits that were operational prior to 1 March 2016 (subject to a notice requirement) had until 31 December 2017 to obtain an IRC Permit in addition, failing which they had to cease engaging in the business.

On 12 January 2018, MIIT issued another circular to reconfirm its position on the requirement for an IRC Permit to engage in cloud business, together with a list of more than 100 companies that have obtained IRC Permits,

including major Chinese cloud players such as Alibaba and Tencent, as well as local partners of overseas cloud operators, as well as listing those who did not requalify for on IRC Permit.

Foreign participation in cloud services

As noted above, MIIT takes the view that IDC services are not open to foreign investment. By making IRC a subset of IDC in the Telecoms Catalogue, MIIT effectively made IRC off-limits to foreign investment as well, thereby severely limiting direct equity participation options in the cloud space. There are, however, several potential options that foreign investors can consider when seeking to participate in the cloud space in China. None of these are a panacea and each has its own pros and cons. Sometimes it may be necessary to mix and match.

Investing under the Closer Economic Partnership Arrangement

In strict legal terms, an investment through a Hong Kong entity qualified under the Mainland China / Hong Kong Closer Economic Partnership Arrangement (CEPA) is the only option for foreign investors to access the Chinese cloud market (primarily IDC as it does not expressly cover IRC) through equity ownership. Under the relevant rules, a CEPA-qualified Hong Kong service provider entity is allowed to establish an equity joint venture with a local Chinese company to engage in IDC business, with the level of Hong Kong ownership capped at 50%. The ownership of Hong Kong companies is not subject to foreign investment restrictions in this sector, meaning that the Hong Kong joint venture partner can be 100% foreign-owned.

However, the arrangements remain subject to approval by MIIT, which in practice is not always supportive of equity joint ventures based on a CEPA arrangement. Consistent with its restrictive interpretation of China's WTO commitments, MIIT has interpreted CEPA as only applying to investors where the ultimate shareholder is from Hong Kong.

VIE structures

The well-known variable interest entity (VIE) structure typically involves a foreign investor entering into a series of contractual arrangements with a Chinese VATS Permit holder that enables the foreign entity to exercise effective control over the licensed business, and seeks to achieve an equity-like return in a sector restricted to foreign investment. VIE structures are popular in industry sectors restricted for foreign investment, including the telecoms and Internet sectors, as well as those where in many cases foreign participation is prohibited, such as many media-related sectors, but do involve substantial risks to foreign investors.

Essentially, the foreign investors have to control the nominee shareholders that own the domestic capital VATS Permit holder. If these nominees turn against the foreign investor and claim outright ownership, they may use, among others, threats of reporting the VIE structure to the regulators because the structure has never been expressly recognized by the Chinese government. Indeed some recent arbitration cases resulted in it being successfully challenged on the basis it was a circumvention of the requirement for the foreign investor to obtain a VATS Permit (with MIIT approval) through a foreign-invested enterprise in China.

In February 2015, the Ministry of Commerce proposed a draft Foreign Investment Law, in which it cast doubt on the legality and sustainability of VIE structures involving control by a foreign investor in restricted sectors (such as all telecoms/internet sectors, including IDC/IRC). This could have a far-reaching impact on many VIEs in China, resulting in challenges for those who have made use of it. However, this proposal has not yet been made law, and there is some expectation that there will be some form of grandfathering or transition for existing VIE structures, as billions of dollars have been invested in Chinese businesses through VIE structures, with the businesses listed in Hong Kong and the US. Expectation is not always the same as what transpires in practice, as those who watched the unwinding of the predecessor Chinese-Chinese-Foreign structures can bear witness. The difference this time around is the personal fortunes of many Chinese entrepreneurs are in the mix too. Notwithstanding the well-known risks, the VIE structure is still the most commonly used structure for foreign investors to enter restricted sectors in China.

However, MIIT appears to take the view that cloud and IDC services are too sensitive to be controlled by foreign investors through VIE structures, and so the apparent administrative tolerance for VIE structures in other restricted sectors does not generally extend to this space. In practice, MIIT may exert pressure on the foreign investor's Chinese partner or VATS Permit holder to remove control elements that are viewed as too aggressive. As things stand now, a full-on version of the VIE structure as seen in the venture capital world in other telecoms/ Internet sectors, for example, seems to be a non¬starter for large-scale cloud businesses in China.

Technical cooperation with domestic Chinese license holders

Currently MIIT seems to be more comfortable with technical cooperation models for delivery of cloud services in China, in which (1) a Chinese domestic capital VATS Permit holder enters into customer-facing contracts, and (2) the foreign cloud service provider enters into cooperation agreements to provide technical support to the VATS Permit-holding domestic capital company. This model is supported by the Draft Cloud Circular, which acknowledges that licensees may enter into technical cooperation arrangements provided that the domestic VATS Permit holder reports its technical cooperation to MIIT in writing. The Draft Cloud Circular has still not become law, but in practice MIIT is implementing most of its provisions. The following activities are not permitted during the course of collaboration:

– the leasing, lending or transfer of a telecommunications services operating license 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

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

The second and third prohibitions are particularly challenging to branded overseas cloud service operators, as this means a foreign company cannot 'own the customer' and can only co-brand the cloud services.

Cyber Security Law implications

On 1 June 2017, the Cyber Security Law came into effect. This is a law with profound implications for global companies doing business in China. The cloud services sector is impacted in a number of important ways. Among other things, the Cyber Security Law requires:

– **Data localization**. Operators of "critical information infrastructure" must store personal information and "important data" collected during its operations within Mainland China, unless the transfer offshore has been approved. The State Council has yet to come up with a final definition for "critical information infrastructure operator."

– **Obligations to provide law enforcement assistance**. Network operators are required to maintain weblogs for six months and provide technical assistance and support to law enforcement investigations.

The Security Assessment for Personal Information and Important Data Transmitted Outside of the People's Republic of China Measures (Amended) (Draft Rules on Overseas Data Transfers) issued in connection with the Cyber Security Law *de facto* widen the net by imposing a variant of the data localization measure (i.e., one cannot transfer overseas without clearing the security review) on "network operators." Network operators is a very broad concept that is thought to include cloud service operators in China, so as to make overseas transfers of personal information and important data collected by network operators subject to a security review by the Chinese government and consent from the data subject. These rules were meant to come into effect at the same time as the Cyber Security Law, but were put on hold as they proved to be hugely controversial, especially as the scope went beyond the scope of the Cyber Security Law.

As noted above, although uncertainties exist as to scope of the Cyber Security Law and its applicability to cloud services providers and operations, it appears likely that cloud service providers with operations in Mainland China will be required to:

– Locate their service facilities and network data within Mainland China, where such services are provided to customers in China

– Ensure that any cross-border data transfers comply with relevant rules, including the Draft Rules on Overseas Data Transfers (when they become law).

Analysis of shared models

Recently announced cases involve US technology companies providing different types of cloud services, including IaaS, PaaS and SaaS on a large scale. Nevertheless, broadly speaking, they appear to have taken a similar approach to providing cloud services in China, as follows:

– Local VATS Permit holder(s) will enter into contracts with end customers and provide cloud services in their own name

– Cloud services are co-branded

– The local VATS Permit holder will operate the cloud services, while receiving technological support from its foreign partner

– Data centers to support the service offering and store the cloud service data are either owned by the local VATS Permit holder or leased from licensed third party vendors, and are located in China.

These all seem to be driven by the Draft Cloud Circular and the Cyber Security Law. However, in reality, customers are choosing to purchase these cloud services not because of the local VATS Permit holding entity that fronts the business, but the technology provided by, and the brand or co-brand of the big name behind it. Essentially, it has to be the global technology provider that will take the lead in managing the core functions of the business, so that people can get comfortable with the quality of the services provided to customers in China, many of whom are Chinese subsidiaries of their global clients. This is not easily achievable in the light of the laundry list of restrictions for such cooperation, not to mention those imposed by MIIT when the cooperation is reported to MIIT. With this in mind, the cooperation relationship must be structured properly, which means satisfying regulatory requirements while granting a minimum level of operational control that is acceptable to the global cloud services provider.

The cooperation structure may also take on board certain elements of a VIE structure. As discussed above, it is virtually impossible to adopt all the elements of a typical VIE, which will result in full control, and such attempts have in our experience been resisted by MIIT. Local partners on the other hand may be willing to accommodate a lot of onerous terms, as they are primarily incentivised by the financial benefit generated from the cloud operations. However, technical cooperations need to be reported to MIIT, which may review the terms of cooperation, so overly aggressive terms will not necessarily work.

Conclusions

For newcomers to the China market, no matter if it is for providing IaaS, PaaS or SaaS, unless the foreign company can get comfortable your model of SaaS does not require an IDC/IRC VATS Permit, it will likely need to team up with a Chinese VATS Permit holder, and structure the cooperation relationship in such a way as to strike a delicate balance between meeting regulatory requirements and achieving operational autonomy.

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

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

China issues second draft of new e-Commerce Law

On 7 November 2017, the Standing Committee of the National People's Congress (NPC) published the second draft of the E-commerce Law (Draft). The goal of the Draft is to regulate China's burgeoning e-commerce sector, and thereby facilitate growth, maintain the "market order" and eradicate scams and counterfeits.

The Draft was published only days before China's biggest online shopping event, "Double Eleven" (Singles' Day), which takes place annually on 11 November. In 2017, no less than USD 25 billion was spent on e-commerce on Single's Day, a 40% increase compared to 2016. These new results emphasize the growing importance of this sector in China and the need for regulation.

