China's New Cybersecurity Law – Also a Data Privacy Law?

GRAHAM GREENLEAF AND SCOTT LIVINGSTON

(2016) 144 Privacy Laws & Business International Report 1-7
[2017] *UNSWLRS* 19

UNSW Law
UNSW Sydney NSW 2052 Australia

China's new Cybersecurity Law – Also a Data Privacy Law?

Graham Greenleaf, Professor of Law & Information System, UNSW Australia

Scott Livingston, Senior Associate, SIPS Asia (Hong Kong)

(2016) 144 *Privacy Laws & Business Report* 1-7

On 7 November 2016, China's Standing Committee of the National People's Congress (SC-NPC) promulgated the *PRC Cybersecurity Law*, which will take effect on 1 June 2017(Art. 79). The Standing Committee is China's highest legislative body after the Congress itself.

As its name suggests, the law is mainly devoted to provisions concerning the security of information networks and, in particular, to mandating security procedures and requirements for 'critical information infrastructure' and 'critical information infrastructure operators'. Except where these topics touch on data privacy issues, they are not the subject of this article.

The *Cybersecurity Law's* provisions relating to data privacy articulate what are China's most comprehensive and broadly applicable set of data privacy principles to date. These provisions reiterate many of the basic principles and requirements found in other laws and regulations – including, most notably, the SC-NPC's 2012-promulgated *Decision of the SC-NPC on Strengthening Network Protection*.[1] But the Law also includes new or more explicit requirements with respect to data correction rights, deletion, re-use and disclosure, breach notification to users and data localization. Still missing, however, are several common elements of other jurisdictions' data privacy laws, such as explicit user access rights, requirements on data quality and special provisions for sensitive data. The Law also does not establish a national data protection authority. While China has long lacked a broadly applicable national data privacy law, the scope and strengthened principles of this new legislation means that it can probably now be considered to be "China's Data Privacy Law," with which other lower-level laws and regulations must be consistent.

This article analyses the privacy-related aspects of the *Cybersecurity Law*, and in particular asks what (if anything) it adds to China's previous set of data privacy laws. The scope of the Law is first considered, followed by a discussion of its principles and substantive provisions (which are mainly found in Chapter IV: Network Information Security, Articles 40-50). We conclude with a brief discussion about the Law's enforcement and personal surveillance aspects (mainly in Chapter VI: Legal Responsibility). Comparisons are made with China's existing data privacy laws.

Scope – 'Network operators' and 'personal information'

Businesses and agencies covered

While the exact scope of the Law remains unclear, its coverage does appear broader than previous laws targeting data privacy.

The *Cybersecurity Law* states that it applies to "construction, operation, maintenance and usage of networks, as well as the supervision and management of networks within the mainland territory of the People's Republic of China' (Art. 2). The Law's substantive requirements apply mainly to 'network operators', including all of the provisions relating to personal privacy.

'Network operators' are defined in the Law as 'network owners, managers and network service providers' (网络的所有者、管理者和网络服务提供者)(Art. 76(3)). This definition

[1] These laws include: MIIT Regulations on IISPs (2011); SC-NPC 'decision' on 'electronic information' (2012); SC-NPC Amendments to the Consumer Law (2013); MIIT Internet/telecommunications Regulation (2013); and MIIT information systems Guidelines (2013). For detailed discussion see G Greenleaf *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (OUP, 2014), pp. 208-220.

appears to be somewhat broader than that found in the 2012 SC-NPC Decision, which applied to "network service providers (网络服务提供者) and other enterprises and public institutions." 其他企业事业单位(Art. 2). In the new law, this "enterprise" or "public institutions" nexus is absent.

'Networks' are defined as referring 'to systems comprised of computers or other information terminals and related equipment that follow certain rules and procedures for information gathering, storage, transmission, exchange and processing' (Art. 76(1)). On its face, this definition appears broad enough to encompass systems as small as two computers using a shared printer or a shared router, and thus could apply to all but the very smallest and most 'unconnected' business in China. But some commentators have questioned whether the Chinese government could possibly intend such broad coverage and it seems unlikely that the law is meant to apply at such a granular level.[2]

Whether or not further steps are taken to narrow the Law's scope, it is likely to retain by far the broadest scope of any current Chinese privacy law.

