Hogan Lovells

After the gold rush: the end of a golden age for China's mobile app market?

MARCH 2016

Contents

Contacts

Further information

If you would like further information please contact a lawyer mentioned below or the lawyer with whom you usually deal.

Shanghai

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

Maggie Shen
Associate
maggie.shen@hoganlovells.com
+86 21 6122 3883

Jing Wang
Associate
jing.wang@hoganlovells.com
+86 21 6122 3839

Beijing

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

Hong Kong

Mark Parsons
Partner
mark.parsons@hoganlovells.com
+852 2840 5033

After the gold rush: the end of a golden age for China's mobile app market?

Corporate China Alert – 14 March 2016

Overview and background

China has finally made a move to regulate the smart mobile devices applications ("**Mobile Apps**") industry, which has been on fire for many years[1] but has experienced certain "growing pains". This move may signal the end of the "gold rush era" for China's Mobile App market and usher in a more orderly and regulated market environment.

On 18 November 2015, the Ministry of Industry and Information Technology ("**MIIT**")[2] released the *Pre-installation and Distribution of Applications for Smart Mobile Devices Interim Administrative Provisions (Draft for Public Comments)* (the "**Consultation Draft**"), the purpose of which is to regulate the pre-installation and distribution of Mobile Apps in China. The public consultation period ended on 18 December 2015 and the final rules are expected to be released soon.

Despite MIIT's proposals as early as 2012 that all Mobile Apps to be released in China would first have to be submitted to the MIIT for approval, the Consultation Draft does not go so far as to mandate a registration and approval system. However it does aim to bring independently-developed Mobile Apps within the regulated scope by establishing a real-names registration system for independent developers. It also imposes a requirement to meet China's standards with respect to all Mobile Apps.

This note provides an overview of the key obligations imposed on industry participants in the Mobile App sector under the Consultation Draft and analyses a number of such obligations and their potential implications, including the following:

(i) Mobile Apps must meet China's standards;

(ii) the need to look beyond the Consultation Draft for requirements on the protection of personal information;

(iii) a question as to whether the proposed administrative obligations placed on manufacturers and app store/platform operators might work in practice in terms of managing Mobile App developers and other industry players; and

(iv) "lacunae" under the Consultation Draft.

History of China's regulation on Mobile Apps

As early as December 2012, commentators were predicting the end of the gold rush era for China's Mobile App developers, when the MIIT made a statement that it intended to regulate the Mobile Apps market by requiring Mobile App store/platform operators to comply with a registration and licensing process. Nothing concrete materialized until 2013, when MIIT issued the *Strengthening the Administration of Network Access by Smart Mobile Devices Circular* (effective 11 January 2013) (the "**Smart Mobile Devices Access Circular**") which prohibits the pre-installation of certain Mobile Apps (e.g., apps that fail to obtain explicit consent for the collection and use of users' personal information, or the use of the devices' communication functions; apps that contain prohibited content) by device manufacturers on smart mobile devices to be used on Chinese networks.

The Consultation Draft goes much further than the Smart Mobile Devices Access Circular in terms of the regulated scope of activities, by regulating not only on the pre-installation of Mobile Apps, but also the distribution of Mobile Apps. In terms of the industry players regulated, not only device manufacturers, but also Internet information service providers that distribute Mobile Apps (such as app stores/platforms) are now caught.

