INTERNET REGULATION IN CHINA

DATA PRIVACY IN CHINA

Overview

January 2014

Thomas M. Shoesmith
Pillsbury Winthrop Shaw Pittman LLP
International Practice Group | China Practice
Silicon Valley | Shanghai
tom.shoesmith@pillsburylaw.com

INTERNET REGULATION IN CHINA

DATA PRIVACY

January 2014

1. ***Overview*** – China is one of the world's fastest growing Internet markets. Given the political system of the PRC, the Internet represents both opportunities and challenges for the government in Beijing.

1.1 *Jurisdictional reach* – the principal means by which the PRC regulates the internet is through its jurisdiction over value-added telecommunications service providers whose operations or servers are located in the PRC. It exerts this jurisdiction through approval, licensing, permitting, inspection and reporting obligations imposed on Internet content and service providers in the PRC. Although the PRC does not apply its Internet regulation extraterritorially, its total control over information passing over the Internet in China permits it to restrict or block altogether communications as well as entire domains at will, and it frequently does, even where the operator and all its servers are located outside of China.

The Wall Street Journal reported that one businessman in Beijing experienced strange interruptions in its online communications with a customer in Sweden:

> Fredrik Bergman ran into a problem when a client in Sweden tried to transfer files to his firm's headquarters here: Each time, the firm lost its Web connection for an hour or so. … After several weeks of multiple outages a day, he says, the firm solved the puzzle: the files were named for the Swedish town of Falun, where the client was working. Mr. Bergman says his firm thinks the name triggered the filters China's online censors use to block discussion of Falun Gong, a religious group long banned in China.

(a) International operators frequently create Chinese-language websites and carry on business without worrying about PRC licensing or regulation. The new Chinese-language website of the New York Times, for example (cn.nytimes.com), is operated entirely on servers located outside of China. This has not, and will not, prevent Beijing from DNS-poisoning or otherwise blocking parts or all of the website if it decides to do so.

(b) Why should an international operator subject itself to PRC licensing and regulations? As a practical matter, there are several reasons.

- Many customers in the PRC cannot or will not pay for services or other items in U.S. dollars. In order to accept Renminbi, the Chinese currency, the operator must have a PRC legal presence.

- Internet speeds are seriously degraded for PRC users accessing websites hosted outside of China because all international Internet traffic is routed through government-controlled gateways. Many companies feel this puts them at a significant enough competitive disadvantage that they are forced at least to mirror their sites on servers in the PRC or set up local servers.

- Companies often feel they need to have permanent employees in China for business reasons, and this requires a local presence. Although a company's servers could still be outside of China, the vulnerability of its local company and the employees to immediate government regulation often leads the company to local its servers in China as well.

1.2 *Restrictions on foreign investment* – unfortunately, foreign investors are restricted by law from owning more than 50% of an entity holding an Internet content provider (ICP) license. As a practical matter, since so few joint venture ICP licenses have been granted, foreign investors cannot hold any ownership interest at all in an ICP company. This forces international internet companies and investors into a "VIE" or variable interest entity structure, which exists in something of a gray area in China. See §3.7.

1.3 *Regulatory environment* – even in a system where it often seems government approval is required for even the most minor activity, the Internet is heavily regulated. The Ministry of Information and Industry Technology (MIIT) and the General Administration of Press and Publication (GAPP) are the two principal agencies involved in regulating activity on the Internet, but at least 20 other national-level agencies are also involved, in addition to an almost countless number of provincial and local authorities. See §2. In addition to overt government regulation, operators are required to engage in extensive and elaborate self-censorship, as well as collection of data on users which must be turned over to authorities on request. The PRC government leads the world in the sophistication of its electronic monitoring of Internet activity, and it can and frequently does intervene to block communications considered offensive or dangerous and punish those involved.