One significant question that remains is whether the *Cybersecurity Law* is meant to apply to the public sector (beyond those public utilities covered by the 'critical information infrastructure' definition found below). Given how the Law defines "network operators," there is no indication that the Law that would exclude public sector bodies from its scope. If true, this would be an extraordinary new development: a single privacy law covering the whole of the private and public sectors. But such application remains to be seen

There is no explicit distinction in the Law between data controllers and data processors, nor have the previous 2012 SC-NPC Decision or sectoral regulations made such a distinction. However, such a concept is found in the (voluntary) 2013 MIIT Guidelines, so it is possible such a provision may be introduced in future legislation.

Personal data covered

On the other key question of scope, 'personal information' is defined to refer to 'all kinds of information, recorded electronically or through other means, that taken alone or together with other information, is sufficient to identify a natural person's identity, including, but not limited to, natural persons' full names, birth dates, identification numbers, personal biometric information, addresses, telephone numbers, and so forth' (Art. 76(5)). Several other Chinese laws and regulations contain similar definitions, but this marks the first time China has included 'personal biometric information' in a definition for 'personal information.'

Otherwise this definition is similar to that found in the data privacy laws of most countries: it is based on the potential for information to identify a person, i.e., 'identifiability'. It only applies to recorded information, not information which is known but not recorded.

As with China's other data privacy laws and regulation, the *Cybersecurity Law* provides no distinction or category for 'sensitive personal information.'[3] However, there is a separate category of 'critical information infrastructure' (CII, discussed later), and personal information held within such CII is subject to separate rules for data localisation and data exports.

---

[2] For example, Carolyn Bigg 'CHINA: significant changes to data and cybersecurity practices under PRC Cybersecurity Law', DLA Piper website <http://blogs.dlapiper.com/privacymatters/china-significant-changes-to-data-and-cybersecurity-practices-under-prc-cybersecurity-law/>.

[3] The only time such a concept has appeared in China is in the 2013 MIIT guidelines, which, as a voluntary national standard, lack the force of law.

Jurisdictional scope

The law does not have extra-territorial effect, and applies only to matters occurring 'within the mainland territory of the People's Republic of China' (Art. 2). There is no exclusion for information about foreigners, once a network within China is involved. There is no exclusion for information controlled by overseas entities but processed in China (eg on Chinese cloud servers).

Privacy principles

In this section we will examine the privacy principles found in the *Cybersecurity Law* and compare them with general global practice, and previous Chinese laws.[4]

General statement of privacy principles

The Cybersecurity Law contains a general statement of obligations for network operators, in which many of the Law's key provisions are found:

> 'Network operators collecting and using personal information shall abide by the principles of legality, propriety and necessity; make public rules for collection and use, explicitly stating the purposes, means, and scope for collecting or using information, and obtaining the consent of the person whose data is gathered' (Art. 41).

Network Operators also 'must not gather personal information unrelated to the services they provide; must not violate the provisions of laws, administrative regulations or agreements between the parties to gather or use personal information; and shall follow the provisions of laws, administrative regulations and agreements with users to process personal information they have stored' (Art. 41, 2nd paragraph). Similar requirements have been found in other Chinese privacy laws and regulations, including, again, the 2012 SC-NPC Decision.

Collection limits, consent and notifications

Article 41 of the Law prohibits network operators from "gathering personal information unrelated to the services they provide.' This reads like a moderate OECD-like collection standard ('related to'), not the stricter minimum collection standard ('necessary for') found in the previous MIIT Regulations and Guidelines. Businesses that come within the scope of those MIIT laws may need to seek clarification as to practical effect of this distinction. The new Law also refers to the principle of 'necessity' in Article 41, but that is unlikely to impose a higher standard.

Network operators must also publish a privacy statement ('make public rules for collection and use, explicitly stating the purposes, means, and scope for collecting or using information': Art. 41), and obtain 'the consent of the person whose data is gathered' (Art. 41). These requirements were previously found in the 2012 NC-SPC decision and other regulations (as applied to their respective covered entities), but the notification obligations here are much less extensive than in the 2013 MIIT Regulations, which contained additional requirements regarding providing users with "channels to consult and correct information" and the consequences for "refusing to provide information."