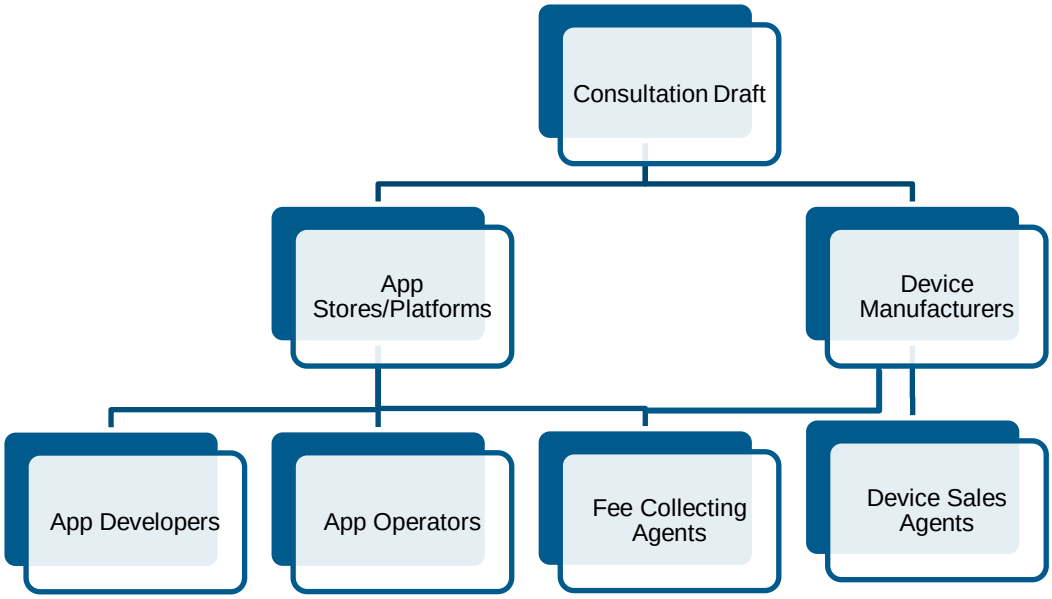
---

1 See, e.g., "There are also many copycat, fraudulent, and malicious apps with bugs and viruses in the Android-based app market.": Chen Yang, "MIIT to tighten app regulations", *Global Times*, 14 December 2012, available at http://www.globaltimes.cn/content/750131.shtml.

2 The Internet and telecommunications regulator, whose remit includes Mobile Apps.

How the Consultation Draft proposes to regulate key players in the Mobile App landscape

Below is a diagram illustrating how the Consultation Draft proposes to regulate the key players in the Mobile App landscape.



As illustrated above, the Consultation Draft seeks to regulate nearly all of the key players in the Mobile App market (except for certain third parties, such as analytics and advertising providers). However one key feature of the Consultation Draft is that it places new and quite onerous obligations on app stores/platforms[3] and device manufacturers to do nearly everything, from ensuring the Mobile Apps they pre-install/distribute are compliant with the provisions of the Consultation Draft, to ensuring the protection of personal information, to information disclosure and content censorship, and to managing app developers, app operators, and third parties commissioned by them such as device sales agents and fee collecting agents. This heavy burden on app stores/platforms maybe due to the fact that app stores are the only party in eco-system with sufficient front-end leverage to require app developers to deliver adequate information about the Mobile Apps.

The need to comply with China's relevant standards – will this prove to be the Achilles Heel of foreign app developers?

Article 5(2) of the Consultation Draft places obligations on manufacturers of smart mobile devices ("**Manufacturers**") and Internet information service providers that provide app distribution services for smart mobile devices (such as app stores, "**Internet Information Service Providers**") to ensure that the Mobile Apps they provide meet the requirements under relevant Chinese standards. It is not clear at this stage whether the relevant standards will only be limited to standards to be issued by the China Communications Standards Association ("**CCSA**"), a Chinese professional standards organization with the responsibility for developing communications technology standards,[4] or will extend to other standards issued by other bodies. Based on our enquiries with the MIIT, an explanation as to which "relevant standards" are being referred to under Article 5(2) will be included in the final version of the law. In any event, this could be an onerous and costly obligation for all Mobile App developers, especially

[3] Under the Consultation Draft called "Internet information service providers that provide app distribution services for smart mobile devices".

[4] Based on our enquiries with the CCSA, it has submitted a set of draft standards containing security and technology requirements on Mobile Apps to MIIT and it is also working on other standards governing Mobile Apps. The issue is whether these standards will include onerous provisions that will essentially force certain players out of the market by requirements to disclose source code and the like.

foreign players who may find it particularly difficult to meet Chinese technical standards, due to their highly technical language, the fact they are not usually available in English and so forth. This may push Mobile App development onshore, where there are native speakers able to interpret such standards and the skill sets needed to interpret these technical documents are more readily available.

Article 5(2) further prohibits Manufacturers and Internet Information Service Providers from doing things that would infringe the legitimate rights and interests of users or compromise cyber-security ("**Prohibited Acts**") such as (i) promoting unrelated apps by forcibly bundling them with the Mobile Apps; and (ii) forced turning on of Mobile Apps.

Requirements on the protection of personal information

The Consultation Draft places obligations on Manufacturers and Internet Information Service Providers to protect users' personal information protection:

- Other Prohibited Acts for Manufacturers and Internet Information Service Providers under Article 5(2) include: (i) calling up device functions not related to the service provided by the Mobile Apps; (ii) collecting and/or using users' personal information without giving ***explicit notice to, and obtaining consent from***, users; and (iii) sending commercial electronic information (i.e. spam) in a "non-compliant" manner without giving explicit notice to, and obtaining consent from, users.

