University of New South Wales
University of New South Wales Faculty of Law Research Series
2012

Year 2012 *Paper* 13

China's Internet data privacy Regulations 2012: 80% of a Great Leap Forward?

Graham Greenleaf*

*University of New South Wales, g.greenleaf@unsw.edu.au

China's Internet data privacy Regulations 2012: 80% of a Great Leap Forward?

Graham Greenleaf

Abstract

Internet-based businesses in China have until now not been required to comply with any comprehensive data privacy law, but from March 15, 2012 business providing 'Internet information services' in China must comply with a much more comprehensive data privacy law, which can be briefly called the Internet Information Services Regulations. 'Internet information service provider' refers to all parties providing information to Internet users over the Internet. The Regulations use a definiton that is similar to the definition of personal data used in laws in other countries, and clearly implies that this is broader than information collected from the user, such as information collected from third parties or information generated by the IISP itself from transactions with the user. They are to be enforced by China's various 'Telecommunications Authorities'.

The data privacy principles in the Regulations are analysed here in accordance with the usual division of privacy principles found in such instruments as the OECD Guidelines, and other principles developed since then. They are on the one hand surprisingly comprehensive, but on the other hand have a couple of major omissions. The enforcement methods in the Regulation are diverse, but primarily at the initiative of the Telecommunications Authorities. They do not include civil damages provisions, but these may be provided by other aspects of Chinese law, read in conjunction with these Regulations.

Commentators on China's Internet industry expect that these Regulations will be actively enforced, in part as a result of a string of widely publicised unauthorized disclosures of user information by Internet companies in 2011, and that some industry sectors will have considerable compliance problems. The article concludes with reasons for the significance of these Regulations, and how they compare with

international standards. The Regulation is a very significant step for China, even if it would be a very limited one in other countries.

China's Internet data privacy Regulations 2012: 80% of a Great Leap Forward?

Graham Greenleaf, Professor of Law & Information Systems, University of New South Wales[*]

Privacy Laws & Business International Report, Issue 116: 1-5, April 2012

15 April 2012

Contents

[*] Paul McKenzie of Morrison & Foerster, Beijing Office, and Bonnie Li and Julianne Doe of SNR Denton, Hong Kong office, have provided valuable comments on this article, but responsibility for any views stated remains with the author.

Internet-based businesses in China have until now not been required to comply with any comprehensive data privacy law, although they could sporadically be affected by the protection of reputation and (more recently) privacy under the General Principles of Civil Law (1986), by the specific protection of privacy under the Tort Liability Law (2010), and under the criminal law.

From March 15, 2012 business providing 'Internet information services' in China must comply with a much more comprehensive data privacy law, which can be briefly called the Internet Information Services Regulations[1], made as a Decree of the Ministry of Industry and Information Technology (MIIT), and available in an unofficial English translation[2].

Scope of the Regulation

Private sector activities regulated: IISPs

The Regulations state that 'All those that are engaged in Internet information services and/or activities relating to Internet information services in the People's Republic of China shall comply with these Regulations' (A 2). The expression 'Internet information services provider' (IISP) is then used throughout. McKenzie and Fang explain[3] that although 'Internet information service' is not defined in the Regulation, the term 'IISP' is broader than it might at first seem:

> 'This is a term drawn from regulations issued by the State Council in 2000 that simply refers to parties providing information to Internet users over the Internet. As such, not only Chinese Internet companies whose principal business is online (and whose operations require a license from MIIT) but also other Chinese companies whose online activities are more limited are required to comply with the Internet Regulations in their online operations.'

The scope is therefore not limited to 'ISPs' but 'can include e-commerce entities, advertising companies and mobile service providers, among others'.[4] However, the scope of the Regulations also seems to apply to non-profit activities using the Internet. Article 2 does not limit its scope to businesses, and the earlier Regulation in 2000 distinguishes 'profitable' and 'non-profitable' Internet information services but applies to both.[5]

Nevertheless, the Regulations do not apply to business or non-profit activities which are not related to Internet information provision, or even to activities which use the Internet but are

---

[1] The full title is 'Several Regulations on Standardizing Market Order for Internet Information Services'. They were adopted at the 22nd Executive Meeting of the Ministry of Industry and Information Technology of the People's Republic of China, as a Decree of the Ministry of Industry and Information Technology (No. 20) (Minister: Miao Wei) on December 7, 2011 and published on December 29, 2011 for implementation as of March 15, 2012.