Although not an explicit provision relating to user information, Article 49 requires "network operators" to "publicly disclose information such as methods for making complaints or reports" which provides some conduit for network users to consult and correct information relating to their personal data.

---

[4] For information on previous laws, see Greenleaf *Asian Data Privacy Laws*, pp. 208-220.

Data quality

The Law does not contain any specific references to data quality principles (i.e those international principles which refer specifically to accuracy, completeness or timeliness of personal information collected), but Art. 41 does refer to 'the principles of legality [and] propriety'. Previous SC-NPC privacy laws did exactly the same.

Network operators must not 'tamper with, or destroy personal information they gather' (Art. 42). The 2013 MIIT Guidelines did refer to the more specific quality requirements, but they were only Guidelines. To some extent, the user rights of correction and deletion in this Law are ex-post-facto substitutes for data quality requirements.

Use and disclosure limitations

Article 41 further prohibits network operators from violating 'agreements between the parties to … use personal information,' thereby obligating such parties to only use personal data for the purposes agreed upon with the users. They 'must not disclose' the personal information they gather, and, 'absent the consent of the person whose information was collected, [they] must not provide personal information to others' (Art. 42). Otherwise, there are no explicit list of exceptions to these use and disclosure limitations based on the purpose of collection ('finality'). This Law expresses these 'finality' obligations clearly, whereas the two previous SC-NPC did not clearly adopt the 'finality' principle. So this aspect is an important strengthening of China's previous laws.

An exception exists in the Law's use and disclosure restrictions for personal information that 'has been processed so that the specific individual is unidentifiable and cannot be recovered' (Art. 42). But the Law is not clear whether such de-identified data is no longer 'personal information', or whether (for example) security obligations persist.

There are further obligations of confidentiality, expressed in numerous ways, on those carrying out network security tasks (Art. 30, Art. 45), breach of which could result in tortious, administrative, or criminal liabilities.

Security and data breach notifications

The Law states the security obligations owed by network operators to individuals only in very general terms such as to 'establish and complete user information protection systems' (Art. 40) and to 'adopt technological measures and other necessary measures to ensure the security of personal information they gather, and prevent personal information from leaking, being destroyed or lost' (Art. 42). This is much the same as previous SC-NPC laws, and does not make clear what standard of care network operators must meet in order to avoid civil liability or other sanctions (eg 'take reasonable steps').

The Cybersecurity Law reiterates previous data breach notification requirements but adds to them a new requirement requiring network operators to notify the users affected: 'When the leak, destruction or loss of personal information occur, or might occur, remedial measures shall be immediately taken, and provisions followed to promptly inform users and to make report to the competent departments in accordance with regulations' (Art. 42). Under previous laws, affected entities were only required to notify the authorities.

User rights: Correction, deletion, whither access?

The Law contains the most explicit provisions to date concerning correction of errors in stored personal data, and the deletion of data unlawfully collected:

> 'Where individuals discover that network operators have violated the provisions of laws, administrative regulations or agreements between the parties to gather or use

> their personal information, they have the right to request network operators delete their personal information; where discovering that personal information gathered or stored by network operators has errors, they have the right to request the network operators make corrections. Network operators shall employ measures for deletions and corrections' (Art. 43).

Some commentators have described the deletion requirement as new,[5] but it was already included in Article 8 of the 2012 SC-NPC Decision (the first of the series of laws), in much the same terms, even though a right of correction was omitted. The correction right was not previously found in China's laws, except in the 2013 MIIT Guidelines, Art. 5.3.6, so its explicit inclusion here is significant. Neither this Law, nor previous ones, have required personal data to be automatically deleted once the purpose of collection has been completed, except for those Guidelines.

Commentators have also stated that the Law addresses 'privacy aspects such as access, data retention, [and] breach notification'.[6] However, access to a data subject's own personal information is nowhere specifically mentioned in this Law, just as it is absent from specific mention in all previous Chinese private sector laws, with the exception once again of the 2013 MIIT Guidelines Art. 5.3.7, which referred to individuals requiring inspection of their personal information.