2. ***National-level ministries and other bodies with oversight or regulatory authority***

2.1 State Council

2.2 State Council Information Office ((SCIO)

2.3 State Commission Office for Public Sector Reform

2.4 Standing Committee of the National People's Congress

2.5 Ministry of Industry and Information Technology (Ministry of Information Industry (now MIIT)), formerly Ministry of Information Industry (now MIIT) and before that, MPT

2.6 Ministry of Commerce (MOFCOM)

2.7 Ministry of Culture (MOC)

2.8 Ministry of Education (MOE)

2.9 Ministry of Public Security (MPS)

2.10 Ministry of Human Resources

2.11 State Administration of Radio, Film and Television (SARFT)

2.12 General Administration of Press and Publication (GAPP)

2.13 State Administration of Industry and Commerce (SAIC)

2.14 State Administration of Foreign Exchange (SAFE) – through regulation of international payments and foreign exchange

2.15 China Securities Regulatory Commission (CSFC)

2.16 National Copyright Administration

2.17 National Office of Combating Pornography and Illegal Publications

2.18 State Food & Drug Administration (SFDA)

2.19 Public Security Bureau (PSB)

2.20 State Secrecy Bureau

2.21 Social Insurance and State Archives Administration

2.22 State Cryptography Administration Bureau (SCAB) (formerly State Encryption Administration Commission

2.23 State Administration of Traditional Chinese Medicine

2.24 People's Bank of China (PBOC)

3. ***Basic regulatory scheme and licensing requirement*** – the PRC has regulated "value-added telecommunications" since 2000. Most activities using or relating to the Internet are swept into the definition of "value-added telecommunications," or VAT. The principal regulatory agencies are Ministry of Information Industry (now MIIT) and GAPP, but many other agencies also have authority over various aspects of the Internet.

3.1 *Telecommunications Regulations of the People's Republic of China* (State Council Decree No. 291, promulgated September 25, 2000) – the primary PRC law governing telecommunications services.

(a) *Definition of VATS*: Arts. 7 and 8 of the *Telecom Regulations* draws a distinction between "basic telecommunications services" and "value-added telecommunications services." The *Telecom Regulations* define value-added telecommunications services as telecommunications and information services provided through public networks. The "*Catalogue of Telecommunications Business,*" which was issued as an attachment to the *Telecom Regulations* and updated in February 2003, identifies online data and transaction processing, on-demand voice and image communications, domestic Internet virtual private networks, Internet data centers, message storage and forwarding (including voice mailbox, e-mail and online fax services), call centers, Internet access, and online information and data search as value-added telecommunications services.

(b) *Licensing requirement.* Art. 7 states that no person may engage in telecommunications business operations activities without an operating permit.

(c) *Basic requirements.* Any person operating any value-added telecommunications business must fulfill certain basic conditions (Art. 13):

- Be a legally established company;
- Have appropriate funds and professionals required for its business;
- Have the reputation or capability of providing long-term service to subscribers; and
- Other conditions as may be prescribed by the authorities.

(d) *Application process.* The approval agency is the MIIT. Original applications and any applications for any changes to business operations must be approved by the competent office of the MIIT (Arts. 14-15).

3.2 The *Regulations (Measures) for the Administration of Internet Information Services* (State Council Decree No. 292, promulgated September 25, 2000), sometimes referred to as the "Internet Information Services Rules" or the "Measures" require all commercial telecommunications service providers to procure operating licenses prior to commencing operations. See below for "non-commercial" operators.

(a) *Internet information services defined.* Art 2 of the Measures defines "internet information services" as "the service activity of providing information to Internet users through the Internet"

(b) *Commercial versus non-commercial operations.* Art. 3 of the Measures draws a distinction between:

- *Commercial Internet information services*, defined as "the provision of information, web page production or other services to Internet users through the Internet for compensation; and
- *Non-commercial Internet information services*, defined as "the provision of public and shared information services to Internet users through the Internet without compensation."

(c) *Permit and licensing system for commercial internet service providers.* Art. 4 establishes a permitting system for all commercial internet information service operators (ICPs).

