Hogan Lovells

New law on internet services addressing competition and personal information protection

China Corporate Alert - March 2012

Further information
If you would like further information on any aspect of the alert please contact a person mentioned below or the person with whom you usually deal.

Contact

Beijing

Jun Wei
jun.wei@hoganlovells.com
+86 10 6582 9501

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

Shanghai

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

Contents

New law on internet services addressing competition and personal information protection

China Corporate Alert - March 2012

1. INTRODUCTION

On 29 December 2011, the Ministry of Industry and Information Technology ("**MIIT**"), the internet and telecoms industry regulator promulgated the *Regulating the Internet Information Service Market Order Several Provisions* (the "**Internet Information Service Provisions**"). The Internet Information Service Provisions will become effective on 15 March 2012 and will be administered by MIIT.

The Internet Information Service Provisions, which primarily address unfair competition issues and the processing of personal data, represent a significant step by China to prescribe the boundaries of acceptable practice on the internet. This note provides a summary of key aspects of the Internet Information Service Provisions.

In this note, paragraph 6 below outlines how the Internet Information Service Provisions address unfair competition issues, paragraph 7 below outlines how the Internet Information Service Provisions address user privacy issues, paragraph 8 below outlines certain commercial practices which are impacted by the Internet Information Service Provisions and paragraph 9 below outlines the penalties for breach of the Internet Information Service Provisions.

2. THE IMPETUS FOR THE NEW LEGISLATION

The Internet Information Service Provisions represent a response to the increasing concerns around user privacy and competition on the internet. Two recent high-profile cases provide good illustrations of the kind of mischief that the Internet Information Service Provisions seek to address:

(a) The 2010 "3Q war"

In this dispute, which concerned both privacy and competition issues, Qihoo 360, China's leading anti-virus software provider, alleged that Tencent, the provider of the hugely popular QQ instant messaging software, was inappropriately accessing QQ users' personal data. In response to that allegation, Tencent threatened to prevent QQ running on devices operating the Qihoo 360 software. This left QQ's over 600 million users with the stark choice of either removing Qihoo 360 or being denied access to QQ. In September 2011, a Beijing court found Qihoo guilty of anti-competitive practices and awarded Tencent damages in an amount of Renminbi 400,000.

(b) The 2011 "CSDN leak"

In this matter, which concerned privacy issues, Qihoo 360 alerted the police that the personal data of more than six million users of the China Software Developer Network had been hacked. Matters escalated and a general panic ensued when it was subsequently alleged that the hackers had also successfully infiltrated a variety of other websites, including popular online shopping, online gaming and personal finance sites. It subsequently transpired that the hacking was much less widespread than originally feared. However, the case underscored the implications of security failings on the internet.

3. OTHER LEGISLATION SPECIFIC TO CHINA'S INTERNET SPACE

Once enacted, in terms of strict legal hierarchies, the Internet Information Service Provisions which are departmental rules (部门规章) will sit below the *Internet Information Services Administrative Procedures* (the "**Internet Information Procedures**")[1] (which are administrative regulations issued by the PRC State Council, China's cabinet (行政法规)) on which they are based. The Internet Information Procedures focus on the interaction between Providers (as defined below) and the State. In contrast, the Internet Information Service Provisions focus more on the interaction between Providers and the internet user.

---

[1] *Measures of Internet Information Services* (互联网信息服务管理办法), issued by the PRC State Council and effective 25 September 2000.

China has promulgated a number of rules based on the Internet Information Procedures affecting various types of internet information services, for example, the provision of healthcare information[2], email services[3] the publication of news[4] and the operation of online bulletin boards[5], to name but a few. These and China's policies on blocking certain well-known websites, such as Facebook and YouTube illustrate the extent to which China views the internet as a particularly "sensitive" space that needs to be heavily regulated, with access to certain content being carefully monitored and controlled.

4. SCOPE OF THE INTERNET INFORMATION SERVICE PROVISIONS

The Internet Information Service Provisions regulate:

"those engaging in the provision of internet information services and activities relating to internet information services within the People's Republic of China"[6]

This is an extremely wide definition which on the face of it could cover both commercial and non-commercial activities, although it does provide a geographical limitation to its scope of regulation (as do the Internet Information Procedures and many other rules in this area). Therefore it would seem at the very least to cover both operational Providers (经营性) (known better as Internet Content Providers or "**ICPs**") and non-operational (non-profit making) Providers (非经营性) as referred to in various local regulations issued around the time of the internet "bubble" such as the *Beijing State Administration of Industry and Commerce Operational Website Record Filing and Registration Administrative Tentative Procedures* effective 1 September 2000.[7]

This scoping provision is important because this provides the whole basis for whether or not an activity is or is not caught. For example, arguably where a company outside China has a website with its server located outside of China, but accessible from China, then on the basis that it is not providing internet information services or engaging in activities relating to internet information services within the mainland of the PRC, then it could be argued it falls outside the scope regulated by the Internet Information Service Provisions. On the other hand, if a company within China, sourcing all its content from China is specifically targeting Chinese customers from an offshore-hosted website which is entirely in Chinese, then it could arguably fall within the scope of engaging in activities relating to internet information services in the PRC (or be seen as blatantly trying to circumvent the rules), although it is not a clear "bright line" test nor is it an easy line to draw. In any event, the mere fact of being a company registered in China *de facto* makes such entity subject to regulation under Chinese law.