Nevertheless, as mentioned above, Art. 49 of the new Law requires "network operators" to "publicly disclose information such as methods for making complaints or reports." This implies that some form of access rights are provided, even if such consultation and correction channels are not explicitly linked to personal information. Furthermore, given that it will not be possible for individuals to effectively utilise the rights of correction and deletion that the new Law clearly gives them, this adds to the likelihood that a right of access will now be regarded as implied. It must be, otherwise China is still missing one key element of a data privacy law. Surprisingly, the right of access to a person's own file is already provided for in the public sector.[7]

Data exports and data localisation

A significant part of the Cybersecurity Law deals with 'critical information infrastructure' (CII), which is defined to include infrastructure involving 'public communication and information services, power, traffic, water, finance, public service, [and] e-governance' as well as 'other critical information infrastructure that if it is destroyed, loses its ability to function or encounters data leaks, might seriously endanger national security, national welfare and the people's livelihood, or the public interest' (Art. 31).[8] Responsibility for drafting a more detailed definition of CII providers is then tasked to the State Council who is instructed to 'formulate the specific scope and security protection measures for critical information infrastructure' (Art. 31). We expect these guidelines to be issued sometime in 2017.

---

[5] Gabriela Kennedy and Xiaoyan Zhang 'China Passes Cybersecurity Law' 15 November 2016 <http://www.mondaq.com/china/x/544584/Security/China+Passes+Cybersecurity+Law>.

[6] Kennedy and Zhang, previous citation.

[7] Regulations on Open Government Information (China), 2007, Arts. 13-14.

[8] The definition of CII has changed with each of the law's three drafts. In the first draft, CII was defined as a similar (but not identical) group of public utilities along with networks with a 'a large number of users'. In the second draft, the responsibility for defining CII was left to the State Council.

The *Cybersecurity Law*'s provisions concerning CII operators impose a higher standard of care for personal data that includes data localization and data export requirements. Article 37 of the Law states that all "personal information and important data collected and produced by CII operators during their activities within the People's Republic of China" shall be stored in mainland China. (Art. 37). "Important data" is undefined in the law and its scope is currently unclear. In the second draft, this article referred to 'important business data', rather than "important data", so it appears that these data localization requirement has been broadened somewhat. It is possible that this term might include data relevant to individuals that falls outside of 'personal information' such as anonymised data or metadata (for instance, aggregated financial information or metadata related to mapping). Of course, much data which is not related to individuals is likely to be 'important data'. It is also possible that some personal information will be held be bodies which do not qualify as CII. It is likely that this subject will be further defined in the forthcoming State Council promulgation concerning CII.

Such 'CII data', as we will call it, can only be exported overseas (with a copy remaining in China) 'where due to business requirements it is truly necessary to provide it outside the mainland' (Art. 37). If such transfer is "truly necessary," then the CII operators must go through a 'security assessment' conducted according to measures jointly formulated by the national cyberspace administration and the relevant departments of the State Council (unless other laws or administrative regulations provide otherwise). The result is that all export of CII data is prima facie prohibited, unless a security assessment provides otherwise and confirms that the transfer is 'truly necessary'. Given the vague definition of 'CII', the scope of this is largely unknown.

Assuming that some personal data will not be CII data, can it be exported? The Cybersecurity Law says that operators of networks outside the CII definition are 'encouraged' by the State to 'voluntarily participate' in the CII protection system (Art. 31), so it is possible that pressure will be brought to bear for the security assessment system to be used more broadly. Otherwise, the Cybersecurity Law does not provide any general rules about data exports, nor do any of the other existing privacy-related laws. The only exception is the 2013 MIIT Guidelines, Art. 5.4.5, which prohibits data exports in the absence of (i) data subject consent, (ii) explicit legal permission, or (ii) consent of the competent authorities. However, the 2013 MIIT Guidelines is a voluntary guideline, and does have the force of law. Still, while only a Guideline, perhaps this is an indication of what is expected with personal information which is not CII data.

Administration and enforcement

In this section, we will outline the administration and enforcement of the Cybersecurity Law and compare them with existing enforcement provisions, noting where measure outside the Law will be important.