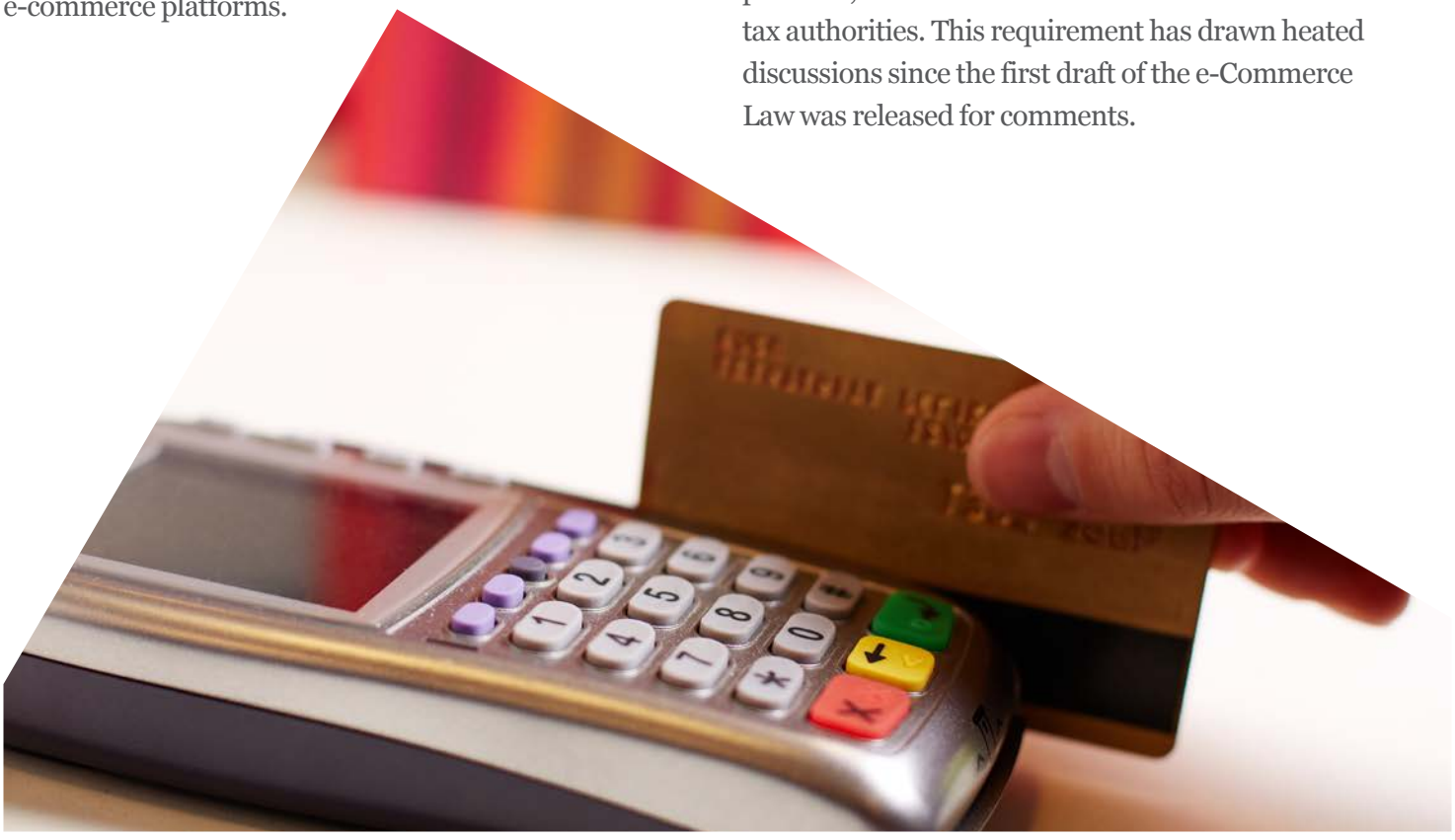
Against this backdrop, the Draft aims to regulate some of the real and perceived problems in the industry.

Scope

The Draft has a wide scope of application, and extends to all "e-commerce operators" in China, which is a new concept encompassing: (1) operators exploiting their own websites, (2) e-commerce platform operators, and (3) e-commerce operators which listed their web shops on e-commerce platforms.

AIC registration and taxation

One of the novelties of the Draft is that all e-commerce operators must be registered and licensed by the Administration for Industry and Commerce (AIC) (exceptions are made for vendors of home-grown agricultural products and arts and crafts). Moreover, all e-commerce operators (i.e., even the individual web shop on e-commerce platforms) will have to pay taxes on their e-commerce revenue, which is, up until now, often not the case for individual web shops. This new rule arises from China's goal to promote e-commerce development while ensuring its convergence with other industries. To ensure this convergence on tax collection and the effective enforcement thereof, the Draft requires platform operators to collect the business license and identity information of individual web shops on their platform, and to transmit this information to the Chinese tax authorities. This requirement has drawn heated discussions since the first draft of the e-Commerce Law was released for comments.



False advertising

The Draft reiterates some of the prohibitions under the Advertising Law, but tailors them to an online setting: e.g. it is forbidden to fabricate false transaction information, write and post fake user reviews or delete genuine user reviews, unless they are defamatory or otherwise forbidden. Moreover, sponsored listings should be clearly marked as such.

Other highlights include:

- **Intellectual property**. The Draft provides a formal framework for the notice-and-take-down procedures that already exist on most e-commerce platforms in China. According to the Draft, e-commerce platform operators must provide takedown procedures, allowing intellectual property (IP) owners to request the takedown of infringing links or even the closure of the web shop, if the IP owner can provide *prima facie* evidence of infringement. Platforms that do not take appropriate measures will be jointly liable for the increase in damages caused by the prolonged IP rights infringement. However, IP owners who erroneously request the takedown of genuine links or web shops will have to indemnify any good faith web shops selling genuine articles.
- **Data protection and cybersecurity**. The Draft simply refers to the Cyber Security Law for the treatment of personal information of e-commerce users. However, the Draft does contain some specificities: the Draft introduces an EU-style right for users to search, correct or delete any of their personal information saved by e-commerce operators, or to deregister altogether. As to cybersecurity, under the Draft, e-commerce, platforms must adopt technical or other measures to protect network security, and to adopt contingency plans for cyber security incidents.
- **Protection for operators from abuses by e-commerce platform operators.** The Draft provides protection for e-commerce operators registered with e-commerce platforms. The Draft points out that e-commerce platform operators must not take advantage of the service agreement, transaction rules or other means to impose unreasonable restrictions or transaction conditions on the transactions of operators on platform or the price of such transactions, or collect unreasonable fees against operators on platform. This provision aims to address recent controversies in relation to some e-commerce platform operators trying to limit participation in certain major promotion events to a selected group of sellers.
- **Risks and liabilities assumed during transportation**. According to the Draft, e-commerce operators shall deliver goods or services to consumers in accordance with what was offered and with the way or time as agreed with consumers, and assume the risks and liabilities during the transportation of goods, unless consumers reach an agreement with e-commerce operators to select another logistic service provider. This is in line with current practice with major e-commerce operators in China, and confirms such accountability system expressly in the Draft.
- **e-commerce dispute resolution**. The Draft provides that e-commerce operators need to set up convenient and effective complaint and reporting mechanisms, disclose the complaint and reporting channels and other information, and timely accept and handle any complaint and reporting. This aims to address the challenges that consumers may encounter at the time they intend to enforce their consumer rights.

– **Sanctions**. The Draft provides for a range of sanctions for infringements. Apart from monetary sanctions of up to RMB 500,000, the Draft also prescribes that any infringement of the law will be registered in the infringers credit file, and made public.

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

Conclusions

All-in-all, the Draft is fairly balanced and largely in line with existing practices. One of the most controversial aspects of the Draft is the obligation for individual web shops on e-commerce platforms to register with AIC and obtain a business license. However, this new obligation could have a markedly positive impact for IP owners, as it would make it harder for bad-faith IP infringers to evade enforcement actions by an IP owner by simply closing their web shop (or having it taken down by the platform) and opening a new one.

Implementing China's Cyber Security Law

On 11 July 2017, the China Cyberspace Administration (CAC) released the Draft Security Protection Measures for Critical Information Infrastructure (Draft Regulations) for public consultation, as another piece of key follow-on legislation to the Cyber Security Law adopted on 6 November 2016 and effective from 1 June 2017.

Article 31 of the Cyber Security Law stipulates that the detailed scope of "critical information infrastructure" (CII) and security protection measures for CII will be formulated by the State Council. Although the Draft Regulations were released in a CAC circular seeking public comment, the Draft Regulations appear to be the measures referred to in Article 31 of the Cyber Security Law.

Of all the provisions in the Cyber Security Law, the rules relating to CII have always attracted the most public attention, as CII operators are subject to the strictest obligations under the Cyber Security Law, especially with respect to data localization requirements and security review for purchases of network products and services. However, because the scope of CII was never made clear in the Cyber Security Law or supporting legislation, many multinational enterprises with a need to move data across borders or purchase overseas network products and services have been waiting with some trepidation for the release of the Draft Regulations, which were supposed to clarify the scope of CII.

However, they will be disappointed once again if the Draft Regulations are finally promulgated in their current form, because the most highly anticipated answer is not provided – they only say that specific guidelines for identifying CII shall be formulated.

Furthermore, under the Draft Regulations:

- additional security obligations are imposed on CII operators
- reporting obligations are imposed with respect to the remote operational maintenance of CII
- additional security review requirements on systems or software developed by outsourcing, and on donated network products are imposed.

Refining the scope of CII

Article 18 of the Draft Regulations provides that network facilities and information systems operated or managed by the following units are included within the scope of protection for CII, if the destruction or experiencing a loss of functionality or data leakage with request to such network facilities and information systems may severely jeopardize national security, the national economy and the people's livelihoods or the public interest:

- government agencies, and units in the fields of energy, finance, transportation, water conservancy, healthcare, education, social security, environmental protection, public utilities and other industries and sectors
- telecoms networks, broadcasting networks, Internet and other such information networks, and units providing cloud computing, big data, and other large-scale public information network services
- scientific research institutes and manufacturers in the fields of national defence science, technology and industry, large-scale equipment, chemical engineering, food and drugs and other such industries
- broadcasting stations, television stations, news agencies and other such press outlets
- other important units.

Compared with Article 31 of the Cyber Security Law, the newly-added industries now considered to constitute CII are "national defence-related science, technology and industries, large-scale equipment, chemical engineering and food and drugs," while other additions can be seen as the refinement of existing industry categories. For instance, the "healthcare, education, social security, environmental protection and public utilities" industries may be seen as elaboration on the theme of the "public services" industry. The "telecoms networks, broadcasting networks, Internet, providers of cloud computing, big data, and other large-scale public information network services, broadcasting stations, television stations, and news agencies" industries may be viewed as elaboration on the theme of the "public communications and information services" industry.

The Draft Regulations follow the two-step methodology for determining what constitutes a CII operator under the Cyber Security Law, which is to:

– first verify whether an enterprise falls under the list of specified industries

– then apply the test of potential hazardous consequences.

Furthermore, the catch-all phrase of "other important units" is tagged on at the end of the list, which means the category can be expanded at will by CAC officials, thereby removing any semblance of finality and definitiveness.

Article 19 of the Draft Regulations goes on to explain that CAC, in conjunction with the relevant telecoms department, public security organs and so forth will formulate guidelines for identifying CII. This indicates that although Article 18 provides some basis for identifying which companies may be CII, ultimately whether a specific network facility or information system will be deemed a CII will be determined based on certain to-be-issued guidelines. This may presage the deployment

of the results of the nationwide network security investigations and enquiries carried out since July 2016, where a set of internal Guidelines for Key Information Infrastructure Identification (Guidelines) were developed and used by the local authorities to conduct surveys on certain enterprises in China. The Guidelines divide CII into three categories:

– websites, such as websites of the Communist Party and government organs, enterprises and public institutions, as well as news websites

– platforms, such as Internet service platforms including instant messaging, online shopping, online payments, search engines, E-mail, BBS, maps, and audio/video

– production and business-related infrastructures, such as office and business systems, industrial control systems, large data centers, cloud computing platforms, and television relay systems.

Further, the Guidelines provide a chart listing key industries and set out a three-step process to identify CII operators:

– identify critical industries (including, for example, financial services and telecoms and Internet services)

– identify information systems or industrial control systems related to critical businesses

– identify a CII based on different materiality thresholds (including, for example, number of users, data volume and influence if damaged) applicable to the abovementioned three types of CIIs (i.e. websites, platforms and production and business-related infrastructures).