[2] The translation quoted in this article is by Morrison & Foerster LLP's Beijing Office, and available on request from <chinamarketingteam@mofo.com>. Their considerable assistance with this article is acknowledged gratefully.

[3] McKenzie P and Fang J 'China's Online Data Privacy Rules Coming into Effect; Other Recent Data Privacy Developments in China' *Morrison & Foerster Client Alert*, February 23, 2012, available at <http://www.mofo.com/files/Uploads/Images/120223-China-Privacy.pdf>

[4] Chan, H 'China e-commerce braces for privacy crackdown' *Business Law Currents* Thomson Reuters ACCELUS, March 8, 2012

[5] Article 3 of the *Regulation on Internet Information Service of the People's Republic of China* (State Council September 25, 2000) provides that 'internet information service is divided into two categories: profitable Internet information service and non-profitable Internet information service'.

not for the provision of information to users, such as purely intra-company matters. The regulations also do not apply to the public sector, in common with the data privacy laws in Vietnam, Malaysia and (for now) India, and as proposed in Singapore.

Personal information covered

The Regulations refer to 'any information that relates to a user and that separately or in combination with other information may be used to identify the user' as 'User's Personal Information' (A 11). This is similar to the definition of personal data used in laws in other countries, and clearly implies that this is broader than information collected from the user, such as information collected from third parties or information generated by the IISP itself from transactions with the user. Other regulations only have more limited scope and apply to 'information uploaded by a user' (A 13), which reinforces the interpretation that 'User's Personal Information' has a broader scope.

Authorities involved

The supervision and administration of IISPs under the Regulation is by 'the Ministry of Industry and Information Technology and the communications administration authorities of all provinces, autonomous regions and municipalities directly under the central government' who are collectively referred to as the 'Telecommunications Authorities' (A 3). Business may therefore have to deal with Chinese authorities at multiple levels of government in relation to these Regulations.

Data privacy principles

The data privacy principles in the Regulations are in detail in Articles 11-14, and also encapsulated briefly in the requirement that IISPs 'shall provide services in accordance with the principles of equality, free will, fairness and good faith' (A 4). They are analysed here in accordance with the usual division of privacy principles found in such instruments as the OECD Guidelines, and other principles developed since then.

Collection limitations

Collection is not simply limited to relevant information, but is limited by the higher standard of minimal collection: 'Without the user's consent [an IISP]… shall not collect any information other than that required for its provision of service …' except as otherwise required by law (A 11).

Notification of purpose of collection

The user must be expressly given notice of the purpose ('use') for which the information is collected: 'When an Internet information service provider collects any User's Personal Information after obtaining the user's consent, such provider shall expressly inform the user of the means by which such User's Personal Information will be collected and processed, as well as the content and use of such information…' (A 11). No such notification is required when information about users is collected from third parties.

Limits on use and disclosure

The same provision limits the use of the information collected to the purpose for which it was collected, stating that an IISP '… shall not use any User's Personal Information for purposes other than its provision of service.' (A 11). Whether 'use' also includes disclosure (provision of information to others) is not clear from the context.

Concerning disclosures to others, Article 13(2) is even more strict, stating that an IISP shall not 'provide the information uploaded by a user to others without the user's consent, except as required by laws or administrative regulations'. These two provisions therefore leave uncertain whether an IISP is limited in whether it can disclose information about its users which it has generated itself or it has collected from third parties.

There is a further specific restriction that an IISP shall not 'transfer the information uploaded by a user without authorization or in the guise of the user's name, or deceive a user into transferring, or mislead or force a user to transfer, the information uploaded by such user' (A 13(3)).

Data quality

There are no requirements on IISPs to maintain the quality of user data (timeliness, relevance etc) except that they must not 'modify or delete the information uploaded by a user without authorization for no justifiable reason' (A 13(1)) or 'do any other things that may harm the information updated by any user' (A 13(4)).