MIIT enforcement – No DPA, but perhaps a PEA

Article 8 of the *Cybersecurity Law* confirms the leading role of the Cyberspace Administration of China (CAC) as the principal agency for overall coordination and planning of cybersecurity efforts. Implementation of the Law (and its related CAC directives) is left to the Public Security Bureau (PSB), and the Ministry of Industry and Information Technology (MIIT), the nation's chief Internet and telecommunications regulator. Under this system, MIIT offices at all levels would be the main body responsible for dealing with privacy-related complaints. This is currently the situation under existing privacy laws in China, although the State Administration of Industry and Commerce plays some role with respect to protection of consumer rights under the Consumer Protection Law.

The Cybersecurity Law does not establish a data protection authority (DPA) in the sense used in Europe and in many other countries. However, it does appear to embed the MIIT as the principal enforcement authority for issues relating to personal information. More than previously, it is now China's 'privacy enforcement agency' (PEA), and could play that role (if China was so minded) in international bodies such as GPEN (Global Privacy Enforcement Network), which are concerned primarily with complaint resolution, not policy issues.

Complaints

Article 14 provides a channel by which "individuals and organizations have the right to report conduct endangering network security" to the aforementioned administrative departments. The definition of 'network security' includes 'ensuring the capacity for network data to be complete, confidential and usable' as well as protecting them from attack (Art. 76(2)). Assuming therefore that 'network security' includes protection of personal information, then it would appear that all individuals and organizations 'have the right' to report conduct endangering personal information to MIIT and PSB, and they obliged to promptly process such reports (Art. 14).

The *Cybersecurity Law* requires network operators themselves to 'establish network information security complaint and reporting systems, publicly disclose information such as the methods for making complaints or reports, and promptly accept and handle complaints and reports' and to cooperate with the relevant departments (Art. 49). Similar provisions have been found in other laws and regulations. There are no provisions requiring individuals to first complain to a network operator before escalating a complaint to the relevant department.

Administrative fines and other penalties

Article 64 provides for administrative fines to be assessed for any breaches of the Law's personal information provisions (ie Arts. 41-43).

These remedial measures allow for administrative departments to issue orders for corrective action along with, either independently or concurrently, warnings, confiscation of unlawful gains, or fines per the below scale:

- Fines between 1 to 10 times any unlawful gains; or, if no unlawful gains,
    - Fines up to RMB 1 million (US $145,000) for organisations; plus
    - Fines between RMB 10,000 to RMB 100,000 (US $1,450 – 14,500) for persons directly in charge and other directly responsible personnel (or five times these amounts where 'the circumstances are serious').

If the violation is "serious," then a fine of between RMB 50,000 and 500,000 may be imposed along with an order to temporarily suspend operations, close down the website, or revoke the entities' operations permit or business license. These are the standard range of sanctions found in most other Chinese privacy laws. Violations of the Law are supposed to be recorded in the social credit register for the relevant organisation or person, and made public (Art. 71), as also set forth in the 2013 MIIT Regulations.

The fines above are comparable to the levels of administrative penalties in most countries, but do not include fines based on a percentage of annual turnover, as in the EU or Korea. Most have existed in the previous laws, but the high levels of fines for individual business executives are new for China, though not for other countries (eg Singapore, Korea).

Private enforcement and damages

Article 74 provides for the right to civil actions where violations of the Law harms an individual's rights. In the privacy context, this would appear to reference protections found in the *PRC Tort Liability* Law's Article 2 protection of an individual's 'civil rights and interests,' which has long been held to protect, inter alia, an individual's civil right to privacy, reputation and/or portraiture. It may also invoke Article 36 of the *PRC Tort Liability Law*, which includes special protections related to online infringement of civil rights appearing on information networks.[9] China's Supreme People's Court (SPC) has recently issued guidance that clarifies procedural questions relating to application of Article 36, and that adds several new substantive provisions. [10]

Criminal law enforcement

Where breaches of the Law constitute a crime, they are to be prosecuted under normal criminal law procedures. (Art. 74). The *Cybersecurity Law* reiterates the extensively-used Art. 253(a) of the Criminal Law[11] which was expanded in 2015 to prohibit any individual or organization from illegally selling or providing the personal information of others to third parties where the conditions are "serious" (undefined)[12] Violation of Art. 253(a) results in a fine and/or fixed-term imprisonment for up to three years, or, if the conditions are "extremely serious," a fine and three to seven years imprisonment.