The Guidelines were widely believed to provide a foretaste of what is to come when they appeared on the Internet, but were never formally promulgated.

Expansion of requirements for data localization and purchases of network products

Among other things, the most controversial requirements under the Cyber Security Law are:

– the data localization requirement and security assessment on cross-border transfers of personal information and important data due to operational needs

– the security review for purchases of network products and services by CII operators which may have an impact on national security.

The above two requirements are also elaborated on in the Draft Regulations in relation to CII.

Similar to the Cyber Security Law, the Draft Regulations restate that CII operators must store personal information and important data collected and generated during the course of their operations within China. Where, due to operational needs, it is truly necessary to send such information or data overseas, an assessment must be carried out in accordance with the Security Assessment Measures. Where laws or administrative regulations provide otherwise, such provisions apply.

Furthermore, in a new twist, Article 34 of the Draft Regulations requires that the operational maintenance of CII must be carried out within China. Where, due to operational needs, it is truly necessary to carry out remote maintenance from overseas, the matter must be reported in advance to the competent industrial supervisory authorities/regulatory agencies and the public security department under the State Council. This raises the issue of whether such arrangements will be permitted going forward. No specific approval is mentioned, but it is only a stone's throw away from the authorities simply determining such arrangements are not acceptable in the interests of national security.

Where global contracts are in place, having separate local maintenance will have cost and security implications.

As to the purchase of network products and services by CII operators, the Draft Regulations restate that where CII operators wish to purchase network products and services:

– if they involve key network equipment and specialized cyber security products, then such purchases must conform to laws and regulations, as well as the mandatory requirements under the relevant national standards.

– if such products or services may potentially have an impact on national security, such purchases must undergo a cyber security review and a security confidentiality agreement must be signed with the relevant product or service provider.

Furthermore, Articles 32 and 33 of the Draft Regulations require CII operators to conduct a security review of systems or software developed by outsourcing, and a security review of network products obtained through donation before such systems, software or products become operational and available. The latter seems to be almost anticipating attempts to sidestep the legislation.

Moreover, upon discovery of any security defects, vulnerabilities and other such risks during the use of network products or services, CII operators must take immediate measures to eliminate any risks and/or hidden hazards and major risks involved must be reported to the relevant authorities. Nowhere is there any mention of the cost of addressing such requirements being borne by the Chinese state. It is one thing to hold a State-owned enterprise to this standard, but quite another to hold a privately-owned foreign-invested enterprise to the same standard, against a background of rocketing labour costs in China.

Conclusions

The Draft Regulations at least may have filled out some of the gaps in the cybersecurity legal framework in China. However, in filling in the blanks left under the Cyber Security Law, the Draft Regulations have created new holes and introduced new uncertainties awaiting further legislation, namely the long-awaited guidelines for identifying CIIs, the rules related to qualifications of key personnel of CII operators, as well as the specific rules setting out the relevant requirements for institutions that:

– provide security testing and assessment for CII

– release information regarding security threats

– provide cloud computing and information technology outsourcing services aimed at CII.

It is not possible to reach any other conclusion than the fact that China's legal regime for cyber security protection is becoming increasingly onerous, costly, and potentially disruptive to business. Operators in the relevant industries are facing new compliance challenges each time a new piece of legislation is added to the list, and still do not know definitively what their obligations are. With regard to the specific scope of CII, the Cyber Security Law left the answer to be provided in the Draft Regulations, and now the Draft Regulations have left business waiting for a set of future guidelines to determine who is a CII. Above all, the cost of compliance with the ever-growing laundry list of requirements looks to become even more prohibitive for those in the CII "bucket."

For foreign-invested enterprises that are designated as CII, it would appear to send a clear message that national security concerns take precedence over the ability to operate a business without interruption from government authorities, and little regard seems to have been paid to the need to maintain a reasonable business cost base in China.

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

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

Foreign investor concerns about new security review for network products

On 2 May 2017, the Cyberspace Administration of China (CAC) issued the Network Products and Services Security Review Measures (for Trial Implementation) (Review Measures), which took effect on 1 June 2017. Under the Review Measures, a Network Security Review Office (NSR Office) will be established that will select network products and services that must undergo a network security review (Security Review) placing emphasis on their (and their supply chain's) security, controllability, transparency, and other facets. Network products and services must pass such Security Review in order to be eligible to be procured by certain industries (such as the finance, energy and communications sectors) or by other operators of "critical information infrastructure" (CII), if such procurement may have an impact on national security.

The background to the Review Measures is that the Cyber Security Law adopted on 7 November 2016, taking effect on 1 June 2017, requires that network products and services purchased by operators of CII (the definition of which is somewhat vague and unsatisfactory) must undergo a national security review if such network products and services "might potentially have an impact on national security." Failing to undergo Security Review, the CII operator risks being ordered to discontinue use and/or being subject to quite stiff fines (up to ten times the purchase price). 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 of between RMB 10,000 and 100,000.

Thus, since the promulgation of the Cyber Security Law, 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.

How this regime would look has been one of several major areas of concern for foreign investors arising out of the implementation of the Cyber Security Law. 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 officially suspended, some such protectionist effects were felt.

Unfortunately, the Review Measures leave some critical questions unanswered, 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 CIIs and therefore potentially limited in their procurement options
- whether there will be a protectionist slant in the Security Reviews, such that their practical implementation will make it difficult for foreign or foreign-invested manufacturers to compete
- how intrusive Security Review will be to the proprietary information underlying the network product or service, and concerns about disclosure or leakage of proprietary information.

Perhaps the biggest concern is that the Review Measures do not set out the specific standards and procedures applicable to Security Review.

Uncertain scope of application

Most broadly, Article 2 of the Review Measures states that network products and services are subject to Security Review if they are: (1) "important" and (2) procured for

networks or information systems relating to national security. However, no standards are set forth for defining when either of these elements are met, leaving these elements open to a high degree of subjective interpretation.

Article 8 goes on to state that the "subjects of a review" will be determined by the NSR Office which will, "according to procedures" (which are not defined), determine the specific subjects of a review based on the requirements of the State (i.e., to-be-issued rules), the recommendations of nationwide industry associations, and feedback from users.

The NSR Office, then, appears to have broad discretion, both in terms of deciding which network products and services are subject to Security Review and the procedures by means of which such determination is made, which creates significant uncertainty.

On the upside, it appears that a network product or service is not subject to Security Review until the NSR Office decides that it is.

Failing Security Review

Network products and services subject to Security Review must pass such Security Review or be subject to market access restrictions. In particular, failure to pass Security Review means that key industries such as public communications and information services, energy, transport, water, finance, public services and e-government systems, as well as other operators of CIIs, would not be able to procure such network products and services, if such purchase might have an impact on national security.

What does Security Review involve?

The Review Measures implicitly require that network products and services must be "secure and controllable" and have "transparent" security mechanisms and technology, and require the assessment of the following potential risks:

- Risks implicit to the products and services themselves, as well as the risk that such products or services might be subject to unlawful control, interference or operational shutdowns
- Supply chain security risks occurring during the course of manufacturing, testing, 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 the detriment of network security or the user's interests
- Other risks which may jeopardize national security.

Foreign manufactured goods or goods manufactured by foreign-invested companies in China are more likely to be at risk of failing security review. A number of risks are fairly focused towards national security concerns, for example, whether the products or services might contain functional risks, contain software "back doors," "logic bombs" and other code that may have been deliberately installed with a view to allowing data extraction or remote operation, or that might be at risk of being hacked, infected by viruses, controlled or turned off remotely. Outside of the product or service itself, production and supply chain risks are also considered as well, potentially including 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.

Security Review process framework

The Review Measures set out a multi-layered, multi-institutional approach to Security Review.

The top layer is CAC, the issuer of the Review Measures.

The next layer down is a Network Security Review Committee (NSR Committee) which 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 the NSR Office. The 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, namely third-party institutions and experts, to actually conduct Security Reviews.

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 factors such as a preference for State-owned enterprises or other forms of 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 (however that may be interpreted) redacted.

Government authorities in "key industries and sectors" such as finance, telecommunications, energy, communications and so forth (and therefore potentially others) are responsible for Security Reviews in their respective industries and sectors. The Review Measures fail to answer 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.

Conclusions

The Review Measures contain some important flaws in relation to the new Security Review process, for example:

- No clarity on which products and services are subject to Security Review
- A national security review test that conflates areas already addressed elsewhere in Chinese law and which do not 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 – this essentially creates an environment where foreign-invested companies and foreign manufacturers are players in a game where they have no input on the rules of the game but can be called to the field at any time
- No definitive list of the "key industries" or final definition of operators of CII which will be under an obligation to purchase certified equipment and services, so the list can be extended based on subjective interpretation
- No mention of whether source code can be requested, but an obligation to cooperate with the various reviewing bodies means that if requested, network product and service providers have an obligation to provide it.

All in all, the Review Measures fail to address or alleviate industry concerns that came out of the passing of the Cyber Security Law in relation to Security Review, leaving many of the uncertainties hanging and key issues unanswered.

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

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

China's revised draft data localisation measures

On 19 May 2017, the Cyberspace Administration of China (CAC) released a revised draft of its Security Assessment for Personal Information and Important Data Transmitted Outside of the People's Republic of China Measures (Second Draft Export Review Measures).

The draft emerged just over a week after public comments closed on the first draft of the measures (First Draft Export Review Measures). There was a significant volume of industry commentary, and the Second Draft Export Review Measures do, to an extent, relax some of the more stringent requirements stated in the First Draft Export Review Measures and originally due to become law on 1 June 2017 when China's Cyber Security Law took effect. However, the revised draft measures as set out in the Second Draft Export Review Measures still leave a significant compliance challenge for businesses operating in China. In addition, the test for when a data localization requirement will kick in has not really changed under the Second Draft Export Review Measures, except to remove the words "must be stored within China" and replace them with "must undergo a security review pursuant to these Measures." This does not change the fundamental position that without security review approval and clearance, by definition data cannot be exported so has to be (logically) stored in China.

Delayed implementation of localisation measures

While the Cyber Security Law took effect from 1 June, 2017, the data localisation measures applicable to "network operators" will take effect from 31 December 2018, introducing a grace period that is important for businesses to evaluate their data processing and storage arrangements under the new law.

Implied consent for exports of personal data

A key question arising under the First Draft Export Review Measures was the standard of data subject consent required in order to allow exports of personal data from mainland China to take place. Would an express form of opt-in consent be required, or would a more relaxed standard of implied consent be acceptable? The Second Draft Export Review Measures confirm the latter, providing that acts initiated by data subjects, such as making international telephone calls, sending emails or instant messages to overseas recipients and making cross-border transactions online would be sufficient to imply consent to export.

Understanding the precise scope for implied consent to export personal data from China will be one of the key areas of interest for companies evaluating the impact of the Cyber Security Law. While no doubt a welcome piece of news for those assessing the impact of the localisation requirement, CAC's acceptance of implied consent is yet to be reconciled with the requirement (retained in the Second Draft Export Review Measures) that the export of personal data be "necessary."

