China's incremental data privacy law: MIIT 'User Data Protection' Regulations, 2013

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

(2013) 125 *Privacy Laws & Business International Report*, 18-19, September 2013

China's Ministry of Industry and Information Technology (MIIT) has issued the *Telecommunications and Internet Personal User Data Protection Regulations* ('User Data Protection Regulations') on 28 June 2013, to take effect on 1 September 2013.[1] The MIIT has previously issued Regulations in 2011 and Guidelines earlier in 2013, and is clearly taking the leading role among Ministries in the area of personal information protection.

These MIIT Regulations should not be considered in isolation, but rather as the latest component of an evolving and incremental body of law. They are best seen in terms of the cumulative effect of what they add to the previous (2011) MIIT Regulation, the 2012 National People's Congress Standing Committee decision on Internet information, and the 2013 MIIT Guidelines,[2] all dealing with Internet information service providers (IISPs). These Regulations cover both IISPs and telecommunications business operators (TBOs) (Article 2).

These Ministry regulations are also made under the *Telecommunications Regulations* 2000,[3] a higher level of legislation made by the State Council of the PRC. The *Telecommunications Regulations* create and regulate telecommunications business operators (TBOs), and must be complied with by 'anyone that engages in telecommunications activities or activities related to telecommunications' in the PRC (A 2). All TBOs must obtain permits to operate (A 7). In Part 5 'Security of Telecommunications', Article 66 protects communications against inspection of their content except where provided for by law[4] (where the exceptions allowed are substantial), and against disclosure by TBOs to third parties.[5] Other provisions prohibit 'using a telecommunications network to steal or damage a third party's information' (A 58(2)) and require a 'sound internal security system' (A 60).

---

[1] *Telecommunications and Internet Personal User Data Protection Regulations* (unofficial English translation) http://chinacopyrightandmedia.wordpress.com/2013/07/16/telecommunications-and-internet-user-individual-information-protection-regulations/.

[2] Greenleaf, G and Tian, G 'China expands data protection through new 2013 guidelines' (2013) *Privacy Laws & Business International Report*, Issue 122, 1, 4-6 (includes an English translation of the guidelines); Greenleaf, G 'China's NPC Standing Committee privacy Decision: A small step, not a great leap forward' *Privacy Laws & Business International Report*, Issue 121: 1, 4-6, February 2013.; Greenleaf, G 'China's Internet Data Privacy Regulations 2012: 80 Percent of a Great Leap Forward?' *Privacy Laws & Business International Report*, Issue 116: 1-5, April 2012.

[3] *Telecommunications Regulations* of People's Republic of China <http://tradeinservices.mofcom.gov.cn/en/b/2000-09-25/18619.shtml>

[4] Article 66: 'Telecommunications subscribers' freedom to legally use telecommunications and the confidentiality of their communications are protected by law. No organization or individual may, for any reason whatsoever, inspect the content of telecommunications, except that public security authorities, the State security authority and the People's Procuratorate may do so in accordance with the procedures stipulated by law in response to the requirements of State security or the investigation of criminal offences.'

[5] A 66: 'No telecommunications business operator or its employees may provide, without authorization, to a third party the content of information transmitted through the telecommunications network by telecommunications subscribers.'

New principles in these regulations

Many aspects of these 2013 User Data Protection Regulations are similar to the 2011 MIIT Regulations, including the requirements of minimum collection of information, notice, and data breach notification (although the details differ somewhat). Other aspects add a significant number of new or stronger forms of regulation, including the following:

- The definition of 'personal user data' may be broader than the previous conventional definitions based on capacity for identification, because it also includes 'other information, as well as the time, and place of the user using the service and other information, collected by [TBOs] and [IISPs] in the process of providing services' (A 4). This provision is ambiguous. Does it mean that 'call data' information is by itself regarded as 'personal user data', or only when it is collected in conjunction with data with the capacity to identify? If it is the former, China is taking a significant step beyond the data privacy laws of most countries.
- TBOs and IISPs must 'formulate personal user data collection and use rules, and publish these in their business or service premises, websites, etc' (A 8), which is much the same as saying they must publish a Privacy Policy.
- Although other laws have required minimal collection of personal data, none have previously required that IISPs and TBOs 'may not collect or use personal user data' 'without user permission' (A 9). This blunt requirement does not differentiate between data collected from the person concerned and that collected from third parties.
- Collection and use of personal data must cease when a user cancels an account (A 9), but there is no requirement here or elsewhere that the data be deleted.
- IISPs and TBOs are required to supervise and manage data protection when they utilise third party processing facilities, and 'may not entrust agents who do not conform to personal user data protection requirements' (A 11). This appears to impose a strict liability on data controllers for the actions of their processors, and no matter where they are located, but it would be necessary to see how this is administered in practice to be certain.
- There are more detailed security protection provisions than in other laws (A 13).

Some aspects of the Guidelines issued earlier in 2013 by MIIT are still not included in these or earlier Regulations, such as data export limitations.

New aspects of administration and enforcement

The financial sanctions for breach of the User Data Protection Regulations are low, only a maximum of 10,000 yuan. However, as with the privacy principles, there are new aspects of administration and enforcement not found in previous laws, such as the following:

- Notifications of data breaches have been required previously, but these regulations add specific requirement of immediate report to and cooperation with the 'relevant telecommunications management organ' wherever 'grave consequences' are possible, where 'especially grave, report of violations to MIIT (A 14).
- There is a requirement of annual 'self inspection' of security measures, and response to what is found (A 16).
- There is greater detail of how supervision and inspection by 'telecommunications management organs' may be carried out (A 17)
- Violations of the Regulations must logged by the telecommunications management organs in the 'social credit register' of an IISPs or TBO, and published (A 20), an unusually strong 'name and shame' sanction. Fines may be similarly published (A 23).
- There is explicit encouragement to telecommunications and internet 'sector associations' to introduce complementary self-regulatory measures (A 21). Similarly, they are encouraged to

'launch personal user data protection self-discipline work' (A 7), which probably means to educate their users how to protect their own personal data.

- Failure by telecommunications management organs to impartially administer the Regulations is to be punished, and is also a crime by individual public officers (A 24). Many consumers and privacy advocates would wish such sanctions applied to some Data Protection Authorities in western countries for failure to pursue powerful interests (A 24).

The 'toolkit' of measures to administer and enforce data privacy principles is therefore expanding considerably in China.

Conclusions

China's data protection law is still evolving, one relatively small step at a time. Although this and the earlier Regulations and Guidelines (and the NPC Standing Committee Decision) focus on the Internet and telecommunications sectors, they may be building up a template for how data privacy legislation could be extended to the whole of China's private sector.