The Internet Information Service Provisions themselves do not define either "Internet Information Services" or "Internet Information Service Providers", however, and there is only a very general definition of "Internet Information Services" set out in the Internet Information Procedures which defines these as:

"activities involving provision of information services to internet subscribers through the internet."[8]

---

2 *Measures for Administration of Information on Pharmaceuticals on the Internet* (互联网药品信息服务管理办法), effective 8 July 2004.

3 *Measures for Administration of E-mail Services on the Internet* (互联网电子邮件服务管理办法), effective 20 February 2006 (the "**E-mail Service Measures**").

4 *Regulations for the Administration of Internet News Information Services* (互联网新闻信息服务管理规定), effective 25 September 2005.

5 *Administrative Provisions on Internet Online Bulletin Boards Services*, effective 8 October 2000.

6 See Article 2 of the Internet Information Service Provisions.

7 The distinction being that operational websites required a permit from MIIT whilst non-operational websites only required a record filing. The distinction has evolved over time, with the current line in the sand being based on whether the service itself as opposed to the article is paid for. Hence taobao, ebay (eachnet) and online gaming companies all of which require certain participants (e.g. players or sellers) to pay charges, all require a permit from MIIT which is required to be displayed on the front page of the website, whilst pure information providers such as government body websites or companies providing information-only websites registered in China normally only display a record filing ICP ("备") approval.

8 Articles 2 and 3 of the Internet Information Procedures.

5. DISTINGUISHING BETWEEN INTERNET INFORMATION SERVICE PROVIDERS AND INTERNET ACCESS PROVIDERS (ISPS)

There is no specific definition of an Internet Information Service Provider (a "**Provider**") in either the Internet Information Procedures or the Internet Information Service Provisions; however it seems to be that the intent behind the Internet Information Service Provisions is to throw the net widely and capture anyone providing Internet Information Services proper as well as those involved in certain activities around Internet Information Services e.g. provision of downloaded software.

For clarity, a Provider should be distinguished from an "internet service provider"; the latter refers generally to the operator of a platform allowing users to access the internet, hence in Chinese they are referred to literally as "internet access services" (互联网接入服务), but are better known elsewhere as Internet Service Providers (or "**ISPs**"); whereas a Provider (or ICP) provides information services over an internet platform. ICPs are in fact major customers of ISPs. Under the *Circular regarding Adjustment to the Catalogue of Classification of Telecommunications Service* (the "**Catalogue**") issued by the Ministry of Information Industry (the predecessor to MIIT) with effect from 1 April 2003, an ISP is defined as:

> "Internet access services means using access servers and the corresponding software and hardware resources to establish a service mode, and using public basic telecommunications facilities to connect such service mode to the internet backbone, in order to provide all types of users with internet access services. Users can use public telephone networks or other methods to connect to the service node and, through such service node, access the internet.
>
> There are two major applications for internet access services: 1) provision of internet access services to internet content providers (ICPs), who will use the internet to conduct their services such as provision of content, online trading and other online applications; and 2) provision of internet access services to allow general users and others who need to access the internet and need to obtain the relevant service."

The scope of activities regulated by the new rules appears to go substantially wider than those internet information services activities requiring an operating permit from MIIT pursuant to *The Telecommunications Regulations of the People's Republic of China*[9] (the **"Telecommunications Regulations"**). These are defined in the Catalogue, and essentially consist of "paid-for" or "pay to play" information services. Internet information services requiring a telecoms business operating permit (电信业务经营许可证) are defined as set out below:

> "Information services business means using information consolidation, development, processing and the building of information platforms to directly provide end user terminals with speech-based information services (voice communication services) or online information and database retrieval and such like information services through fixed-line networks, mobile networks, internet networks and such like public communication networks.
>
> The main types of information services business include provision of contents, entertainment/online gaming, commercial information, positioning information and such like services. The users interfacing with the information services business can be fixed-line mobile communications network, internet users, or the users of other data transmission networks."

MIIT has confirmed on its website that the Internet Information Service Provisions also cover software products insofar as such software provides either a platform for internet services (e.g. software-as-a service as a cloud computing service) or interacts with internet services[10].

---

[9] *The Telecommunications Regulations of the People's Republic of China* (中华人民共和国电信条例), effective 25 September 2000.

[10] http://www.miit.gov.cn/n11293472/n11293832/n11293907/n11368223/14414996.html

6. UNFAIR COMPETITION

Much of the Internet Information Service Provisions reads like a catalogue of perceived abuses and newly-outlawed conduct, perhaps reflecting MIIT's collective regulatory experience to date.

6.1 Providers' activities which infringe the rights of other Providers

Under Article 5 of the Internet Information Service Provisions, the following activities by a Provider are considered to be damaging to, and an infringement of, the lawful rights and interests of other Providers, and hence are prohibited:

- Maliciously interfering with the services provided by other Providers on a user terminal; or maliciously interfering with the downloading, installation, running and upgrading of the software and other such products associated with internet information services;
- Fabricating or disseminating false information, or maligning the services or products provided by other Providers;
- Maliciously designing its own products to be incompatible with the services or products of other Providers;
- Employing deceptive, misleading or coercive means whereby users are forced to use or not use the services or products of other Providers;
- Maliciously modifying, deceiving, misleading or coercing users into modifying, the parameters of services or products provided by other Providers; and
- Any other acts which violate the laws and regulations of the State, or infringe upon the lawful rights and interests of other Providers.