- Operators must apply to the local Communications Administration Bureau of the Ministry of Information Industry (now MIIT) for a license. This is generally a provincial-level office, but in areas under the direct supervision of the central government (such as Beijing and Shanghai), the application is to municipal authorities (Art. 7).
- There may also be separate local licensing requirements, as there are in Shanghai and Guangzhou.
- Among other things, an applicant must maintain a business development plan; maintain network and information security procedures, including measures to ensure user privacy; and obtain permits from sector-specific ministries, where applicable (Arts. 5, 6).
- The local MIIT office is required to act within 60 days of the application (Art. 7); if the permit is denied, a written explanation of the reasons must be provided.
- The operator must also obtain a business license from the relevant office of the State Administration of Industry and Commerce (AIC) (Art. 7).
- Operators are strictly limited to the activities set out in their operating permits and any changes to business scope, website address, etc. must be approved in advance (Art. 11).
- ICPs must post their operation license numbers on their websites (Art. 12).
- Licenses are domain-specific, so multiple domains will require multiple licenses.
- Operators must maintain records for up to 60 days of all content on their websites, subscriber access counts, account numbers of subscribers, and other in-

formation—and to submit that information to the relevant government authorities.

(d) *Non-commercial ICPs* – non-commercial ICPs are subject to a record filing procedure rather than a licensing requirement (*Measures*, Art. 8). Non-commercial ICPs may not engage in services for compensation (Art. 11).

Until draft regulations were circulated for comment in 2012, the distinction between commercial and non-commercial ICPs turned on whether users of the content are charged, see §3.2(b). It has not been clear how to apply this in situations where the business model depends on advertising revenue or other approached. The rule of thumb that, if you are using the Internet to make money—from anyone—you are in the commercial sphere, was useful but difficult to support in the actual letter of the law.

- In the *Circular on Issues Concerning the Administration of Internet Information Services* (Ministry of Information Industry, the Ministry of Information Industry, effective 16 September 2002) the Ministry of Information Industry (now MIIT) tried to clarify this question by suggesting that ICPs which do not charge users for accessing content and which do not provide paid-for webpage design services and which are driven by, say, advertising revenues—for example, a company website—are not treated as commercial ICPs. On the other hand, websites where sellers pay fees, or online gaming websites where users pay a fee to access online content, would clearly involve "commercial ICP" operations. One commentator draws the distinction between whether it is the service or the article which is paid for. Local authorities in Beijing and elsewhere took a differing view, adding to the confusion.

- The problem of this definition arises most often where the Internet service is a component of another product or service, such as a company's website which offers downloadable support, online support or other information to customers buying its product.

(e) *Bulletin board services.* Art. 9 of the Measures requires a special filing for operators of electronic notice services.

(f) *Information collection and retention.* Art. 14 of the Measures requires all ICPs that engage in news, publishing and electronic notice services to record the contents of information distributed and the time distributed, as well as Internet addresses or domain names, and record user online time, user account numbers, Internet addresses or domain names and the telephone numbers of Internet users. These records must be kept for 60 days and made available to the authorities on request.

(g) *Prohibited content*. Art. 15 of the Measures contains an extensive list of topics which ICPs may not permit to be published, see §3.6.

(h) *Self-censorship.* Art. 16 of the Measures requires any ICP which discovers impermissible content being transmitted by its website to discontinue the transmission, keep "relevant records" and report the matter to the authorities.

(i) *Penalties.* The September 25, 2000 Measures provide for civil and criminal penalties, including suspension or revocation of licenses, forced suspension of operations, etc. (Arts. 19-26).

3.3 *Measures on the Administration of Telecommunications Business Operating Permits* (Ministry of Information Industry (now MIIT), promulgated March 1, 2009) (the "Telecom License Measures)

(replaces the previous *Administrative Measures for Telecommunications Business Operating Licenses* (or 2001 Telecom Operating Measures)).

(a) The Telecom License Measures draw a distinction between operators involved in basic telecommunications services and those involved in value-added telecommunications services.