Security of data

There is a general obligation on IISPs to 'properly keep' User's Personal Information (A 12), and an additional obligation that only applies to information uploaded by users, to 'strengthen their system security protection, legally safeguarding the security of information uploaded by users, and ensure users' ability to use, modify and delete the information updated by them' (A 13).

Data breach notification

The Regulation has a broad provision requiring data breach notifications to the authorities:

> 'when any User's Personal Information kept by [an IISP] has been leaked or may be leaked, it shall immediately take remedies therefore; in the event that such leakage has resulted in or may result in any serious consequence, the [IISP] shall immediately report such event to the Telecommunications Authority that granted the provider its Internet information service permit or filing, and shall cooperate with the relevant authority in investigating and dealing with the event.' (A 12)

Taken literally this does not require any notification to the data subjects. However, it is apparently the usual practice of the MIIT to request IISPs to notify data subjects when User's Personal Information kept by the IISP has been leaked or may be leaked. For example, when there were large scale personal data leaks from ISPs in 2011, the MIIT issued a notice to all IISPs in the PRC requesting them to notify and remind users to change their user name and passwords. The notification method required may include website announcement, email, phone calls and SMS.

Accountable data controller

An OECD-like notion of an accountable data controller requires an IISP to 'prominently publicize its effective contact details, accept complaints from users and other [IISPs], and respond to complaints within fifteen days after receiving it.' (A 14)

Where are user rights? – Access, correction, blocking and deletion

Surprising omissions from the Regulation are the normal 'user rights' in relation to a person's own personal information: access, correction, and (less frequently) blocking of use, and deletion/de-identification. If users do not have the ability to obtain access to their own User's

Personal Information and to ensure it is correct, then one of the fundamental elements of a data privacy law is missing. No other Chinese law provides a general rights of access to, or correction of, personal information held by the private sector. The requirement on a data controller to accept complaints from users and respond to them within 15 days does not in itself seem to imply rights of access and correction.

In relation of information uploaded by users, IISPs are required 'to ensure users' ability to use, modify and delete the information updated by them' (A 13), so there is a deletion right in relation to this more limited class of information.

Data export limitations

There are no express limitations on the export of personal data outside China in these Regulations, and at present no general restrictions on the private sector to be found in other laws (though laws concerning state secrets or other specific matters could be quite restrictive). In 2011, the MIIT website published for comment draft non-mandatory guidelines developed by the Standardization Administration of China (SAC) which said that there should not be transfer of personal data out of China without the express consent of the 'governing administrative authority' (a technical committee under the SAC). One commentator noted that 'the position in the draft Guidelines is far more restrictive than the proposed Draft Privacy Law [of 2007], which would generally allow international transfer of information subject to informed consent, national security considerations and the adequacy of data privacy laws in the recipient's jurisdiction'.[6] These Guidelines have not yet been finalised, but it is reported that a new draft has been completed and is expected to soon be promulgated[7].

Enforcement provisions

The enforcement methods in the Regulation are diverse, but primarily at the initiative of the Telecommunications Authorities. They do not include civil damages provisions, but these may be provided by other aspects of Chinese law, read in conjunction with these Regulations.

Administrative orders, penalties, and adverse publicity

Breaches of any of the privacy-related provisions may result in a Telecommunications Authority ordering the IISP to take corrective actions, and give it a warning, and may impose a concurrent fine from RMB10,000 (US$1,250) to RMB30,000 (US$4,750), and it is required to make a public announcement if it does so (A16 and A 18). Breaches of Article 13 may also result in legal liability under other laws (A 16). A Telecommunications Authority may, before it makes a decision on a matter require an IISP to suspend an activity and the IISP must comply (A 15). If a Telecommunications Authority concludes in an investigation that a violation may have 'an extraordinarily material effect', the event must be reported to MIIT. IISPs are also required to report other IISPs to the relevant Telecommunications Authority if they become aware of activities which may cause 'a material impact on the interests of users' (A 15).