This article suggests that many market participants are resorting to highly dubious strategies to win over customers. They suggest that "knocking copy" in company materials is not permitted to be used to gain a competitive advantage[11], but more interestingly also hint at the fact that certain Providers are in a dominant market position so as to be able to coerce users and consumers into using their services or to "knock out" competing services. Part of Article 7 covers similar ground.

6.2 Providers' activities which infringe users' rights

Under Article 7 of the Internet Information Service Provisions, the following activities by a Provider are considered to be damaging to, and an infringement of, the lawful rights and interests of the internet user and hence are prohibited:

- Refusing to provide a user with access to, delaying access to or suspending the provision of internet information services or products to a user without justifiable cause;
- Restricting users to using, or from using, internet information services or products designated by Provider without justifiable cause;
- Providing internet information services to users through deceptive, misleading or coercive means;

[11] This is also prohibited under Article 12 of the *People's Republic of China Advertising Law* effective 1 February 1995.

- Providing internet information services or products which fail to comply with the promotional claims or undertakings made to users by the Provider of such services or products;
- Arbitrarily amending service agreements or business rules, thereby compromising the quality of services or increasing the liabilities on users;
- Failing to actively notify users when their services or products are not compatible with those of other Providers;
- Modifying a user's browser configuration or other settings without notifying the user of the same or obtaining the user's positive opt-in consent; and
- Any other acts which violate the provisions of the State, or infringe upon the lawful rights and interests of users.

6.3 Challenges in applying the Internet Information Service Provisions

Inevitably, the complexities of the underlying technology will present challenges in applying the Internet Information Service Provisions. For example, the extent to which an interaction between different products and services is such as to render them "incompatible" will be open to debate. Even in cases where the "incompatibility" is beyond doubt, for example, where one product can only work if another is completely uninstalled, whether that incompatibility arises out of a Provider's bad faith desire to secure a competitive advantage or out of an unavoidable technical issue will require detailed technical analysis.

The Internet Information Service Provisions also do not provide any guidance on what would constitute "justifiable cause", which will also generate debate.

6.4 Interaction with existing legislation

(a) Interaction with specific competition legislation

Infringing anti-competitive activity under the Internet Information Service Provisions may also constitute a general breach of competition law under the *People's Republic of China Anti-Unfair Competition Law* (the "**AUCL**")[12]. For the AUCL to apply there must be the sale of a product or service. Therefore, for example, if in the context of selling its software product, a company disseminated false or fabricated information on a competing software product that would be a breach of the Internet Information Service Provisions, it would also be a breach of the AUCL[13]. The same would apply if one Provider claimed its rival's free storage capacity to users was lower than it actually was. There may also be a case to answer under the *People's Republic of China Anti-Monopoly Law*[14](the **"AML"**) in circumstances where either the infringing company was in a dominant market position or where the relevant activity involved the conclusion of a "monopolistic agreement", the most flagrant example of which is cartel type behaviour.

Both the AUCL and AML are laws promulgated by the Standing Committee of the National People's Congress and thus rank above, and are not in any way supplanted by, the Internet Information Service Provisions. Therefore, Providers must continue to monitor their activity to ensure compliance with both the AUCL and the AML particularly as the penalties under the AUCL and the AML are much more serious than under the Internet Information Service Provisions (see paragraph 9 below). For example:

---

[12] *Anti-Unfair Competition Law of the People's Republic of China* (中华人民共和国反不正当竞争法), effective 2 September 1993.

[13] Article 9 of the AUCL.

[14] *The People's Republic of China Anti-Monopoly Law* (中华人民共和国反垄断法), effective 1 August 2008.

- Under Article 20 of the AUCL, an infringer is liable to the infringed party for damages and, if the losses of the infringed party are difficult to estimate, the profits derived from the infringer during the period of infringement are substituted as the determinant of the damages.

- Under Articles 46 and 47 of the AML, where there has been an abuse of a dominant market position or the conclusion of a "monopolistic agreement", in addition to confiscating an infringer's illegal gains, the Anti-Monopoly Enforcement Authority can levy a fine in an amount between one to ten per cent of the infringer's total annual turnover[15].

Article 20 of the AUCL is also significant as it creates an independent right for an infringed party to pursue a private claim for damages for their loss. This is also the case under Article 50 of the AML. However, no equivalent right has been created under the Internet Information Service Provisions. Therefore, Providers with genuine commercial grievances have been deprived of what would otherwise have been a useful route to take matters into their own hands (to the extent they could not already do so under the AUCL or the AML). A private right to damages would have allowed the market itself to shape market behaviour. Instead, the market must stand back and look to MIIT to act effectively. Given the limited penalties available to MIIT to enforce compliance (see paragraph 9 below), it is doubtful that the market will put much faith in the mechanism under the Internet Information Service Provisions being effective in shaping market behaviour.