(b) A distinction is also made as to whether a license is granted for intra-provincial or "trans-regional" (inter-provincial) activities. An appendix to each license granted will detail the permitted activities of the enterprise to which it was granted.

3.4 *Sector-specific permits, licenses and approvals* – a wide range of agencies with authority over various aspects of the Chinese economy (health care, media, education, etc.) have concurrent jurisdiction over Internet-based or -enabled activities within those industries. The authority of the various ministries to regulate internet activity in their areas was explicitly confirmed in Art. 5 of the September 25, 2000 State Council Measures (see §3.2).

3.5 *Local and provincial regulation* – in addition to national-level laws, regulations and administrative circulars, many provincial and even local jurisdictions have promulgated their own regulations and procedures. Some of these supplement or complement national regulations; in other cases they address matters not yet addressed at the national level, such as e-signatures (Guangdong). Generally the provincial or local office of MIIT is the place to start, along with the local office of the relevant sectoral ministry.

3.6 *Broad control over content* – a number of regulations, including Art. 15 of the September 25, 2000 Measures, prohibit any involvement in Internet content that:

(a) opposes the fundamental principles stated in the PRC constitution;

(b) compromises national security, divulges state secrets, subverts state power or damages national unity;

(c) harms the dignity or interests of the state;

(d) incites ethnic hatred or racial discrimination or damages inter-ethnic unity;

(e) undermines the PRC's religious policy or propagates heretical teachings or feudal superstitions;

(f) disseminates rumors, disturbs social order or disrupts social stability;

(g) disseminates obscenity or pornography, encourages gambling, violence, murder or fear or incites the commission of a crime;

(h) insults or slanders a third party or infringes upon the lawful rights and interests of a third party; or

(i) is otherwise prohibited by law or administrative regulations

3.7 *Regulation of foreign investment in value-added telecommunications* – in theory, 50/50 joint ventures are possible, but they are rare in practice.

(a) The *Regulations for the Administration of Foreign-Invested Telecommunications Enterprises* (the "FITE Regulations") (State Council, promulgated December 11, 2001 and

amended on September 10, 2008) require that telecommunications enterprises in the PRC with foreign investors (FITEs), must be established as Sino-foreign equity joint ventures.

(b) The *Notice of the Ministry of Information Industry on Intensifying the Administration of Foreign Investment in Value-added Telecommunications Services* (MIIT, July 13, 2006) states that its purpose is to strengthen of the administration of foreign investment in PRC telecommunication businesses, particularly those involving value-added telecommunications services. The notice requires value-added telecommunications companies to have sufficient business premises and facilities (including servers), within the region covered by their ICP licenses, to support the services that they provide in the applicable region. The notice also provides that the entity holding the ICP license must be the entity that possesses the key intellectual property rights, e.g., domain names and trademarks. For discussion of regulation of ICPs, see §4. Note that MIIT approval is needed for any ICP Joint Venture.

(c) The restrictions on foreign investment in the Internet have forced virtually all international investment into "VIE" or "variable interest entity" structures. These are described in Annex B.

4. *Internet information services and Internet Content Providers, or (ICPs)*

4.1 *Measures for the Administration of Internet Information Services* (or the "ICP Measures") (State Council, September 25, 2000), also discussed above at §3.2.

(a) *License requirement.* Any entity that provides information to online users on the Internet is obliged to obtain an operating license from the Ministry of Information Industry (now MIIT) or its local branch at the provincial or municipal level in accordance with the *Telecom Regulations*, see §3.1. Non-commercial Internet information service providers must register but the 2000 Internet Information Services Rules (Art. 4) do not require a license.

(b) *Foreign JVs.* ICPs must obtain the prior consent of MIIT prior to establishing an equity or cooperative joint venture with a foreign partner.

(c) *Coordinate jurisdiction.* Entities providing online information services regarding news, publishing, education, medicine, health, pharmaceuticals and medical equipment must procure the consent of the national authorities responsible for such areas prior to applying for an operating license from MIIT or its local branch at the provincial or municipal level.