- Article 6(1) requires Manufacturers and Internet Information Service Providers to "provide information about the Mobile Apps provided (including, without limitation, the ***content, purpose, method and scope*** of the apps' use and collection of users' personal information) by way of user notice or on company websites".

- Article 8(6) provides that Internet Information Service Providers that provide app stores or other app distribution platform services and Manufacturers that pre-install app distribution platforms on their smart mobile smart devices must "strengthen the protection of network security and training of the relevant personnel to ensure the security of their own systems and users' personal information".

It is important for device manufactures and app stores/platforms to note that merely meeting the above-listed requirements is not enough: in addition to these requirements which are already included in the Smart Mobile Devices Access Circular and a number of existing laws, regulations and rules on data protection and privacy ("**Existing Data Privacy Laws**")[5] [6], there are other data privacy requirements which must be complied with.

The table setting out the key obligations on providers of telecommunications services, internet information services and/or business operators which are already imposed under Existing Data Privacy Laws is on the next page. It specifies whether those key obligations are also imposed under the Smart Mobile Devices Access Circular and the Consultation Draft.

---

[5] For a detailed discussion of these laws and regulations, see our client note *China Turns up the Heat in the Battle Against Abuses of Personal Data* dated 20 August 2013 (updated in March 2014).

[6] The key rules are:

- *Regulating the Internet Information Service Market Order Several Provisions* issued by the MIIT which became effective on 15 March 2012;
- *the Decision by the Standing Committee of the National People's Congress on the Strengthening of the Protection of Network Information* (the "**Network Information Protection Decision**") that came into force on 28 December 2012;
- *the Guidelines of Personal Information Protection within Information System for Public and Commercial Services on Information Security Technology* which became effective on 1 February 2013, jointly issued by the PRC General Administration of Quality Supervision, Inspection and Quarantine and the PRC Standardization Administration;
- *the Provisions on Protection of Personal Information of Telecommunications and Internet Users* issued by the MIIT and became effective on 1 September2013;
- certain provisions of the *NPC Decision on Amending the People's Republic of China Protection of Consumer Rights and Interests Law*, amending certain provisions of the People's Republic of China Protection of Consumer Rights and Interests Law (2nd Revision) ("**Amendments to the Consumer Protection Law**") that came into force on 15 March 2014; and
- certain provisions in the *NPC Decision on Amending the People's Republic of China Advertising Law*, amending certain provisions of the *People's Republic of China Advertising Law* that came into force on 1 September 2015.

Key Obligations Under Existing Data Privacy Laws	Under Smart Mobile Devices Access Circular?	Under Consultation Draft?
User consent	✓	✓ Article 5(2)
Inform users as to purpose, method, content and scope of personal information collection and use.		✓ Article 6(1)
Must take technical measures and other necessary measures to safeguard information security and prevent the personal information of users/consumers from being divulged or lost.		✓ Article 8(6)
Must not send commercial electronic information without consent or request.		✓ Article 5(2)
Must disclose the true identity and contact details of the sender of advertisements where any advertisement is sent in electronic form, along with instructions on how to opt out of receiving further advertisements.		
Must not collect personal information other than as is necessary in connection with the product or service provided by them.		
Must not violate any laws or any agreements with the user, must refrain from using it in a fraudulent, misleading or coercive manner.		
Must keep strictly confidential all personal information which is collected and used and must not divulge, alter, destroy or sell such information, or unlawfully provide such information to third parties.		
Must immediately take remedial measures where information has been or may be divulged or lost.		
Must formulate rules on the collection and use of personal information of users, which must be displayed on their business premises, websites and so forth.		
Monitor and regulate the performance of third parties that are engaged to offer marketing, technical and other agency services to users involving the collection and use of personal information.		
Internet information services provides must clearly inform users of the channels for accessing or making corrections to information, and the consequences of refusing to provide information.		

Note that the key obligations under the Existing Data Privacy Laws are imposed on business operators, Internet information service providers (and for certain key obligations, on all entities) who **collect and use** users' personal information. As such, those key obligations not only catch Manufacturers (if they collect and process user personal information for their own purposes such as to allow the device to operate normally, for security verification purposes, for instance, if they collect user details on registration, or if the device has a back-up or remote facility), the Internet Information Service Providers (for their collection and processing of user registration details such as name, address and financial data, and may be combined with data about purchasing and usage behaviour), but will also catch app operators and other players in the Mobile App market if they collect and use users' personal information.