(b) **Interaction with the Telecommunications Regulations**

Infringing anti-competitive activity under the Internet Information Service Provisions may also constitute a breach under certain existing prohibitions under the Telecommunications Regulations.

The Telecommunications Regulations are promulgated by the PRC State Council and therefore rank above, and are not in any way supplanted by, the Internet Information Service Provisions. Therefore, as with the AUCL and AML, Providers must continue to monitor their activity to ensure compliance with the Telecommunications Regulations particularly as the penalties under the Telecommunications Regulations are also much more serious than under the Internet Information Service Provisions (see paragraph 9 below).

Articles 41 and 42 of the Telecommunications Regulations set out a number of prohibited activities which in many respects overlap with activities prohibited under Article 7 of the Internet Information Service Provisions. For example, under Article 41(4) of the Telecommunications Regulations, a telecommunications business operator is prohibited from:

"rejecting, delaying or suspending provision of telecommunications services to telecommunications subscribers without any proper reason."

This mirrors the prohibition under Article 7 of the Internet Information Service Provisions against:

"Refusing to provide a user with access to, delaying access to or suspending the provision of internet information services or products to a user without justifiable cause" (see the first bullet point at paragraph 6.2 above).

However, whilst they prohibit similar activities, the consequences for breach under the Internet Information Service Provisions for such activity (see paragraph 9) are much lighter than under the Telecommunications Regulations. Under Article 75 of the Telecommunications Regulations the penalties for breach of Article 41(4) are:

- a fine of between Renminbi 10,000 and 100,000; and

[15] It is not clear whether "turnover" here is intended to capture the infringer's global sales or only sales in the relevant market.

- in circumstances where the violation is serious, the competent authority ordering the infringer to suspend its business pending rectification.

This points to what seems to be overall the most fundamental issue with the Internet Information Service Provisions: their lack of real "teeth".

(c) **Interaction with consumer legislation**

With regard to the activity regulated by Article 7 (see paragraph 6.2 above), much of this activity would also be prohibited under the *Law on the Protection of Consumer Rights and Interests* (the **"Consumer Protection Law"**) [16] and the *Product Quality Law* (the **"Product Quality Law"**)[17]. However, the foregoing legislation only applies where there is a "consumer relationship"[18] whereas the Internet Information Service Provisions will apply in all cases within the regulated scope.

7. USER PRIVACY

7.1 A major development in protecting personal privacy

Websites frequently collect personal information from their users, with or without their knowledge. The Internet Information Service Provisions seek to protect the legitimate expectation of privacy from perceived abuses in this regard.

China does not currently have a stand-alone law which deals specifically and comprehensively with privacy or protection of personal data. The right to privacy in China stems mainly from the fundamental rights under the constitution[19], criminal law (see paragraph 7.7(a) below), tort law (see paragraph 7.7(b) below) and other pieces of law. However, since the right to privacy under these laws remains relatively underdeveloped, there is little guidance as to the scope of personal information protected and the circumstances under which a breach of the right to privacy may or may not be established. Proposals have been made to enact more comprehensive laws and regulations addressing personal data privacy but to date they have not been enacted. The two most significant published proposals are the draft *Personal Information Protection Law* (the "**Draft Privacy Law**") (see paragraph 7.7(d) below) and the draft *Information Security Technology -- Guide to Personal Information Protection* (the "**Draft Guidelines**") (see paragraph 7.7(e) below). In the meantime, a number of diverse laws and regulations have attempted to fill in the vacuum and address the right to privacy.

In the internet space, the E-mail Service Measures[20], a piece of legislation which preceded the Internet Information Service Provisions, defines personal information as:

"information provided during the registration of an email account"[21]

This is a very limited definition of personal data confined to the specific purpose of that piece of legislation and the business model of email service providers who often require subscribers to fill in extensive registration forms, often containing non-essential data which has commercial value to the service provider.

---

16 *Law of the People's Republic of China on the Protection of Consumer Rights and Interests* (中华人民共和国消费者权益保护法), effective 13 October 1993.

17 *The People's Republic of China Product Quality Law* (中华人民共和国产品质量法), effective 8 July 2000.

18 For example, see Article 22 of the Consumer Protection Law and Chapter 3 of the Product Quality Law with respect to a product's fitness for purpose and Article 8 of the Consumer Law with respect to a consumer's right to information.

19 The right to privacy is in principle protected by the *Constitution of the People's Republic of China* (宪法, "**PRC Constitution**") effective as of 4 December 1982 (and as subsequently amended on various occasions). For example, (i) Article 40 of the PRC Constitution provides for freedom of, and privacy to, communications (subject to rights of interception for criminal investigations etc.) and (ii) Article 38 of the PRC Constitution provides that a citizen's "personal dignity" is protected as a fundamental right. Although the PRC Constitution does not define what constitutes "personal dignity" leading Chinese scholars take the view that it should include a right to privacy.

20 *Measures for Administration of E-mail Service on the Internet* (互联网电子邮件服务管理办法), effective 20 February 2006.

21 Article 9 of the E-mail Service Measures.

In the consumer space, Article 29 of the *Regulations of Shanghai Municipality on the Protection of Consumers' Rights and Interests*[22] (the **"Shanghai Consumer Protection Rules"**) prohibits a business from obtaining "personal information" from a consumer other than such "personal information" as relates to the relevant business transaction and prohibits disclosure of such "personal information" to third parties. The limitation on collecting only such information as relates to the relevant business transaction has implications for businesses which view a single transaction with a consumer as an opportunity to collect as much useful marketing information from that consumer as possible.