(d) *Display of ICP licenses.* ICPs must display their operating license numbers in conspicuous locations on their home pages. Note that a separate license is required for each domain name.

(e) *Self-censorship.* ICPs are required to police their websites and remove certain prohibited content. This is known as "information security."

5. *Privacy and data protection*

5.1 *Overview*

(a) *Privacy from governmental authorities.* As a general proposition not much, if anything, that passes over the Internet in China is private from the government. Various regulations require record-keeping by operators and the turning over of that information to the government on request or on a periodic basis. The PRC Constitution implies a right to privacy, but the law in this area is not well developed.

(b) *Privacy protection for personal data.* "Personal information" has been variously defined over the years, most recently in the 2011 MIIT Provisions, see §5.7, and the 2013 non-binding national standards, see §5.9. As noted below, however, data privacy has only recently been addressed on a comprehensive basis in the PRC.

5.2 *Background.* Until very recently, data privacy was only addressed on a piecemeal basis under PRC law. The seminal regulations in September 2000, see §3, did not address data privacy. Over the following years, various agencies of the Chinese government promulgated rules touching on data privacy in the banking, health care, and other sectors, but no comprehensive legislation or regulatory pronouncements appeared more than ten years later.

(a) The PRC Constitution contains provisions some observers have pointed to as creating a right to privacy. For example, Art. 40 guarantees the right to freedom of communication and purports to protect private communications. Art. 38 guarantees the right of individuals to be free from restrictions on "dignity" and from defamation, false accusations and insults.

(b) In 2003, the PRC government established a working group composed of lawyers and academics to study the question of the protection of personal information. The group produced draft *Personal Information Protection Measures* in 2005. The Measures were never enacted but served as a reference for local authorities considering their own regulations.

(c) General principles of the PRC Civil Law protect an individual's right to his/her name, likeness, reputation and honor (see Art. 120).

(d) The PRC Postal Law guarantees the security of material sent by physical or electronic mail.

(e) The Social Insurance Law prohibits the government from disclosing personal information.

(f) In 2009, revisions to the PRC *Criminal Law* added sanctions for the unlawful disclosure or acquisition of certain kinds of personal information.

(g) The 2010 PRC *Tort Law* also contained new privacy provisions, see §5.11.

(h) The 2011 regulation concerning PRC identity cards contained provisions protecting information gathered by the authorities, see ¶5.6.

(i) The 2013 *Provisions on Protecting the Personal Information of Telecommunications and Internet Users* regulates the collection and use of personal data on the internet.

5.3 On June 7, 2011, the MIIT and the National Internet Information Office jointly published draft amendments to the September 25, 2000 *Regulations of Internet Information Services*; see §3.2 above. The Draft Amendments would add data privacy provisions to this basic regulation, and would also add a "real name" requirement.

(a) *Scope.* The Draft Amendments would make the basic regulation applicable to anyone that "engages in internet information service activity in the People's Republic of China." The phrase "internet information services" means "the service activity of providing information services through the internet" (Art. 2), and persons providing that service are referred to as "internet information service providers" or IISPs.

- Note that the Draft deleted the phrase "to online subscribers" from the original definition in the Regulations.

(b) *ISP versus ICP*. The Draft Amendments continue the confusion caused by the original *Regulations* by referring to persons who provide information services using the Internet as "ISPs" rather than ICPs. For example, Art. 11 of the Draft Amendments contains the following confusing sentence: "The provider of internet access service shall verify the qualification of the ISP, and shall not provide the service to the unqualified ISP." The term "Internet Service Provider" is generally understood to refer to a person who provides Internet access services, and it seems clear that the drafters are using "ISP" to mean what the industry refers to as an "ICP."

(c) *Commercial versus non-commercial.* The Draft Amendments (Art. 6) would continue the licensing requirement for commercial ICPs and the record filing requirement for non-commercial ICPs.