Under the amended Criminal Law's new Article 286(a), "network service providers" that fail to fufil "information network security administration duties prescribed by laws and/or administrative regulations," and do not take remedial action as required by authorities may face criminal liability if one of four conditions are present:

(1) Illegal information has been widely disseminated
(2) User information is divulged and the circumstances are serious
(3) Evidence in a criminal case is lost and the condtions are serious;
(4) Other "Serious" circumstances are involved.

In such circumstances, violators may face either a fine or a fine with fixed-term imprisonment not to exceed three years, criminal detention, or public surveillance.

Surveillance provisions

The Cybersecurity Law contains various provisions which are intended to increase the Chinese state's capacity for surveillance of individuals, but often in ways found in other countries. This article does not focus on that aspect, but provisions such as those following should be noted:

- Network operators must 'require users to provide real identity information' when contracting to obtain most types of telecommunications or online services (Art. 24). Such 'real name' provisions have been required in China since at least the 2012 SC-NPC

[9] S Livingston and G Greenleaf 'Tort Liability for Online Privacy Violations in China: The 2014 SPC Regulation' (2015) 136 *Privacy Laws & Business International Report,* 24-27.

[10] Livingston and Greenleaf, previous citation.

[11] S Livingston and G Greenleaf 'China Whys and Wherefores – Illegal Provision and Obtaining of Personal Information Under Chinese Law' (2014) 131 *Privacy Laws & Business International Report* 1-5.

[12] Ashwin Kaja and Eric Carlson 'China Amends Criminal Law Related to Data Privacy and Cybersecurity' 1 September 2015 <https://www.insideprivacy.com/uncategorized/china-amends-criminal-law-related-to-data-privacy-and-cybersecurity/>.

Decision, and are common in other countries. They do not prevent the use of online pseudonyms.

- Network logs must be kept for at least six months, in accordance with other data retention provisions (Art. 21(3)). Again, such provisions are not unusual elsewhere (eg Australia).
- 'Network operators shall provide technical support and assistance to public security organs' and state security organs; lawful activities preserving national security and investigating crimes' (Art. 28). Will this go so far as network operators being required to provide software 'backdoors' and other means of surveillance?
- 'The State supports cooperation between network operators in areas such as gathering, analyzing, reporting and responding to network security information, increasing the security safeguard capacity of network operators' (Art. 29). However, information gathered 'can only be used as necessary for the protection of network security, and must not be used in other ways' (Art. 30).

Outside the areas specifically to do with personal information and privacy, the Cybersecurity Law has many other provisions of considerable concern to overseas businesses.

Conclusions: Five year evolution towards a data privacy law

The personal information aspects of the Cybersecurity Law are best seen as the culmination of an evolving set of data privacy laws and principles enacted over the five years since December 2011.

While calls remain for a specific law relating to data privacy, the privacy principles set forth in the *Cybersecurity Law* contain the most comprehensive treatment to date and include several modest advances compared with previous legislation. These include more explicit 'finality' limits on use and disclosure; deletion and correction provisions previously found in only some laws; and the extension of data breach notification to users. The enforcement penalties are slightly stronger, and several have not been previously found in such a high level law. The CII data localisation and data export prohibition provisions would likely be regarded as data privacy protections by the drafters, but have already come under much criticism from foreign observers who view them as unnecessarily restrictive of global data flows and therefore harmful to China's professed drive to promote innovation.[13] The one puzzling element is the continuing omission of an explicit right of access to a person's own information, though this may well be implied.

But what may be most significant about the Law is its scope as it would appear to extend these data privacy provisions to most, perhaps almost all, of the private sector in China. It is also possible that the Law extends them to the public sector, though this remains unlikely. This coverage, and the strengthening of principles, means that it is now sensible to say that China has a data privacy law containing the normal elements of such laws.

[13] Josh Chin and Eva Dou 'China's New Cybersecurity Law Rattles Foreign Tech Firms ' *Wall St Journal*, 7 November 2016 <http://www.wsj.com/articles/china-approves-cybersecurity-law-1478491064>