Obligations to manage app developers, app operators and third parties

The Consultation Draft imposes the following management obligations on Manufacturers and Internet Information Service Providers:

- Managing fee collecting agents – Article 5 (3) tackles the business of monetizing apps, requiring companies which entrust a third party to collect charges for Mobile Apps ("**Fee Collecting Agents**") to have in place necessary technical measures to strengthen the security protection of relevant codes used in fee calculation, preventing them from being modified, forged or abused and avoiding any unclear charges. In addition, the fee collecting agent has to meet the data retention requirement – storing the user confirmation data and original payment data for at least five months, while making it easier for users to check this data.

- Managing device sales agents – Article 5 (4) obligates Manufacturers to take effective actions to ensure that device sales agents do not install Mobile Apps without user consent. Manufacturers are also obliged to inform users of the possibility, potential risks and counter-measures available in relation to smart mobile devices having apps installed during the sales process.

- Managing app operators and app developers – Article 8 sets out the management obligations for Internet Information Service Providers engaging in app store or other app distribution platform businesses and Manufacturers that pre-install app distribution platforms on their smart mobile devices. These include:

    - **registering the real identity and contact information of the app operator and app developer**;

    - establishing an app management system to test, assess and monitor the security of relevant apps, remove malicious and other illegal apps, together with providing a user complaint mechanism to help remove malicious and other illegal apps;

    - requiring app providers to furnish a list of permissions they propose to obtain for the purpose of accessing users' devices and the purpose of obtaining these permissions, and providing explicit notice of this information to users;

    - keeping the apps and relevant information (version, online time, profiles of functions, usage, MD5 and server access, etc.) for at least 60 days; any apps that fail to comply with this requirement or are found to be malicious by the authorities must be removed; and

    - strengthen the protection of network security and training of relevant personnel, so as to ensure the security of their own systems and users' personal information.

App store security is clearly a primary concern for the Chinese government. Anecdotal evidence suggests that some of the Android-based apps stores operating in China are infested with malicious apps and pirated apps containing viruses and defects.

It can be seen from the above requirements that the Consultation Draft attempts to tackle these problems by requiring the device manufactures and app stores/platforms to play a management role in ensuring app security and personal information security, as well maintaining a register recording the real names of app developers[7]. It remains to be seen how well device manufactures and app stores/platforms will be able to adapt to this new and quite onerous role.

---

[7] The real name registration requirement ties in with Article 6 of the *Network Information Protection Decision* and Article 21 of the *Anti-Terrorism Law* (defined later).

Requirements on uninstallation of non-basic apps

One of the highlights of the Consultation Draft on which the media and stakeholders (for instance, device manufacturers, app developers and smart phone users) have focused is the requirement that the Manufacturers and Internet Information Service Providers must ensure that all Mobile Apps can be uninstalled except for basic function software.

Articles 7 of the Consultation Draft sets out a set of obligations on Manufacturers and Internet Information Service Providers regarding uninstallation of Mobile Apps other than basic function software ("**Non-basic Apps**")[8].

These requirements are viewed by some as the biggest challenge to device makers, as a substantial percentage of their profit comes from pre-installed software, not the smart phones themselves. On the flip side, they are also the most populist provisions in the Consultation Draft in the eyes of certain smart phone users. These requirements are also said to be the authorities' response to address some of the concerns in relation to pre-installed Mobile Apps – on 1 July last year, the Shanghai Consumer Council brought a case before the Shanghai No.1 Intermediate People's Court against Samsung and Oppo for violating consumers' legal rights by pre-installing Mobile Apps that cannot be uninstalled.

Requirements on information disclosure

- Privacy Notice

  Apart from requiring Manufacturers and Internet Information Service Providers to provide information on the content, purpose, method and scope of the apps' use and collection of users' personal information, Article 6(1) of the Consultation Draft also requires such "privacy notice" to include the name, function description, uninstall method, information on the developer, a list of permissions required to install and run the software and so forth.

  What is lacking in the above requirement is a description of third parties to whom the data will be disclosed and the contact details of app developers. The former is a piece of important information that users would need to have before he or she is able to give informed consent.

- Product User Manual

  Manufacturers are required to provide information on pre-installed apps in product user manuals and to provide the means for accessing detailed information in relation to the pre-installed apps in product user manual or on product packaging.

- Fee Disclosure

  For paid apps, Manufacturers and Internet Information Service Providers are required to strictly comply with the relevant stipulations on clearly marking prices and charges and may only charge after obtaining confirmation from users.