(d) *Real name requirement.* Art. 15 of the Draft Amendments would require the collection of a user's real name and identification, perhaps limited to situations where the user was posting or publishing information over the Internet (as opposed to merely viewing or downloading).

5.4 On July 27, 2011, MIIT published draft *Provisions on the Administration of Internet Information Services*. The draft provisions eventually became the December 29, 2011 *Several Provisions*, discussed below at §5.7.

5.5 On September 23, 2011, the Standing Committee of the Jiangsu Provincial People's Congress issued the *Regulation of Information Technology of Jiangsu Province*. Jiangsu was the first province to put in place general rules for the protection of personal data, as opposed to regulations only applicable to certain industries, such as banking or health care. The Jiangsu regulations took an approach which was later substantially mirrored in the 2013 national guidelines discussed below.

5.6 On October 29, 2011, the Standing Committee of the National People's Congress promulgated an amendment to the *PRC Law on Resident Identity Cards* to further protect the information on those cards. Every PRC citizen must obtain a resident identity card when reaching 16 years of age, and the cards must be presented in a wide variety of situations. The amendments obligate any third party who gains access to the information on a resident identity card to keep that information confidential, and provide for administrative fines for breaches of this obligation.

5.7 On December 29, 2011, the MIIT published the *Several Provisions on the Order of the Internet Information Service Market*, which became effective March 15, 2012.

(a) *Scope.* The Provisions regulate any person or entity "engaging in the provision of internet information services and activities relating to internet information services within the People's Republic of China."

(b) *Personal information defined.* The Provisions define "personal information" for the first time in PRC law as "any information associated with a user which, either independently or when combined with other information, is able to identify such user (Art. 11).

(c) *Protection of data privacy.* Art. 11 of the Provisions requires ICPs to:

- Refrain from collecting users' personal information without their consent, unless otherwise required or permitted by law or regulation;

- Only collect personal information necessary to provide their services;

- Expressly inform users of the method, content and purpose of the collection, process and use of personal information;

- Only use personal information as necessary for the stated purpose;

- Maintain the security of personal information and not disclose it to any third party without the individual's consent, unless otherwise provided by law or regulation; and

- Immediately take remedial measures in the event of any actual or potential data breach, if there are or could be "serious consequences" resulting, including reporting to the relevant governmental authorities, and cooperate with the authorities in any subsequent investigation or proceeding.

(d) *Provisions on data security.* The Provisions also contain a number of prohibitions intended to strengthen the security of personal data maintained by ICPs. Thus, Art. 13 of the Provisions states:

- ICPs may not arbitrarily modify or delete personal information without justifiable cause;

- ICPs may not provide personal information to a third party without the consent of the user (this tracks the provisions of Art. 11);

- ICPs may not transfer user information, either arbitrarily or by falsely using the user's name; and

- ICPs may not deceive, coerce or mislead a user into consenting to the release of personal information to third parties.

(e) *What constitutes "consent?"* The Provisions are silent on what constitutes a user's "consent." EULAs and standard privacy policies are likely to become a regular feature of PRC websites, with all the uncertainty they bring in other parts of the world.

5.8 On December 28, 2012, almost exactly one year after the MIIT *Provisions,* the Standing Committee of the National People's Congress published a *Resolution Relating to Strengthening the Protection of Information on the Internet.* The Standing Committee has the power to enact laws of national application which rank just below the "basic laws" promulgated by the National People's Congress itself.

(a) The Resolution provides that the State will protect "electronic information that can identify individuals and implicate their private affairs." This is a description of data which comes close to the 2011 MIIT *Provisions*' definition of "private information."

(b) The Resolution also provides that no organization or individual may misappropriate or otherwise obtain electronic personal information by unlawful means, or sell or otherwise unlawfully provide it to any third party.