For the purposes of the Shanghai Consumer Protection Rules, "personal information" is defined as including:

"the names, sex, occupations, education, contact details, marital status, income and property, finger prints, blood types, medical history and other information that is closely related to the consumers themselves and their families."

The Shanghai Consumer Protection Rules are, however, only local government regulations applicable within Shanghai and only apply where a consumer relationship exists. They were, however, reportedly used to provide the basis for defining personal data in the Draft Privacy Law.

Therefore, although confined to the internet space, the Internet Information Service Provisions are a significant step forward in recognising an individual's right to privacy in cyberspace.

7.2 New rules on the processing of personal information

The Internet Information Service Provisions introduce a broad duty of care in respect of the collection and processing of Personal Information (as defined below).

Under Article 11 of the Internet Information Service Provisions "users' personal information" is defined as follows:

"any information associated with a user, which, either independently or when combined with other information, is able to identify such user " ("**Personal Information**").

In respect of Personal Information, Article 11 of the Internet Information Service Provisions:

- Prohibits Providers from collecting Personal Information without the prior consent of the user;
- Requires that Providers must clearly inform users of the method, content and purpose of collecting Personal Information;
- Prohibits Providers from collecting Personal Information other than as is necessary in connection with the product or service provided by them;
- Requires that Providers keep Personal Information secure; and
- Prohibits Providers disclosing Personal Information to any other person, except where laws and administrative regulations provide otherwise.

Article 12 deals with losses of Personal Information by the Provider and requires Providers to:

- Take immediate remedial action in the event that Personal Information is leaked; and

[22] *Regulations of Shanghai Municipality on the Protection of Consumers' Rights and Interests* (上海市消费者权益保护条例), effective 1 March 2003.

- If there is a risk of serious consequences flowing from a leak, to report it to the local department of MIIT and co-operate with the relevant department in conducting investigations.

7.3 New rules on data security

Article 13 of the Internet Information Service Provisions deals with data security and requires Internet Information Service Providers to strengthen system security threat prevention measures to protect the security of users' uploaded information and protect the rights of users to use, amend or delete uploaded information. It prohibits the following acts:

- Arbitrarily modifying or deleting any Personal Information uploaded by a user without justifiable cause;
- Providing user uploaded Personal Information to a third party absent the consent of the user, except where laws or administrative regulations provide otherwise;
- Transferring user uploaded Personal Information, either arbitrarily or under the pretence of a user's name; or deceiving, misleading or coercing a user into transferring any information which it has uploaded; and
- Other acts endangering the security of uploaded user information.

7.4 Prohibition on using information gathering software without consent

Spyware is the generic term for software that facilitates the collection of Personal Information on a user without their knowledge. Under the Internet Information Service Provisions, if a third party wishes to obtain Personal Information on a user they will have to obtain the user's specific consent to do so. This will mean that the use of non-consented-to-spyware (presumably including cookies and the like) will become unlawful in the absence of express user consent.

7.5 What will constitute an informed consent?

The Internet Information Service Provisions require that the Personal Information only be collected with user "consent". In reality, the vast majority of internet users accessing products and services online simply click that they have "read and agreed to" a Provider's lengthy "policy" documentation, when in fact they have not read it at all, and, even if they had read it, would probably not fully grasp its implications. The Internet Information Service Provisions do not specify what should be disclosed to a user and in what manner to duly procure consent. However, in the context of determining whether a user has consented to the installation of software, Article 8 of the Internet Information Service Provisions requires that before downloading, installing, operating upgrading, downloading software ("**Software Changes**") the prior disclosure must be:

"clear and complete information on the functions of the software and so forth."

Acts involving Software Changes through deceit or misleading or compelling users to accept Software Changes are also banned. MIIT will be the final arbiter of whether there has been adequate disclosure. In considering disclosure, Providers would be prudent to put themselves in the position of the user and not assume a level of user sophistication that is unrealistic. However, many Providers will be concerned that full disclosure will cause significant numbers to decline to download at all, thereby damaging their business.

7.6 The requirement for self-policing

Where there has been hacking of Personal Information the relevant Provider may, (assuming they are aware of the hacking), wish to keep it secret for commercial reasons. Whether the leak is the Provider's fault or not,

publicity of the leak is likely to affect the Provider's reputation. The Internet Information Service Provisions now require a Provider to notify the leak to the local department of MIIT where there are, or are likely to be, "serious consequences" (see Article 12). If it is unlikely that the leak will otherwise come to the public's attention, a Provider might consider the penalty (see paragraph 9 below) for not making that notification an insufficient deterrent versus the negative publicity and (wrongly) allow that commercial consideration to override its regulatory obligations.

7.7 **Interaction with existing legislation**

(a) **The Criminal Law**

As mentioned at paragraph 7.1 above, China does not have a stand-alone law which deals specifically and comprehensively with privacy or protection of personal data. However, in 2009 the *People's Republic of China Criminal Law*[23] (the **"Criminal Law"**) was amended so that it is now a crime:

- For government or private sector employees in financial, telecommunication, transportation, education or medical sectors to sell or otherwise "unlawfully" provide to third parties the personal data that has been collected by them in the course of performing their work duties; and

- For any person to obtain such information by means of theft or other "unlawful" means.