No consent required for emergency transfers

The Second Draft Export Review Measures sensibly exempt transfers necessitated by an emergency that endangers the life or property of data subjects.

Material transfers still require official review, but...

- **No 1,000 GB trigger**. The First Draft Data Export Review Measures proposed a number of thresholds which, if triggered, would require network operators to submit to an official data export security review. An export volume of 1,000 GB or more was included amongst the triggers, irrespective of the sensitivity of the information. This has been dropped.
- **Exports operators of critical information infrastructure not deemed material**. The First Draft Export Review Measures had effectively deemed any export of personal data or important data by an operator of "critical information infrastructure" (CII) to be a material export requiring official review.

The Second Draft Data Export Review Measures remove this trigger, meaning that data exports by CII operators are assessed by reference to the same triggers as those by network operators. This is logical and welcome.

The remaining triggers for official review of a data export are whether or not the export involves:

– personal data of more than 500,000 data subjects

– nuclear facilities, bio-chemistry, national defence and military sectors, public health and other such fields, as well as data on large-scale engineering projects, marine environments and sensitive geographical information, or

– system vulnerabilities and security safeguards for key information infrastructure or other such-like cyber security information.

Scope of "Personal Data" expanded to include location and behavioural information: Like the First Draft Export Review Measures, the Second Draft Export Review Measures contain a non-exhaustive definition of "personal data." The new version clarifies that location data and behavioural data may, alone or in combination with other information, be personal data within the meaning of the export review measures.

Review process timeframe and ability to stop exports: Article 10 of the First Draft Export Review Measures had proposed a 60 working day timeframe for regulatory authorities to provide network operators with feedback on export review assessments. This long-stop period has been replaced with a more general requirement for the authorities to provide feedback in a timely manner. This is not very helpful, as it means businesses are not able to plan around a defined timeline framework. The version of Article 10 in the Second Draft Export Review Measures includes a materially revised stipulation that reviewing

authorities shall direct that an export be stopped if any of the matters listed in Article 9 are identified in relation to an export, namely:

- the export would violate laws, regulations or departmental rules
- data subjects have not consented to the export of personal data
- the export is likely to prejudice the public or national interest
- the overseas transmission of data would jeopardise the security of national politics, military affairs, society, scientific and technological matters, information, ecology, resources, nuclear facilities and so forth
- any other situations where CAC, the Ministry of Public Security or the Ministry of State Security and so forth determine that the export cannot take place in accordance with law.

The last two are new in the Second Draft Export Review Measures. It is hard to envisage how a transfer overseas of data could harm "ecological" or even "resource" security, but we take this as an implicit reference to information, for example on ecological damage or abuse of natural resources which are not at the level of state secrets (noting the previous cases where China determined that the location of natural resources was determined to be State secrets in the hands of certain foreign individuals). There is a still a carve-out for State secrets in Article 14 which appear to remain regulated under the rules governing State secrets, including criminal penalties in certain cases.

Conclusions

The changes introduced by the Second Draft Export Review Measures make a few sensible technical adjustments and include a temporary reprieve from China's new data localisation measures through to 31 December 2018. Given the typical lead times for technology procurement, most businesses will be forced to make decisions on their processing arrangements long before this date materialises. However, the broad thrust of the First Draft Export Review Measures has not changed nor has the scope encompassed by the key definition of "network operators" got any clearer.

For many companies, the main practical benefit of the grace period will be to enable time to gain a better understanding of the standards of export review that the authorities will apply and assess alternative structuring approaches that, for example, the allowance for implied consent to data subject-initiated exports of personal data, may generate, such as requiring data subjects to send an email to the proposed export destination address to confirm their consent.

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

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

First Cyberspace Court set up in China: the Chinese judiciary enters the digital age

China's first Cyberspace Court was inaugurated on 18 August 2017 in Hangzhou, Zhejiang Province. This new court is expected to handle all Internet-related disputes in all districts of Hangzhou through a fully digitalized, online procedure. The establishment of a specialized cyberspace court in China's internet capital Hangzhou is an encouraging step for the Chinese internet sector as well as for intellectual property (IP) owners: it promises a more flexible procedure and higher quality judgments, handed down by specialist judges.

The new Cyberspace Court draws on the existing experience of the Hangzhou courts, including the Cyberspace Court's predecessor – the pilot e-commerce online tribunal. The courts and tribunal have collectively dealt with the largest – and still growing – number of Internet-related cases in China: from 600 cases in 2013 to more than 10,000 in 2016. This large number of internet-related cases is mainly due to the fact that some of China's largest internet companies are established in Hangzhou: companies such as Alibaba and NetEase have their corporate headquarters in the city.

Currently, the understanding is that this new cyberspace court will largely follow the procedure used by its predecessor, the pilot e-commerce online tribunal. The procedure would be entirely online; from the filing and mediation stage, to the publication of the judgment, and would even include the option to have online video-conference hearings. The bench of the Cyberspace Court would consist of judges that have already obtained experience with Internet cases. The Cyberspace Court has jurisdiction over:

- Online copyright disputes (including the unlawful dissemination of films, music and other copyrighted works)
- Online defamation
- Domain name disputes
- E-commerce disputes (including purchase contract disputes, product liability disputes, service contract disputes)
- Online loan contract disputes.

The first case heard after this official launch was a copyright dispute where the author of a novel sued an online platform operator for making available the novel to the public. It was reported that the hearing was conducted by video-conferencing linking up the respective parties in Hangzhou and Beijing. The transcription was done by voice-recognition technology. The hearing took 20 minutes to finish (the parties agreed to mediate), and the parties simply clicked "Accept" to confirm the transcript.

The Cyberspace Court is hailed as a positive development for China's e-commerce sector, in which the piracy of copyright works and the sale of counterfeits is still rampant. The Hangzhou Cyberspace Court is considered a pilot project, and more cyberspace courts may be established throughout the country. We hope that cyberspace courts may bring the same professionalism to Internet-related litigation as the specialized IP Courts did with IP litigation in China.

Helen Xia
Partner, Beijing
T +86 10 6582 9580
helen.xia@hoganlovells.com


Time Flight Destination Gate Status
17:25 A 1106 Dalian Est 20:20
18:15 K 659 Kuala Lumpur Boarding
18:20 Z 634 Guangzhou Est 19:25
18:50 Shanghai/SHA Est 19:30
19:05 O 1292 Shanghai/PVG Cancelled
19:10 Melbourne Final Call
19:15 Mumbai Final Call
19:15 X 709 Denpasar Final Call
19:20 E 1822 Taichung Boarding
19:20 I 920 Taipei Boarding
19:20 Z 4050 Sydney Boarding
19:25 R 872 Taipei
19:25 X 464 Taipei Boarding
19:30 J 119 Manila
19:30 Shanghai/PVG Boarding
19:35 A 452 Kaohsiung
19:40 Delhi
19:45 A 428 Chengdu
19:50 AK 6803 Kota Kinabalu Est 19:40
19:50 Shenyang
19:55 Taipei
19:55 Singapore
20:00 Beijing Est 21:00
Time Flight Destination Gate Status
20:00 A 622 Hangzhou
20:05 CI 642 Taipei
20:05 A 895 Singapore
20:10 Z 7431 Medan Est 20:00
20:15 O 304 Beijing
20:25 Shanghai/PVG
20:30 K 696 Singapore
20:30 Brisbane
20:35 R 2965 Singapore Est 21:15
20:40 Z 3090 Nanning
20:40 A 869 Ho Chi Minh
20:40 O 192 Taichung
20:45 Mumbai
20:45 Xiamen
20:45 G 607 Bangkok
20:50 D 3862 Bangkok
20:55 Guam
20:55 Sydney
21:00 R 858 Taipei
Taipei
K 679 Kuala Lumpur Est 20:55
X 107 Auckland
Time
21:10
21:10
21:20
21:25
21:30
21:30
21:40
21:40
21:40
21:50
21:50
21:55
21:55
22:00
22:10
22:15
22:15
22:20
22:25
22:25
22:40
22:45
22:45
22:45
22:50

China to embrace and accommodate the sharing economy

On 28 February 2017, the National Development and Reform Commission (NDRC) issued the Sharing Economy Development Guidelines (Consultation Draft) (Guidelines) for public comment in March 2017. The Guidelines set out broad instructions to Chinese regulators to embrace and accommodate the sharing economy

The guidelines call for NDRC together with other government departments to establish, within the framework of a joint inter-ministerial meeting, a sharing economy expert consulting committee to strengthen unified coordination on the sharing economy, clearly set out the lead department and responsible bodies within the various sub-fields, promptly evaluate and solve regulatory issues that arise, and put forward reasonable suggestions.

The Guidelines come at a time when the sharing economy is rapidly developing in China but in an environment of regulatory uncertainty, with pioneering companies (and their investors) often on pins and needles that their experimental business models will be hindered or even killed off by:

- ill-fitting existing regulations being applied to them, as if they were traditional businesses (for example, if hotel regulations were to be applied to the short-term subleasing of residential apartments)
- by passage of new regulations that address their business sector, but are out-of-step with the features of the sharing economy (for example, earlier draft regulations that proposed that only commercially registered vehicles could be hailed under ride-hailing platforms)
- protectionism in favor of the traditional industries that the sharing economy disrupts (for example, by limiting the number of participants who may share in the sharing economy, like an earlier proposal by the transportation ministry to limit the number of drivers who could accept work through ride-hailing platforms)
- by a lack of regulations that might be needed to allow sharing economy businesses to achieve certain types of compliance and/or effectively compete with traditional businesses (for example, if existing regulations or practice do not provide an effective or cost-effective means of participation in the VAT system, or other operational issues).

It is not unusual that such challenges exist, as change is often hard-fought and hard-won. Disruption can be unpleasant when introduced. New business models can be difficult to anticipate and prepare for in advance.

The Guidelines will not change that, and certainly not in one stroke. But, very importantly, what the Guidelines do set out to accomplish is to reset the baseline attitude that government agencies in China should adopt when encountering the sharing economy, and the overall message, while not stated in these exact words, may be interpreted as: find a way to make it work.

In the words of the Guidelines themselves, government agencies should, as guiding principles:

- permit and encourage all types of market actors to actively explore the new service offerings and new modalities of the sharing economy
- accelerate the formation of a policy environment that accommodates the special characteristics of the sharing economy
- strengthen tailored field-specific guidance
- lower market entrance thresholds
- preserve fair competition, particularly by regulating and preventing platform operators' anti-competitive conduct
- raise the level of de-regulation, de¬centralized regulation and optimization of government services

– reduce the policy risk on the development of the sharing economy.