(c) The Resolution gives some indication of what means might be "unlawful" by providing that ISPs and "other businesses that handle electronic personal information" must:

- Adopt and comply with rules for collection and use of electronic personal information, and make such rules known;

- Clearly state the purpose, means and scope of their collection and use of electronic personal information;
- Obtain the consent of the data subject for any collection and use of data;
- Maintain electronic personal information in strict confidentiality;
- Not sell, divulge, alter or destroy electronic personal information obtained in the course of their business activities;
- Adopt information security safeguards to protect the confidentiality of electronic personal information;
- Take immediate remedial measures in the event of any data breach; and
- Report any data breaches to "relevant government agencies."

(d) The Resolution requires all ISPs to require all users to provide their real names on agreements for the provision of access- or information-related services.

(e) The Resolution provides for a private right of action for anyone injured by a breach of the provisions.

(f) There were no clear penalty provisions or delegations of administrative authority in the *Provisions*, so they did not appear to have a significant impact on company practices.

5.9 On February 1, 2013, the *Guidelines for Personal Information Protection within Public and Commercial Information Systems* (MIIT Standardization Administration of China, issued Nov. 5, 2012)(the "Guidelines") became effective. These were first national-level data privacy standards in China. These Guidelines do not have the force of law but are intended to serve as a national standard. The Guidelines are sometimes called the "Third Line" of protection, after the 2011 *Provisions* and the 2012 State Council *Resolutions.*

(a) *Personal information defined.* The Guidelines define "personal information" as "computer data that may be processed by an information system, relevant to a certain natural person, and that may be used solely or along with other information to identify such natural person."

- The 2011 MIIT Provisions used a similar definition, see §5.7(b).
- The 2006 E-mail Measures had defined personal information as any "information provided during the registration of an email account," a definition which is at once narrower and broader than in the Guidelines.
- The 2003 *Regulations of the Shanghai Municipality on the Protection of Consumers' Rights and Interests* more broadly defined "personal information" as including "the names, sex, occupations, education, contact details, marital status, income and property, fingerprints, blood types, medical history and other information that is closely related to the consumers themselves and their families." Although these Regulations were limited to consumer transactions within Shanghai, some reporters believe they were considered in arriving at the definition in the 2013 Guidelines.

(b) *Sensitive personal information defined.* The Guidelines define "sensitive" personal information as information that could have a negative impact on an individual if publicly disclosed, such as identifying data, political or religious views, etc.

(c) *Broad scope*. The Guidelines apply generally to all organizations and entities, including government bodies (unless engaged in "public management functions") and non-commercial enterprises. This is broader than other promulgations, which apply only to telecommunications service providers (TSPs) and ISPs. All "computer information systems" are covered, and notably, there is no requirement that such systems be connected to the internet.

- *Administrators of personal information.* The Guidelines define "administrators of personal information" as "organizations and institutions, which determine the purpose and manner of personal information processing, actually control personal information, and use information systems to process personal information." (Art. 3.4). This is written in the conjunctive, so all three legs must be satisfied. Administrators must notify individuals when there are data breaches, report "major incidents" to the authorities, and the like.

- *Receivers of personal information.* The Guidelines define "receivers of personal information" as "individuals, organizations and institutions, which obtain personal information for information systems, and handle [the information] in accordance with the consent of the individual." This is often called a "data processor" in other countries.

(d) *Basic principles*. The Guidelines set out eight general principles (the "Eight Principles") for handling personal information and data:

- The collection and use of personal information should be with at least the *tacit* informed consent of the individual, and the individual should have raised no objection to the collection and use of the data;

- Sensitive personal information should not be collected or used without the *express* consent of the individual, and evidence of that consent should be retained by the entity collecting or using the information;

- The individual should have the right to receive accurate information on the content of the information retained, the source of the information, purpose and scope of use, and purpose and scope of any dissemination;

- The individual should have the right to request emendation or correction of information maintained, as well as the right to request the operator to cease using and to delete information;

- Collection of information on children would be prohibited without parental consent

- Personal information should not be transferred outside of the PRC without the individual's express consent, government permission or other explicit legal or regulatory permission;

- Entities should establish internal procedures and measures to protect personal information from unintended or unauthorized disclosure; and

- Personal information should not be retained for longer than necessary.