Where the violation is severe, the offender will be subject to imprisonment or criminal detention for up to three years and/or a monetary fine. Where the offender is an organisation (such as a corporate entity) the organisation is responsible for a monetary fine and the responsible person at the organisation may be personally liable for criminal charges.

Unfortunately, the Criminal Law does not provide guidance on any of: how to construe "personal data", what would constitute the "unlawful provision" of personal data or what would be considered a "severe" violation. It is not unusual for major national-level PRC laws to be vaguely drafted with the expectation that subsequent implementing regulations or interpretations of the Supreme People's Court will provide guidance in due course[24].

It is possible that where the processing, dissemination or collection of Personal Information is such as to be "unlawful" under the Internet Information Service Provisions, that this could satisfy the relevant "unlawful" requirement under the Criminal Law. The prospect of a "cross breach" of the Criminal Law in this way is a compelling reason for market participants to adhere to the Internet Information Service Provisions in the first place and certainly more compelling than the direct penalties under the Internet Information Service Provisions themselves (as to which see paragraph 9 below).

(b) **The Tort Law**

The *Tortious Liability Law*[25] (the **"Tort Law"**) states a general principle that any person who infringes on and damages "civil rights and interests" of other persons has committed a tort. Article 2 of the Tort Law expressly includes the "right to privacy" on the list of protected "civil rights and interests". Therefore, where a person's "right to privacy" is infringed they can pursue a private action against the infringer. Remedies for that claim include damages for their actual losses and, where the infringement has caused "serious mental injury", damages for "mental distress".

---

[23] *Criminal Law of the People's Republic of China* (中华人民共和国刑法), amended 28 February 2009.

[24] For details on China's first criminal case relating to the protection of personal information under the Criminal Law please refer to the Hogan Lovells' blog dated 8 January 2010 available at this link: http://www.hldataprotection.com/2010/01/articles/international-eu-privacy/chinas-first-criminal-case-regarding-the-infringement-of-the-security-of-personal-information/.

[25] *The People's Republic of China Tortious Liability Law* (中华人民共和国侵权责任法), effective 1 July 2010.

The introduction of a "right to privacy" is significant as previously an individual had no recourse for abuse of their personal information unless they could demonstrate that their "reputation right" had been infringed thereby (i.e. they had to pursue a claim in defamation). Therefore, this opens the door to many more claims. Unfortunately the actual scope of the "right of privacy" has not been defined in any further detail, so it is difficult to predict how those claims will be approached by the courts.

In addition to the introduction of a general (but undefined) "right to privacy", the Tort Law imposes a specific liability on an internet service provider in circumstances where either:

- They have been notified that an act of infringement under the Tort Law has occurred on their site and they do not promptly take necessary measures such as deletion, blocking, disconnecting the link and so forth; or

- They are aware that that an internet user is infringing upon the rights and interests of another user through their site and yet fail to take necessary measures.[26]

In both cases, the liability assumed by the ISP is joint and several with that of the infringing party. This places a quite onerous burden on the ISP because it will have to make a judgment call as to whether the accusation is spurious or not, although both legs do depend on knowledge or awareness of the infringement.

Applying a similar analysis to the risk of "cross breach" under the Criminal Law (as described at paragraph 7.7(a) above) it could also be the case that where an individual pursues a claim under the Tort Law that their "right to privacy" has been infringed by the collection and processing of personal information, a court could be persuaded to find in their favour if the circumstances involved a breach of the Internet Information Service Provisions. Put another way, it would probably be helpful to the defendant in that action if they could prove full compliance with the Internet Information Service Provisions with regard to the processing of the Personal Information.

(c) **The Telecommunications Regulations**

Paragraph 6.4(b) above provides commentary on the interaction between the Internet Information Service Provisions and the Telecommunications Regulations as regards competition. There is also interaction with regard to data protection. For example:

- Similar prohibitions on deleting transmitted/uploaded information

Under Article 58(1) of the Telecommunications Regulations, a telecommunications business operator is prohibited from:

"deleting or modifying any functions of telecommunications networks, or stored, processed or transmitted data, or application programs."

This closely reflects the prohibition in the Internet Information Service Provisions against amending or deleting information uploaded by users without "justifiable cause" (see the first bullet point in paragraph 7.3 above). Under Article 78 of the Telecommunications Regulations, if there is a "serious" breach of, among other things, Article 58(1), the original authority issuing the infringer's telecommunications business operating permit is authorised to revoke that permit. This is obviously a much more serious punishment than can be meted out under the Internet Information Service Provisions for the same activity (see paragraph 9 below).

- Similar prohibitions on disclosing information to third parties

Under Article 66 of the Telecommunications Regulations, it is an offence if:

[26] See Article 36 of the Tort Law.

"unless they have proper authorisation, telecommunications business operators and their staff make available to third parties information which telecommunications subscribers have transmitted using the telecommunications networks."

This mirrors the prohibition in the Internet Information Service Provisions against Providers providing the user's uploaded information to a third party without consent, save where otherwise provided by laws and administrative regulations (see the second bullet point in paragraph 7.3 above).