In addition to these pro-sharing economy general principles, participants in the sharing economy may take some comfort in Guidelines provisions that appear to address the "pins and needles" concerns first outlined above. For example, the Guidelines specify that government authorities should:

– **on existing regulations**: Give full consideration to the cross-industry nature of the sharing economy and avoid using old measures to govern new business models; reasonably classify different models and regulate accordingly, avoiding one-size-fits-all approaches

– **on new regulations**: Maintain a "bottom-line" approach to regulation that strictly standardizes entrance requirements when business models implicate the safety of life or property, social stability, cultural security or risk to finances, but otherwise clear away licensing and registration requirements that restrict the development of the sharing economy and further liberalize conditions that are restrictive to market entrance by contributors of resources

– **on protectionism**: Break industry barriers and regional restrictions

– **on new approaches to enable and stimulate the sharing economy**: Make government and public data and resources available, increase government purchasing of sharing economy products and services, delineate obligations and liabilities as between platforms and those contributing resources, research insurance policy to facilitate insurance or other market mechanisms for protection of consumers, research and perfect measures appropriate to the sharing economy for allowing non-employee flexible working participants to pay into the social insurance system, research and perfect measures to enable tax payments and electric VAT invoices.

Undoubtedly, it will take time to actually bring about the reforms proposed in the Guidelines, and there is always risk that some aspects will never come to fruition, but the hope for now at least is that the Guidelines, if and when enacted, will bring about an atmosphere conducive to innovation, and that the NDRC-led joint inter-ministerial committee on the sharing economy will be an effective advocate across regulatory departments to ensure the healthy development of the sharing economy across China.

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

Decrypting China's first crack at a Cryptography Law

On 13 April 2017, the Office of the State Commercial Cryptography Administration (OSCCA) published a draft of the Cryptography Law (Draft Cryptography Law) for comment on its website. The Draft Cryptography Law marks a clear stepping up of the regulatory emphasis in the area of encryption and will, once passed, serve as the most authoritative source of law in the area of cryptography in China.

Prior to the newly released Draft Cryptography Law, the main rules governing encryption equipment and technology in China were the Commercial Encryption Administration Regulations, which are now 18 years old, and four major relevant sets of rules passed by OSCCA between 2005 and 2007 governing commercial encryption manufacturing, sales, use and scientific development, respectively.

Since then, the need for further legislation has been recognized, and this year the State Council listed the promulgation of a Cryptography Law in its 2017 legislative work plan as one of the "items with an immediate and urgent need for comprehensively deepening reform."

The Draft Cryptography Law defines "cryptography" as the items and technologies which are used to encrypt or certify the data and other information through the application of certain algorithms. The scope of the law is broad, covering all aspects of the development and supply chain for cryptographic products and services, from scientific research, manufacturing, use in business operations, importation and export, testing, certification, supervision and management and other such like activities.

OSCCA and its respective local branches are tasked with administering all aspects of cryptography related work under a system of unified leadership, which the Draft Cryptography Law makes a specific point of stating is ultimately vested with the Chinese Communist Party. This underscores the somewhat heavy political and State security overtones of this area.

Classifications of cryptography

The Draft Cryptography Law categorizes cryptography products and services into three types:

- core cryptography products and services (Core Cryptography)
- general cryptography products and services (General Cryptography)
- commercial cryptography products and services (Commercial Cryptography).

Each category of cryptography products and services is subject to different use restrictions and regulation, with some of the key differences discussed below.

State secrets

The former two types can be used to protect State secrets, while the latter can only be used to protect information not deemed to constitute State secrets. The restriction on commercial encryption devices being used to protect state encryption technologies secrets is not a new concept. Presumably, the concern is that commercial encryption technology is less reliable and decryption keys may be more readily available. Article 2 of the Commercial Encryption Administration Regulations expressly defines commercial encryption as technologies not used for protection of State secrets.

Import and export

Core Cryptography and General Cryptography cannot be exported.

Commercial Cryptography may be imported or exported, subject to having obtained government approvals. Under the current Commercial Encryption Administration Regulations, such approvals have to be obtained from OSCCA, with the importation of foreign Commercial Cryptography further regulated by the Catalogue for the Administration of the Importation of Encryption Products

and Equipment Incorporating Encryption Technology issued by OSCCA and the General Administration of Customs (GAC). The latest version of that catalogue is dated 31 December 2013 and lists the following 9 categories of products and equipment as being regulated under it: (1) electrostatic photosensitive multi-functional integrated encrypted fax machines (which can be connected to automatic data processing equipment or networks); (2) other multi-functional integrated encrypted fax machines (with one or more of printing and copying functions); (3) other encrypted fax machines (can be connected to automatic data processing equipment or network); (4) cordless encrypted telephones; (5) other encrypted telephones; (6) optical communication encrypted routers; (7) non-optical communication encrypted Ethernet switches; (8) non-optical communication encrypted routers; and (9) encryption machines and encryption cards (not including digital TV smart cards, Bluetooth modules, or dongles used for the protection of intellectual property rights).

The Draft Cryptography Law provides a slightly different regime, bringing into play one more government authority, i.e. the Ministry of Commerce (MOFCOM), whereby both the export and importation of Commercial Cryptography will be subject to a permit from MOFCOM and OSCCA. MOFCOM, together with OSCCA and GAC will publish a list of Commercial Cryptography products and services which are subject to restrictions in relation to imports and exports.

Currently, imported Commercial Cryptography products cannot be sold in the China market and can only be imported for restricted use by foreigners, representative offices, and foreign-invested enterprises for internal communications with their parent companies with an import permit and approval from OSCCA. The Draft Cryptography Law does not address this point. Presumably, the restrictions on sale found in existing legislation will remain in place or will otherwise be carried forward.

Sale and usage of domestic Commercial Cryptography

Article 11 of the Draft Cryptography Law sets out the rules with respect to domestic sales and use of Commercial Cryptography, such that the sale of and use of Commercial Cryptography products as well as the provision of Commercial Cryptography services by an entity in China (e.g. repairs) will require a permit from OSCCA. OSCCA will formulate and publish a catalogue of (domestic) Commercial Cryptography products and services. The Catalogue of (Domestic) Commercial Encryption Products previously issued by OSCCA dated 22 March 2017 contains 1,817 products approved for sale in the Chinese market. It is unclear, given how recent in origin this is, whether the plan is to replace this with a new catalogue. Chinese citizens and legal persons are currently allowed to use Commercial Cryptography products as long as such use is not for protecting information relating to state secrets.

What is very clear from the above two catalogues is that the distinction between imported and domestically produced encryption products is likely to remain under the Draft Cryptography Law, with no relaxation on the heavy restrictions on imported products in sight.

Link to the Cyber Security Law

Adopted on 7 November 2016 and in effect since 1 June 2017, the Cyber Security Law designates certain systems as "critical information infrastructure" (CII), which are subject to a number of specific requirements under the Cyber Security Law. One of the key requirements is the obligation under Article 35 to submit purchases of network products and services which may potentially have an impact on national security to a national security review before purchase by a CII.

The ultimate definition of what constitutes a CII operator will be issued by the State Council, but CII 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, experience a loss of functionality or data leakage.

Additional rules implementing the Cyber Security Law state that "networks which relate to national security and important network products and services purchased for information systems" are subject to a network security review, which leaves it open as to what are "networks which relate to national security" and, more worryingly, "important network products and services."

Cryptography will undoubtedly play an important role in security systems for CIIs. Articles 12 and 18 of the Draft Cryptography Law relate directly to the use of cryptography by CIIs. They state that CIIs must use cryptography to protect their systems and must plan, build and operate cryptology protection systems in accordance with laws, regulations and mandatory provisions in standards relating to cryptography in tandem. Article 18 goes on to say that the State will use a tiered review system to categorize the security status of cryptography products used in CIIs, and where they impact, or are likely to impact state security, and will carry out security reviews of cryptography products and services and systems based on state review requirements.

In short, it seems almost a given that even domestically manufactured cryptography products are going to be subject to a security review process where these is a potential impact on national security (or even where classified as "important network products"). Thus, it seems highly unlikely that any foreign-made Commercial Cryptography product will be permitted to be used in the systems of any CII, as they are currently banned from sale in China in any event. What remains to be seen is whether any foreign-invested enterprise in China that is currently using a foreign manufactured Commercial Cryptology product (with an import permit and OSCCA approval to use) will be allowed to continue to use it after it has been designated a CII.

Link to the "secure and controllable" concept

The Draft Cryptography Law has come out amongst a backdrop of various efforts by China to tighten the regulation of overseas-originated technology on several fronts with the stated objective of making technology "secure and controllable." The term "secure and controllable" has found its way into the National Security Law, adopted on 1 July 2015, which pre-dated the Cyber Security Law. Already the rolling out of the concept has had a very significant impact on foreign-invested companies in sectors providing equipment and services to the banking industry in particular, which previously were not subject to policy restrictions. National security review procedures under the Network Product Review Measures may become the legal basis for the Chinese government to wade into the overseas-sourced technology and equipment supply sectors in an even more intrusive manner. The Draft Cryptography Law provides no evidence to the contrary and, in fact, points clearly in that direction.

Compulsory duty to cooperate with the Chinese authorities on investigations

Article 20 of the Draft Cryptography Law provides that Chinese authorities including the People's Procuratorate, the Ministry of Public Security (MPS) and the Ministry of National Security (MNS) are authorised to require telecommunications operators and Internet services providers to cooperate and provide decryption technical support where required due to national security concerns or investigations into criminal offences, and the latter must keep such cooperation confidential. This provision adds to the already fulsome set of powers the Chinese government authorities have to investigate

information transmitted through telecom services and the Internet. The respective industry regulators may impose a monetary fine (the amount is not stated) on the operators or providers and the persons directly in charge and other directly responsible persons for failure to cooperate or provide decryption technological support or for "disclosing the relevant circumstances." In serious cases, the MPS or MNS may impose criminal detention ranging from five to fifteen days on persons directly in charge and other directly responsible persons. Unlike some of their overseas counterparts, telecoms operators and Internet services providers in China do not have the right or option of challenging or refusing to cooperate in China. Article 27 seems to go even further, providing that relevant organisations and individuals must cooperate when the cryptography departments are carrying out their regulatory and administrative duties.

Clarifying and strengthening of OSCCA's surveillance

The Draft Cryptography Law grants OSCCA sweeping and intrusive investigatory powers. Under Article 29, OSCCA may:

- conduct on-site investigations in places where cryptology products or services are manufactured, sold, imported or exported, examined, certified or used
- make enquiries of the main persons in charge or other relevant persons in enterprises or institutions manufacturing, selling, importing and exporting, examining, certifying and utilizing encryption products or services
- access and copy relevant contracts, bills of exchange, accounting books and other materials
- seal up or confiscate unlawful facilities for manufacturing, operating, importing and exporting,

examining, certifying or using cryptography products or services

– seal up places used for the unlawful manufacturing, selling, importing and exporting, examining, certifying and utilizing of cryptography products or services.

In short, OSCCA can do basically whatever it deems necessary for the purposes of enforcing its rights as the regulatory authority in charge of cryptography (including investigating foreign-invested enterprises which have already obtained an import permit and OSCCA approval to use), again pointing to how China sees cryptography as essentially an extension of State secrecy and national security administration. The only concession to abuse of powers and so forth by OSCCA officials is set out in Article 39 where it suggests that they will be subject to administrative disciplinary measures in accordance with law.