Requirements on content censorship

Article 4 of the Consultation Draft imposes a requirement on Manufacturers and Internet Information Service Providers to refrain from supplying apps that contain information and content prohibited from being released or disseminated under the *People's Republic of China Telecommunications Regulation*s ("**Telecoms Regulations**"). Article 57 of the Telecoms Regulations sets out the categories of information that cannot be sent, transmitted or reproduced (e.g., pornography or seditious material), but these are expressed in very broad-brush language that is open to interpretation. The same content censorship obligation is placed on Manufacturers under the Smart Mobile Devices Access Notice.

Further, under the recently passed *People's Republic of China Counter-Terrorism Law* ("**Anti-Terrorism Law**")[9], providers of internet services (which is likely to include Internet information service providers) are required to implement systems and technical measures in accordance with relevant (presumably forthcoming) regulations to prevent the spread of terrorist and extremist content, remove any terrorist/extremist

---

[8]
- Among the pre-installed basic function software performing the same functions, at most one piece can be set as not uninstallable;
- Manufacturers and Internet Information Service Providers must make sure that Non-basic Apps can be conveniently uninstalled by users without affecting the normal operation of the smart mobile device, and the files adjunct to the software on smart mobile devices (such as resource files, configuration files and user data files) must also be conveniently uninstallable and deletable; and
- Manufacturers must ensure pre-installed software that has been uninstalled is not forcedly recovered when the operating system of the smart mobile device is upgraded, and any newly added pre-installed software or major functional changes must be record-filed with MIIT.

[9] Issue by the Standing Committee of the National People's Congress and effect on 1 January 2016.

content that is discovered, and report such incidents to the relevant authorities.[10]

Enforcement mechanism and penalties

The Consultation Draft provides that the MIIT will supervise app pre-installation and distribution at the national level, and local telecommunications administrative bureaus will supervise apps pre-installation and distribution within their respective jurisdictions. It also sets out detailed requirements on supervision and inspection, including publishing results of inspections to the public.

Users are also given a right to complain to the company in question, to lodge official complaints with the authorities, or to report violations to the authorities.

The penalties spelt out under the Consultation Draft are quite limited: administrative penalties such as an order to rectify, and/or having administrative penalties recorded in the company's credit worthiness file, and/or the possibility of being placed on a malicious apps list (recommended to be formed by the relevant social organizations). However, the violation of certain requirements (such as non-compliance or inaccuracy in a privacy notice) may be considered to constitute false or misleading promotion of goods or services which can lead to claims under the Amendments to the Consumer Protection Law.

"Lacunae" under the Consultation Draft and the Existing Data Privacy Laws

In the light of stipulations in data privacy laws/guidelines in other jurisdictions[11], there remain certain "lacunae" under the Consultation Draft and the Existing Data Privacy Laws on the regulation of Mobile Apps:

- App information should also contain the contact details of the app developer, and the descriptions of third parties to whom the data will be disclosed;
- App users should be given the right to withdraw their consent and request deletion of data.
- App developers should define a reasonable retention period for data collected with Mobile Apps and predefine a period of inactivity after which the accounts will be treated as expired;
- For Mobile Apps aimed at children, based on the age limit defining children or minors under relevant laws there should be requirements to (i) give notice to parents and get their verifiable consent before collecting, using, or disclosing such personal information; (ii) prohibit conditioning children's participation in activities on the collection of more personal information than is reasonably necessary for children using the Mobile App to participate in its functions; (iii) refrain from processing children's data for behavioural advertising purposes; and (iv) refrain from collecting data through the children about their relatives and/or friends.

Conclusions

It can be seen from the above that after the enactment of the Consultation Draft (if in its current form), it will have substantive implications for all key players in China's Mobile App market, especially foreign players, as all Mobile Apps will need to meet the new China's standards (which could be very onerous and in the worst case scenario, tailored to favour compliance by local players). Device manufacturers and app stores/platforms may also suddenly find themselves forced to take on onerous and costly management responsibilities, which under other jurisdictions such as the EU[12] are the responsibility of government.

It also remains to be seen whether the Chinese regulators will move to fill in some or all of "lacunae" identified in the preceding paragraphs to bring the new regime more in line with international standards.

---

10 For a detailed discussion of these provisions, see our client note *China's Counter-Terrorism Law enlists the support of Technology Providers (and just about everyone else)* dated 18 January 2016.

11 For instance the EU and the United States.

12 See, for example, discussion in the EU Article 29 *Data Protection Working Party's Opinion 02/2013 on Apps on Smart Devices*, which was adopted on 27 February 2013, and made public on 14 March 2013.

www.hoganlovells.com

Hogan Lovells has offices in:

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

*Associated offices