Under Article 71 of the Telecommunications Regulations, if there is a breach of Article 66 the relevant competent authority can order the infringing operator to rectify their conduct, confiscate the illegal proceeds and impose a penalty in an amount greater than such illegal proceeds but not more than three times the amount of such proceeds. If no illegal proceeds have been obtained or if the illegal proceeds are less than Renminbi 10,000, a penalty of over Renminbi 10,000 but less than Renminbi 100,000 can be imposed. Again, these penalties are (depending on the facts) likely to be greater than those imposed under the Internet Information Service Provisions (see paragraph 9 below). In circumstances where the violation of Article 66 of the Telecommunications Regulations is serious, Article 71 allows the competent authority to order the infringer to suspend its business pending rectification.

Therefore, as mentioned above in the context of competition, Providers must continue to monitor their activity to ensure compliance with the Telecommunications Regulations particularly as the penalties are much more serious than under the Internet Information Service Provisions (see paragraph 9 below).

(d) **Draft Privacy Law**

The Draft Privacy Law was published in late 2006, however, it remains under review and has not been enacted by the National People's Congress. Under the Draft Privacy Law, “personal information” would be defined broadly as including any information that can individually (or together with other information) lead to the identification of a specific person, such as name, address, date of birth, PRC Identification Card number, medical records, photographs, etc. Following the enactment of the Draft Privacy Law, the act of sharing or processing another's personal information without permission would subject the perpetrator to legal liability. However, the Draft Privacy Law provides that personal information may be used subject to obtaining an express waiver from the data subject - accordingly obtaining an express waiver may be considered as a minimum requirement prior to monitoring correspondence which may contain personal information.

However, the Draft Privacy Law is not currently effective law, and the version which is finally approved could differ significantly from the draft currently in circulation, if and when it becomes law. Those with long memories will recall that due to the difficulty of reconciling the interests of all the government stakeholders, the *People's Republic of China Telecommunications Law* remains in draft over 15 years after it was first drafted. Some Chinese people argue that at the current stage of development China is not yet ready for a fully-blown data privacy law.

(e) **Draft Guidelines on Data Privacy Protection**

On 10 February 2011, the General Administration for Quality Supervision, Inspection and Quarantine and the Commission for the Administration of Standardisation circulated the Draft Guidelines.

If issued, the Draft Guidelines would constitute recommended standards rather than laws; they would be non-binding. However, in practice market participants may be motivated to comply with the Draft Guidelines as compliance with them may assist in defending actions against them under binding pieces of legislation, such as the Criminal Law and the Tort Law (see paragraphs 7(a) and (b) above for a discussion of how compliance with the Internet Information Service Provisions may also prove helpful in this regard).

The Draft Guidelines were formulated following extensive consultation with major Chinese internet market participants (such as Baidu, Tencent and Sina) so provide an indication of where both the legislator and the market believe the balance should be struck between providing a competitive, innovative and fluid business

environment whilst also protecting personal privacy. In due course it is likely that some variation of the Draft Guidelines (or parts of them) may eventually be enacted in legislation.

The Draft Guidelines contain a set of rules and principles for the storing, handling and processing of personal information on "computer networks" (as opposed to other data storage media in hard copy form). The overarching principle is that personal information must be kept confidential and express consent must be obtained for all third party disclosure of such personal information.

With respect to the collection of, processing, use and maintenance of personal information the Draft Guidelines state that an individual must be notified in plain language of:

- the purpose of collecting the such information and the proposed scope of its use;
- the period of storing the information;
- the information protection policies in place to safeguard the information;
- the rights of the data subject;
- the individual responsible for data processing; and
- other relevant information.

The Draft Guidelines also take a restrictive position on the transmission of personal information between data processors and preclude the transmission of personal information overseas, unless specific industry rules allow such transmission or it has government approval. Construed narrowly this could prohibit the transfer of information to overseas affiliates which would be unnecessary restrictive and impractical for many business.

The Draft Guidelines define personal information as:

"Any knowable information relating to a natural person that can be used, either alone or in combination with any other information, to specifically identify such natural person."

It is noteworthy that this definition of personal information is very similar to the definition used in the Internet Information Service Provisions (see paragraph 7.2 above).

8. SPECIFIC COMMERCIAL PRACTICES IMPACTED BY THE PROVISIONS

8.1 Ratings and Review

Websites which contain reviews by users or Providers of a Provider's services are popular and, when properly administered, can be a good way of informing consumers on the quality and value-for-money of products and services. However, these rating tools and processes can also be manipulated for commercial gain or otherwise.[27]

Under Article 6 of the Internet Information Service Provisions, where a Provider posts its own or user ratings or reviews of another Provider's services, the methodology and presentation of those ratings and reviews must be fair, objective, and transparent and should not be misleading. The Internet Information Service Provisions specify certain matters for disclosure, for example, information on the reviewer or rater, the methodology of the rating or review, the source of the underlying data and any change to the methodology of rating and review.

[27] A similar debate is going on in the UK about user reports published by Trip Advisor, with claims that many of the reports are from people connected with the hotels or resorts they are supposed to be (objectively) reviewing.