Conclusions

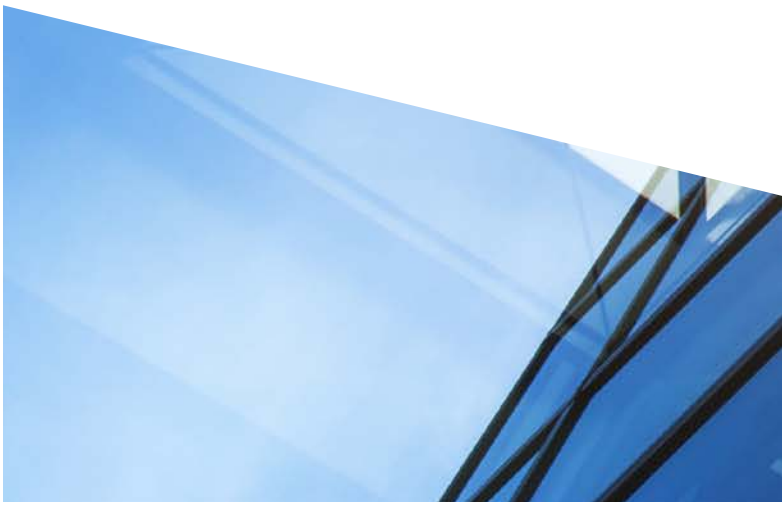
The Draft Cryptography Law is the first comprehensive law in the cryptography field in China. It is heavily politicized, with over half of the 43 articles relating to government supervision and liability for breach; many of the provisions are high-level 'government speak' or administrative and inward-looking in nature.

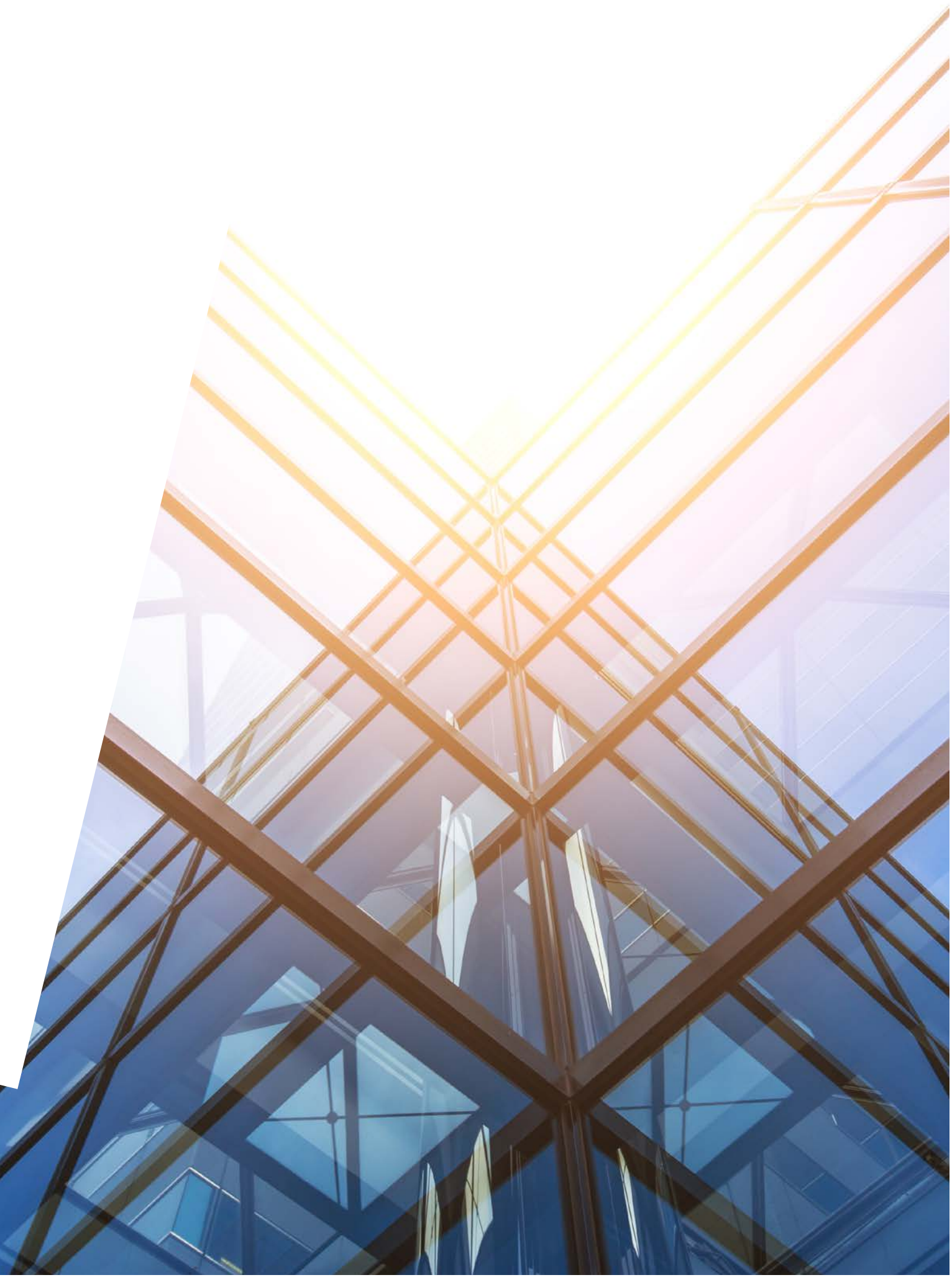
Perhaps the most worrying, albeit unsurprising aspect of the Draft Cryptography Law is the way it overtly leaves telecom operators and Internet content providers (and arguably anyone else in China) with little choice when government authorities demand decryption support. Effectively this allows government to drive a coach and horses through the regime for protecting data privacy in the name of investigating national security concerns or alleged crimes. The potential for abuse is obvious: if someone wants to say chase down a certain individual, all they have to do is convince someone in the MPS or MNS to use their powers to find that person's data trail and the relevant telecoms or Internet service providers have to decrypt the traffic on request (or possibly supply the decryption key to the Chinese authorities to allow them to decrypt future traffic). This means that the Chinese State security organs essentially have access to decrypted private correspondence on demand.

For foreign cryptography technology providers, it basically means they are still shut out of Chinese cryptography product market for the simple reason that they cannot sell into China except to foreign-invested enterprises and other limited foreign organs with an import permit and OSCCA approval to use. Even if they were to get a permit to manufacture or sell locally, they may find the concept of having to allow their customers to provide the Chinese government with decryption keys on demand difficult to swallow.

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

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





SFC proposes baseline cyber security requirements for Internet trading in Hong Kong

On 8 May 2017, the Hong Kong Securities and Futures Commission (SFC) issued a paper containing proposals to introduce cyber security guidelines under the Securities and Futures Ordinance (SFO) applicable to Internet brokers (Cyber Security Consultation Paper).

Background

The Cyber Security Consultation Paper reflects a sharpening of focus by the SFC on cyber security issues. The SFC notes that in the 18 months up to 31 March 2017, 12 licenced corporations reported 27 cyber incidents – the majority involving access to clients' trading accounts. These incidents resulted in unauthorised trades to the value of HK$110 million. The Hong Kong Computer Emergency Response Team Coordination Centre is reported to have handled 6,058 cyber security incidents in 2016, an increase of 23% from 2015.

The Cyber Security Consultation Paper highlights the prevalence of a particular form of "pump and dump" scheme in which hackers gain unauthorised access to internet trading accounts and use the cash and securities in these accounts to fund the purchase of penny stocks targeted by the hackers. The hacked accounts are used to pump up the prices of these penny stocks, following which the hackers dump the stock, causing significant losses to the hacked accounts.

Against this backdrop, the SFC conducted a 2016 cyber security review which consisted of fact finding surveys, on-site inspections of brokers' technology controls, discussions with vendors to evaluate the feasibility, cost and benefits of various systems, and a benchmarking exercise against local and overseas regulations and market practices. Based on its findings, the SFC has proposed a framework of "baseline requirements" which licensed and registered persons are expected to comply with.

Existing SFC controls

Cyber security risks are currently addressed to a limited extent in the Code of Conduct for Persons Licensed by or Registered with the SFC (Code of Conduct).

Paragraph 18 and Schedule 7 of the Code of Conduct contain a set of requirements for mitigating security risks which apply to electronic trading (including internet trading) of securities and futures contracts that are listed or traded on an exchange. The Cyber Security Consultation Paper proposes to extend these provisions to electronic trading of securities and futures contracts that are not listed or traded on an exchange.

The Code of Conduct requirements are stated in general terms that reflect a principles-based, "risk-based" approach, rather than imposing specific technical requirements on brokers. For example, the Code of Practice requires a licensed or registered person to ensure the trading system's "reliability, security and capacity" and have "appropriate contingency measures" in place (paragraph 18.5), and Schedule 7 of the Code of Practice requires, among other things, appropriate governance and accountability for systems, testing of systems before deployment, prompt reporting of material service interruptions, reliable authentication techniques and appropriate operating controls to prevent and detect cyber attacks.

In addition to the Code of Conduct, the SFC has over the years elaborated on a number of security and cyber risk management themes in the following circulars and publications:

- Circular on Cybersecurity (23 March 2016)
- Tips on Protection of Online Trading Accounts (29 January 2016)
- Circular on Internet Trading – Internet Trading Self-Assessment Checklist (11 June 2015)
- Circular on Mitigating Cybersecurity Risks (27 November 2014)

– Circular on Internet Trading – Information Security Management and System Adequacy (26 November 2014)

– Circular on Internet Trading – Reducing Internet Hacking Risks (27 January 2014).

As with the Code of Conduct, the SFC's Circulars tend to be principles based rather than prescriptive in their requirements on cyber security.

However, it is fair to say that the SFC has imposed fairly limited technology risk management (TRM) requirements compared to the requirements imposed by the Monetary Authority (MA) on its licensed banks, restricted licence banks and deposit-taking companies. The MA's overarching TRM principles are set out in Module TM-G-1 (General Principles for TRM) and Module TM-E-1 of the Supervisory Policy Manual (Risk Management of E-banking), and more specific guidance on the security measures expected of internet banking businesses are set out in various Circulars. In turn, the MA moves forward with a Cyber Fortification Initiative that would further advance the regulation of cyber security risks in the banking industry.

The MA also regulates the outsourcing activities of authorised institutions by way of Module SA-2 of the Supervisory Policy Manual. By contrast, the SFC imposes very little control over outsourcing by market participants, although it has endorsed the internationally recognised "Principles on Outsourcing of Financial Services for Market Intermediaries" published by the International Organisation of Securities Commissions.

Proposed baseline requirements

The proposed baseline requirements are divided into three categories:

– protection of clients' internet trading accounts

– infrastructure security management

– cybersecurity management and supervision.