---

[6] Fernandez, G 'China Publishes Draft Privacy Guidelines', Hogan Lovells website, 14 April 2011 at <http://www.hldataprotection.com/2011/04/articles/international-eu-privacy/china-publishes-draft-privacy-guidelines/>

[7] Li, J 'China unveils personal data protection guidelines', FutureGov Asia website, 6 April 2012 at <http://www.futuregov.asia/articles/2012/apr/06/china-unveils-personal-data-protection-guidelines/#>, referring to 'Personal Data Protection Guidelines for Public and Commercial Service Information Systems'.

Civil damages

The Regulation does not include any specific provisions concerning the payment of civil damages because a breach of its Articles resulting in harm, so it is necessary to ask whether any other law may provide the basis for such a damages action. Although a claim for infringement of privacy could be considered under recent case law under the *General Principles of Civil Law*, it is more likely that liability could arise under the *Tort Liability Law* (effective 1 July 2010) which provides that infringements of civil rights and interests results in tort liability, and also lists the right to privacy (not further defined) as one of the civil rights concerned. Furthermore, Article 36 of the Tort Liability Law provides that 'an Internet user or Internet service provider who infringes on the civil right or interest of another person through the Internet shall assume the tort liability'. It is possible to pursue claims for emotional harm and mental distress, and there are provisions for joint and several liability of users and ISP, and take-down procedures that may need to be observed.[8] The applicability of the *Tort Liability Law* to breaches of this Regulation is speculative, but may be significant.

Conclusions: Approaching international standards?

Serious enforcement expected

Commentators on China's Internet industry expect that these Regulations will be actively enforced, in part as a result of a string of widely publicised unauthorized disclosures of user information by Internet companies in 2011, and that some industry sectors will have considerable compliance problems. McKenzie and Fang comment:

> 'Promulgation of the Internet Regulations comes at a time of greater activism on the part of the public security authorities and other government agencies in dealing with cases of data theft. The MIIT has a record of relatively aggressive exercise of its jurisdiction over the Internet. For all of these reasons, it is expected that the privacy provisions of the Internet Regulations will be actively enforced'.

China does not yet have a 'data privacy law'

China does not yet have a general data privacy law in the sense of one that applies to most aspects of the private sector and meets international standards for principles and enforcement[9], for two reasons. The scope of the law is limited to only some business and non-profit activities, but its broad coverage of Internet activities means that it does have one of the most extensive and important sectoral data privacy laws, given the size and importance of China's Internet sector. Secondly, it is missing essential user rights of access and correction of personal information.

Comparison with the 2005-07 draft data privacy law

From 2005-7 a group of experts led by Professor Zhou Hanhua, the director of the Institute of Law at the Chinese Academy of Social Sciences, were commissioned to draft a national data protection law ('draft law') to be considered by the Informatics Committee of the State

---

[8] Discussed in Ong, R 'Recognition of the right to privacy on the Internet in China' (2011) *International Data Privacy Law* Vol 1 No 3, 72 at 78

[9] See the criteria used in Greenleaf, G 'Global Data Privacy Laws: 89 Countries, and Accelerating', *Privacy Laws & Business International Report*, Issue 115, Special Supplement, February 2012; also available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000034>

Council[10], but it did not proceed. How does this Regulation compare? The draft law was stronger in many respects: it applied to the public sector and the whole of the private sector; it had explicit rights of subject access and correction; it had provisions allowing data exports to be prevented; and it provided a right to take court action for breaches. However, the limitations on collection appear stronger in the Regulation, and it also includes data breach notification requirements not found in 2007's draft.

Comparison with OECD/APEC and European standards

While the Chinese Regulation obviously falls short of all international standards because of its lack of access and correction rights, and its limited scope to Internet information providers, it meets the basic standards of the principles in the OECD Guidelines in many other respects. The other significant place at which it falls short is that the limitations on disclosure only apply to user-provided personal data, and not that which has been collected from third parties or generated from transaction. In a few respects (minimal collection; data breach notification), the Regulation includes more recent privacy principles. It is a very significant step for China, even if it would be a very limited one in other countries.

[10] See Greenleaf, G 'China's Proposed Personal Information Protection Act' *Privacy Laws & Business International Newsletter*, Issues 91 and 92, 2008, available at < http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2023065>