8.2 **Pop-up Windows**

Pop-up advertisements on internet sites are a frequent irritant to the web browsing experience; however, they are a favoured advertising tool that is here to stay. The Internet Information Service Provisions do not limit the number of pop-up advertisements on any site or forbid any category of Provider to engage in pop-up advertising, however, the Internet Information Service Provisions require that, where pop-up advertising is deployed, it is accompanied by a prominently sign-posted option to remove it. It is common in China and elsewhere to see pop-ups on the internet that are virtually impossible to remove or where clicking "removal" or "close" actually takes you into the advertiser's website.

By strengthening the ability of the user to remove pop-up advertising, the Internet Information Service Provisions avoid straying into the difficult territory of defining what is too much or too invasive pop-up advertising. The reality is that both web-hosts and Providers need to use pop-up advertising in a manner and to an extent that will not deter the user otherwise that will be counter-productive to their commercial goals to drive traffic and sales.

8.3 **Software Bundling**

Under Article 9 of the Internet Information Service Provisions, where a Provider has bundled its software with other software it must:

- Give prominent notification of that to the internet user;
- Allow the internet user to positively opt-in as to whether or not to install or use such software; and
- Provide methods to independently uninstall or turn-off such software, without the inclusion of additional or unreasonable conditions.

This is not the first piece of legislation targeted at tie-in selling. Under Article 12 of the AUCL, businesses are already prohibited from:

"against the will of the purchaser, conducting tie-in sale of commodities".

However, perhaps the additional provisions in the Internet Information Service Provisions can be seen as a helpful delineation of the circumstances where software bundling will not be seen as "against the will of the purchaser". Non-compliance with the AUCL has much more serious potential consequences for the infringer than non-compliance with Internet Information Service Provisions (see paragraph 6.4(a) above and paragraph 9 below). The message is again that Providers should monitor their compliance with both the Internet Information Service Provisions and the AUCL.

Please note there are certain other specific commercial practices which are impacted by the Internet Information Service Provisions in addition to reviews, pop-up advertising and software bundling.

9. **PENALTIES AND DISPUTE RESOLUTION**

Under the Internet Information Service Provisions, if a Provider engages in infringing conduct, it can be given a warning, ordered to desist from such conduct and fined between 10,000 and 30,000 Renminbi. These penalties are so minimal that they may not sufficiently deter some Providers from seeking to obtain a competitive advantage by means of acts in breach of the Internet Information Service Provisions. However, as MIIT has the power to make public announcements regarding infringements, reputational concerns might prove a more compelling motor for compliance.

Article 15 of the Internet Information Service Provisions prescribes a dispute resolution mechanism between Providers; it requires that an aggrieved Provider must notify its local MIIT department if it believes that another

Provider has infringed its rights and that this has had a significant negative impact on the consumer. The local MIIT department will then carry out a preliminary assessment of that incident and, where it is thought to be significant, report it to MIIT. This could lead to potential conflicts of interest where MIIT or one of its commercial arms is an investor in the infringer or even where the infringer is a majority state-owned enterprise.

10. CONCLUSION

The Internet Information Service Provisions are a reasonably prompt legislative response by MIIT to the increasing concerns on privacy and competition in the internet space (as highlighted by the "3Q War" and the "CSDN leak" cases (see paragraph 2 above)).

Looked at in isolation, the Internet Information Service Provisions simply contain a shopping list of prohibited activities. At first glance that might appear to be helpful to the market. However, this new legislation does not exist in isolation, and it must be assessed against the wider legislative and regulatory background. When assessed against that background, it is clear that there is much overlap with existing, higher ranking legislation which has more severe penalties and real "teeth". In addition, the failure to give Providers or consumers an independent right of action to pursue damages against a non-compliant Provider where they have suffered losses leaves MIIT with all policing and enforcement responsibilities. It would perhaps have been more effective for Providers (i.e. the market) to have been given a policing role as is the case under the AUCL and the AML (see paragraph 6.4(a) above) or to have given consumers a right to seek redress for non-compliant behaviour.

Therefore, it is unlikely that the Internet Information Service Provisions will significantly change market behaviour. Instead, they create a rather toothless layer of compliance which will not frighten the bigger and dominant players who may be the ones that are driving the smaller players out of the market by a combination of market power and "dirty tricks", and whose strategies and tactics are damaging the rights and interests of consumers.

In short, while overall this appears to be a piece of consumer friendly-legislation, unless the damage to reputation card can be played successfully to force a settlement or the threat of "cross-breach" to the Criminal Law used as negotiating leverage, it is difficult to see how this piece of legislation, of itself, will really help the consumer or smaller companies in the market to combat what appears to be fairly prevalent abusive market behaviour by some of the larger and more powerful players.

www.hoganlovells.com

Hogan Lovells has offices in:

Abu Dhabi
Alicante
Amsterdam
Baltimore
Beijing
Berlin
Brussels
Budapest*
Caracas
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jeddah*
London
Los Angeles
Madrid
Miami
Milan
Moscow
Munich
New York
Northern Virginia
Paris
Philadelphia
Prague
Riyadh*
Rome
San Francisco
Shanghai
Silicon Valley
Singapore
Tokyo
Ulaanbaatar
Warsaw
Washington DC
Zagreb*

*Associated offices