Of particular note is the requirement for two-factor authentication (2FA) (i.e., requiring two forms of authentication for account access, such as a password plus a hard or virtual token). The Cyber Security Consultation Paper notes that a number of recent hacking incidents have occurred as a result of brute force attacks using applications that decode single or dual passwords, but there have been no reported hacking incidents in cases where 2FA has been enforced. 2FA has long been a requirement of the MA for internet banking systems, and the Monetary Authority of Singapore (MAS) went further in December 2016 to extend this requirement to all online trading accounts with the exception of institutional investors.

The Cyber Security Consultation Paper proposes that brokers would only need to implement 2FA in respect of account logins, on the basis that the use of 2FA for placing trading orders could adversely impact the timeliness of order execution. Moreover, brokers would have discretion in deciding what type of 2FA solution is implemented as long as the solution is "commensurate with its business model."

Other noteworthy baseline requirements proposed in the Cyber Security Consultation Paper include:

– the requirement to evaluate software security patches or hotfixes released by software providers on a timely basis and, subject to evaluation, to implement them within one month from release

– encryption of sensitive information such as client login credentials and trade data during transmission between internal networks and client devices, recognising that encryption of all data would significantly slow down transmission which could be contrary to investors' interests

– the requirement to conduct a review of user-access to systems on at least an annual basis

– the need to notify clients of account activities such as system login, password reset, trade execution,

third party fund transfers and changes to account information, with clients being allowed to opt-out of "trade execution" notifications only

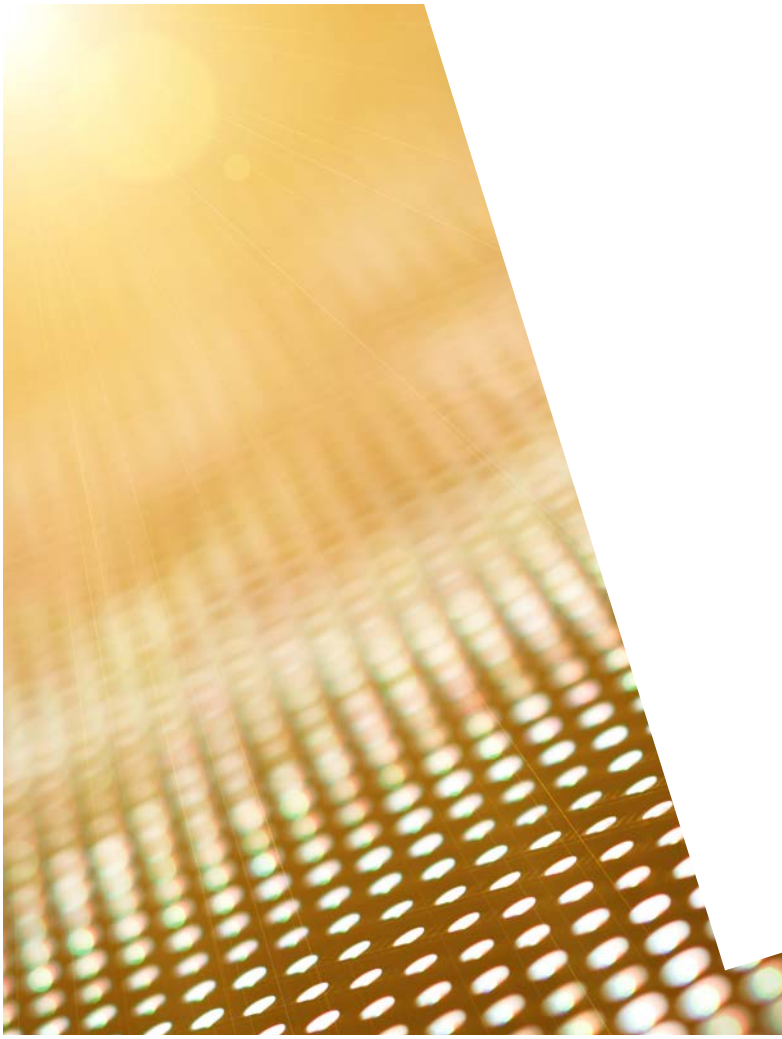
- the back-up of business records, client and transaction databases servers and supporting documentation in an offline medium on at least a daily basis
- the requirement to enter a formal service level agreement with service providers engaged for internet trading, specifying the terms of service and responsibilities of the provider, and ensuring that the services will enable the licensed or registered person to comply with the Code of Conduct and the baseline requirements.

The last requirement is much less prescriptive than the MA's outsourcing guidelines which specify in considerably more detail the required content of outsourcing agreements. The MA also requires notification of certain outsourcing arrangements, whereas there is no equivalent obligation for brokers.

While the proposed new measures are more prescriptive than the SFC's existing security requirements, and will go some way towards bridging the gap between the MA's and the SFC's approach to cyber security, there is still the recognition that brokers are driven by the need to remain competitive and any measures that overly compromise performance and speed would clearly be met with resistance, and could be contrary to investors' interests. The encryption of communications between brokers and clients, for example, is a challenging one, as the introduction of encryption controls will inevitably impact the speed of data transmission. By proposing to limit encryption, at this stage, to sensitive information passing between brokers and their clients and not, for example, inter-broker communications, the proposals appear to be taking a risk-based approach that address the specific problem of the "pump and dump" schemes uncovered by the SFC's research, which involved client-access passwords being compromised.

More broadly, the requirements set out in the Cyber Security Consultation Paper are stated to be baseline requirements, and many of them would afford a degree of flexibility in implementation. The effect of the baseline requirements, if implemented, will be to better protect investors and also to 'level the playing field' for brokers in adopting cyber risk management measures.

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



New generic top level domains for China

On 2017, the Ministry of Industry and Information Technology (MIIT) granted licenses to a number of legacy and new generic Top Level Domains (gTLDs) allowing them to be sold and operated within China. This is in line with a continuing trend towards greater openness to the domain name world on the part of China.

China opened up to greater engagement with the domain name market subsequent to MIIT's revision last year of the Measures for the Administration of Domain Names from 2004. The rules implemented pursuant to this revision clarified that, in order to host a website in China, the associated domain name must be registered with a registrar in China and imposed fines of RMB 30,000 for violation of this rule. They did not, however, prohibit the ownership of domain names by Chinese nationals registered outside the country.

The new gTLD .XYZ was one of the first to be awarded a license by MIIT in December 2016 and Chinese registrants accounted for one third of all of its domain names even before its accreditation. Other Top Level Domains (TLDs) to have received licenses so far include .CN, .CHINA, .COMPANY, .WEBSITE and .WANG.

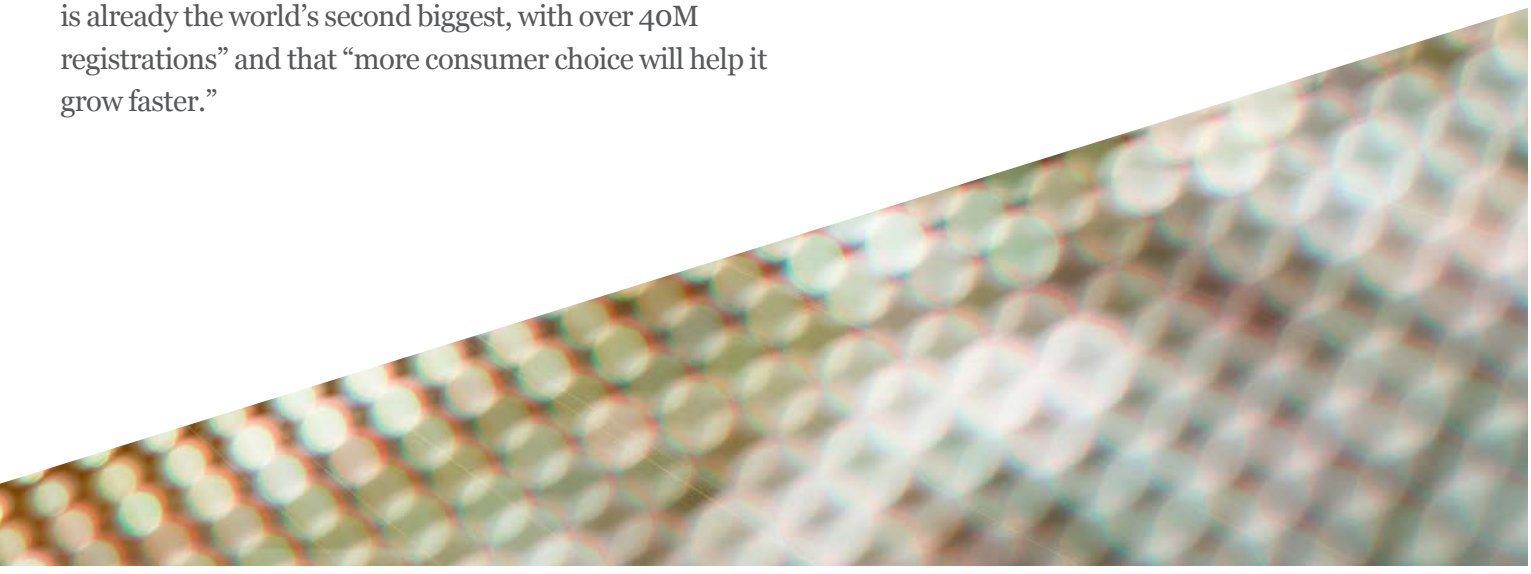
Most recently, MIIT awarded licenses to the legacy gTLDs .INFO, .PRO and .MOBI, as well as the new gTLDs .RED and .KIM.

Roland LaPlante, Senior Vice President of Afilias, which runs the .INFO, .PRO, .MOBI, .RED and .KIM TLDs was quoted as saying that "China's domain name market is already the world's second biggest, with over 40M registrations" and that "more consumer choice will help it grow faster."

As well as aiming to give more choice to Chinese domain name owners, registrars are of course keen to tap into the vast Chinese domain name market. Afilias has stated that it believes making its five domain name extensions available to Chinese businesses and other Chinese domain name users will allow Chinese businesses to enhance their global online presence as well as helping them to "compete in today's marketplace."

It will be interesting to see whether MIIT will in the future award similar licenses to other registries and for other TLDs.

David Taylor
Partner, Paris
T +33 1 53 67 47 47
david.taylor@hoganlovells.com



Hong Kong to launch statutory "do-not-call" register targeting P2P telemarketing

Following the completion of the public consultation on strengthening regulation of person-to-person telemarketing calls (P2P) in July 2017, the Commerce and Economic Development Bureau (Bureau) submitted its report on the public consultation to the Legislative Council Panel on Information Technology and Broadcasting on 9 April 2018.

The public consultation paper, which was issued to the public and various bodies (including relevant industry stakeholders, District Council secretariats, and other relevant bodies such as the Consumer Council and the Office of the Privacy Commissioner for Personal Data), focused on gauging public views on whether regulation on P2P calls should be strengthened by statutory or non-statutory regimes. In particular, three options to enhance regulation of P2P telemarketing were proposed: improving trade specific self-regulatory regime, promoting the use of call-filtering applications in smartphones, and establishing a statutory "Do-not-call Register" (DNC Register).