(e) *Life cycle guidance.* The Guidelines describe what operators should do throughout the life cycle of data collection (collection, processing, transfer, deletion).

- *Collection phase.* At the time of data collection, the individual must receive notice of nine categories of matters – purpose, means and content of collection; duration of retention; security measures; risks of inadvertent disclosure; consequences of not providing the information; contact details for the administrator, and complaint process. The individual must also be informed of the circumstances under which data may be transferred to a third party. The Guidelines prohibit indirect or undisclosed gathering of information and collection of data on minors or those who are not legally competent.

- *Processing phase.* Individuals whose data is collected are given certain rights during the "processing phase." For example, they have the right to access and correction, and the Guidelines specify what administrators must do when subjects request either access or correction.

- *Transfer phase.* Article 5.4.5 makes clear that no transfer of personal information to an overseas receiver is permitted without the express consent of the subject. There is no exception for intra-company transfers. It is not clear whether the use of a cloud constitutes an overseas transfer.

- *Deletion phase.* Art. 5.5 gives the data subjects the right to seek timely deletion of personal information "for proper reasons" in addition to the general obligation to delete information when it is no longer needed.

5.10 On July 16, 2013, the MIIT promulgated the *Rules Regarding the Protection of Personal Information of Telecommunications and Internet Users* (MIIT, adopted July 16, 2013, effective Sept. 1, 2013) (the "2013 Rules"). These are the first regulations specifically addressing the protection of personal information in e-commerce situations.

(a) The 2013 Rules apply to telecommunications service providers and all ICPs.

- Note that an email service provider or a cloud computing company could be classified as a telecommunications service provider under the Rules.

- The Rules do not apply to the use of personal data by individuals or other types of businesses.

(b) "Personal information" refers to information that can be used to identify an individual, including names, birth dates, ID numbers, addresses, telephone and account numbers, passwords, etc. Information tracking time and place of use of internet services can also be seen as constituting "personal information."

(c) Requirements of the 2013 Rules:

- Users' consents must be obtained before collecting or using personal information

- Users must be informed of the reason, measure and scope of any collection or use

- Personal information may not be disclosed, destroyed, sold or illegally provided to a third party

- TSPs and ICPs must formulate and public detailed rules regarding their collection and use of personal data, and post the rules at their physical and virtual premises

- Collection of data which is not necessary for the provision of the relevant services is prohibited

- Collection must cease upon termination of the service; and users must be given the option to cancel their accounts

- TSPs and ICPs are required to supervise third-party outsourcers or service providers (e.g., cloud computing company) to ensure compliance with the Rules

- TSPs and ICPs must establish security management systems and policies, ensure that physical media are kept secure, and monitor their systems

- Penalties include warnings and fines.

5.11 The *PRC Tort Liability Law* (adopted by the Standing Committee of the National People's Congress on December 26, 2009, effective July 1, 2010) provides generally for a "right to privacy", and includes a private right of action for violations of that right. Provisions of the *Law* make website operators liable for infringement of an individual's privacy right if they are warned of the infringement and refuse to remove the offending post.

5.12 The 2009 amendments to the *PRC Criminal Law* make it illegal to sell or otherwise unlawfully provide to third parties personal data which has been collected by the defendant in the course of his duties, and for any person to obtain personal information from any source by means of theft or other unlawful means.

5.13 *Medical records*. The 2010 *PRC Tort Law* required medical institutions to establish and keep various types of medical records, and the maintain the confidentiality of those records. Patients have a private right of action for unauthorized disclosure of their information. The Ministry of Health published the *Basic Norms for Electronic Medical Records* on February 22, 2010, effective April 1, 2010, which prohibit the unauthorized disclosure of patient information. The *Norms for Electronic Medical Records of Traditional Chinese Medicine (Trial Implementation)* (State Administration of Traditional Chinese Medicine, issued April 21, 2010, effective May 1, 2010) establish information security requirements for electronic medical records.