Key findings in the public consultation report

- A vast majority of 89% of individuals who put forward their views have expressed support towards legislative regulation of P2P telemarketing. Amongst these individuals, 86% are in favour of adopting a DNC Register.
- The Bureau proposes the establishment of a DNC Register to be administered by the Office of the Privacy Commissioner for Personal Data. The DNC Register prohibits telemarketers from making P2P calls to phone numbers on the register unless proven that the call recipients' prior consent has been obtained.
- The DNC Register is anticipated to include clear definitions of telemarketers and telemarketing, procedures for phone users to register or de-register their numbers, identification and suitable authorisation of the implementation agency, ways to make the DNC Register available to telemarketers, handling of personal data and establishment of enforcement mechanisms and legal responsibilities. Suggestions on incorporating criminal liability sanctions will be further discussed with the Department of Justice during the law drafting process.
- Suggestions to assign designated telephone number prefixes to telemarketers and to operate sector-by-sector registers were rejected by the Bureau as these can be easily circumvented by telemarketers choosing to call from numbers without these prefixes or from overseas and that there are no clear delineations or definitions of most business/trade "sectors" in Hong Kong.
- There will be no differentiation between "warm calls" (calls whereby the caller from the company is able to identify the call recipient) and "cold calls" (calls generated from computer call machines whereby the caller does not know the recipient) under the statutory regime. However, the Bureau explains the more appropriate approach for telemarketers wishing to make "warm calls" is to obtain phone users' prior consent in receiving such "warm calls."
- Pending the introduction of the statutory bills on the DNC Register, the Bureau suggested non-statutory measures to alleviate interim concerns of the public regarding P2P telemarketing. These include enhancement of existing self-regulatory regimes, enhancement of call-filtering mobile applications and promoting public education on using call-filtering mobile applications.
- Provisions will be made to clearly define the scope of P2P calls to prevent important calls (e.g., from hospitals or important public service providers) be inadvertently caught by the statutory regime.

How will this impact the use of P2P telemarketing in Hong Kong?

The proposed DNC Register represents a shift in the legislative attitude and approach towards regulation of P2P telemarketing in Hong Kong and will help bring Hong Kong's regulation in this area in line with major jurisdictions around the world.

In fact, the operation of a DNC Register is not a new regulatory measure in Hong Kong. Under the Unsolicited Electronic Messages Ordinance (Cap. 593), since 2007 the Communications Authority had established three registers to regulate the sending of unsolicited fax, short messaging service (SMS) messages and pre-recorded telephone calls.

Tighter regulation and compliance requirements are envisaged to apply, and also the possibility of imposing stricter penalties for non-compliance. Businesses engaged in the use of P2P telemarketing should be alert to on-going changes in legislative development on P2P telemarketing regulations and in particular on the establishment of the DNC Register. Businesses should also consider conducting reviews of their own telemarketing policies to determine how these impending legislative changes may affect their practices, and whether it will give rise to new or greater exposure.

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

Isolde Tsukabayashi
Trainee Solicitor, Hong Kong
T +852 2840 5646
isolde.tsukabayashi@hoganlovells.com

What's next for robo-advice? SFC consults on proposed guidelines on online distribution and advisory platforms

With the rapid development of technology, there is an increasing trend of intermediaries providing investment services and distributing investment products over the internet. Whilst the Securities and Futures Commission (SFC) has published regulations which govern the conduct of intermediaries registered or licensed with the SFC, these regulations were drafted to cater for offline situations. In light of the increasing reliance on online platforms for sale and distribution of investment products, and the additional risks involved with these new business models, the SFC proposes to introduce a set of guidelines applicable to all persons licensed or registered with the SFC in conducting regulated activities, including order execution, distribution and provision of advisory services. On 5 May 2017, it launched a three-month consultation period on the proposed Guidelines on Online Distribution and Advisory Platform (Guidelines).

The proposed Guidelines provide guidance and clarity on existing business conduct and suitability requirements which apply to persons licensed by or registered with the SFC, and compliance with these requirements in an online context. They also contain new proposed requirements in respect of complex products for further protection of investors. The Guidelines include a three-stage requirement which online platform providers licensed or registered with the SFC are required to consider:

- general requirements which all online platform providers should take into account and comply with
- suitability requirements under the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission (Code of Conduct) which will be triggered if there is "recommendation" or "solicitation" by intermediaries, and how suitability obligations may be discharged
- new suitability requirements applicable to "complex products" even if there is no "recommendation" or "solicitation" by intermediaries.

The SFC explains in the consultation paper its view that the complexity of products does not directly correlate with the level of risk involved. That is, simple products can be risky whilst complex products might not. Rather than proposing to introduce additional regulatory requirements in relation to online distribution of simple investment products, the SFC is placing its focus on ensuring that investors have the means to fully understand the nature and risks of complex investment products through appropriate disclosures, in the online context where there investors will not have the benefit of face-to-face communication with intermediaries.

General core principles

There are six core principles which are proposed to be included in the Guidelines. These core principles apply to all licensed or registered persons when conducting regulated activities in providing order execution, distribution and advisory services online.

- **Proper design**: such as restricting retail clients to access information relating to exchange-traded funds not authorised by the SFC, and operating the online platform with due skill, care and diligence
- **Information for clients**: such as providing clear and up-to-date product offering documents and disclosure as to the scope and limitations of services and commission, fees and charges
- **Risk management**: such as testing and monitoring the systems regularly, having a contingency plan to deal with emergencies and cybersecurity

- **Governance, capabilities and resources**: such as adequate resources to oversee and manage the operations of the online platform
- **Review and monitoring**: such as on-going supervision and monitoring of the online platform
- **Record keeping**: including documentation on the platform design, operations, tests and reviews, which should be retained for at least two years after the online platform ceases to operate, and audit trails of transactions, to be retained for at least seven years for non-exchange traded products and two years for exchange traded products.

The proposed Guidelines contain a section on the general requirements of business conduct of licensed or registered persons in accordance with the Code of Conduct and other codes, guidelines and circulars published by the SFC. These requirements are the same as those which apply in an offline environment, such as the usual know-your-customer requirements, the requirement to ensure best execution and the requirement to disclose monetary and non-monetary benefits. This section is a clarification of the general obligations of licensed or registered individuals in the context of an online environment, but does not impose new requirements.

The proposed Guidelines also feature a separate section which discusses specifically the application of the current general conduct requirements and the suitability requirements in the context of robo-advisory services, i.e. provision of financial advice through online platforms using algorithms and other technology. Under this section, accurate description of investment products and easily comprehensible disclosures must be provided to enable investors to make informed decisions. Licensed or registered intermediaries will also be required to ensure client profiling tools are properly designed (for example designs to ensure sufficient information is obtained and inconsistencies in such information are identified and reconciled), algorithms properly programmed, appropriate on-going testing and supervision is performed, and adequate resources are deployed to maintain and develop the systems.

Suitability requirements

Under the Code of Conduct, the suitability requirement is the obligation to ensure the suitability of a recommendation or solicitation that is made by a licensed or registered person to a client. Whether an intermediary has "recommended" or "solicited" is a question of fact. The suitability requirements apply the same way to both online and offline regulated activities. The use of an online platform will not deem an intermediary to have recommended or solicited any products. Nonetheless, provision of robo-advice would normally trigger the suitability requirements.

The principles regarding suitability discussed in the SFC's consultation paper do not impose new obligations, but are only clarifications of the existing requirements under the Code of Conduct as they are applied to the online context. The discussions focus mainly on when the Suitability Requirements are triggered, and the discharge of suitability obligations.

In determining whether there is "solicitation" or "recommendation", the context and content of product-specific materials posted on an online platform coupled with the design and overall impression created by the platform content should be considered. Whether the materials posted are factual, fair and balanced, and whether there is influence on investors to purchase a particular product are key factors. The SFC proposes to include certain examples of situations when and when not the suitability requirements will be triggered. For example, posting of general market news or updates, or product-specific materials which are factual, fair and balanced will not in itself trigger the suitability requirements, neither would the posting of lists of investment products that are selected using objective criteria (for example performance data, sales figures and research data). On the other hand, posting of advertisements with product-specific incentives for any

transactions in a specific investment product, or the generation of a list of investment products following a client's query through a client profiling tool, will trigger the suitability requirements.

With respect to discharging obligations when the suitability requirements are triggered, the SFC emphasised that mere mechanical matching of a product's risk rating with a customer's risk tolerance level may not be sufficient. The SFC expects online platform providers to at a minimum make an assessment of a customer's risk tolerance and risk profile, and conduct product due diligence to ascertain the risk return profile of an investment product. The SFC proposes to consolidate all SFC guidance materials on the Suitability Requirements (including the FAQs published in December 2016) into one page on the SFC's website for ease of reference.

New requirements for complex products

On the basis that it may be more difficult for investors to understand complex products in an online environment, the SFC proposes to extend the suitability requirements to "complex products" even in situations where there is no solicitation or recommendation. Intermediaries may be exempt from this requirement in respect of corporate professional investors provided that certain steps are taken, but exemption will not be applicable to Individual Professional Investors.

The proposed Guidelines set out factors which will be considered in determining whether product is "complex." These are, for example, whether the product is a derivative product, whether there is a risk of losing more than the amount invested, and whether there are features which may render the investment illiquid. The SFC proposes to publish a non-exhaustive list of examples of "complex" and "non-complex" products to assist intermediaries with their classification. For example, futures contracts, synthetic ETFs and funds or other structured products which are not authorised by the SFC are proposed to be classified as "complex" products.

In addition to extending the suitability requirements to complex products, the SFC also proposes the requirement for platform providers to provide warning statements and basic and key information on complex products at the minimum. The proposed Guidelines include an appendix setting out a non-exhaustive list of examples of minimum information and warning statements which must be provided in relation to complex products on online platforms. These are, for example, the product nature, key terms and features, whether the product is principal protected or not, and whether there are penalties for early exit.

Conclusions

The consultation represents an important reaction to a significant shift in the market for financial services in Hong Kong and elsewhere, as investors seek the convenience and speed of online transacting and greater choice in terms of how they receive financial services. In line with the other principal Hong Kong financial regulators, the SFC has established a Fintech Contact Point that is meant to encourage greater engagement with fintechs and recently entered into a fintech cooperation agreement with the UK Financial Conduct Authority, the UK regulator being seen as a leader in regulatory innovation on this front. The SFC has clearly been undertaking a broader review of its compliance requirements in light of Hong Kong's fintech surge.

It is also interesting to see that the SFC has taken the view that additional requirements should be imposed with respect to the sale of complex investment products, which echoes the concern of the Insurance Authority, who in its guidance note (GN16 – Guidance Note on Underwriting Long Term Insurance Business (Other Than Class C Business)) stated that products with complex features may not be suitable for distribution through online channels, as advice cannot be given to customers during the sale process. With these reference points in mind, the SFC clearly sees fintech innovation as an opportunity for Hong Kong but also recognises the importance of a measured approach to re-adjusting risk allocations in order to protect investors.

Katherine Tsang
Associate, Hong Kong
T +852 2219 0888
katherine.tsang@hoganlovells.com

Alicante
Amsterdam
Baltimore
Beijing
Brussels
Budapest
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