Bloomberg BNA

Privacy and Security Law Report®

China Update: Privacy Law and Network Security Developments

By Paul D. McKenzie and Jing Bu

The past 16 months have been eventful in China in connection with privacy law and network security developments.

Key privacy law developments included:

- the coming into effect of new privacy provisions of the Consumer Protection Law;
- a high-profile prosecution under the privacy law provisions of the Criminal Law;
- proposed changes to the Criminal Law in order to broaden the scope of criminal liability for the misuse of personal data, including through the addition of an offense that would cover corporate as well as individual offenders; and
- a number of sector-specific developments.

Chinese privacy developments continue to be relatively piecemeal, with standards and definitions as they develop often being different in privacy provisions governing different sectors and activities.

This same period saw significant developments on the data security front, including the launch of a new system for certifying the network security of information technology (IT) products and services used by banks and other financial institutions, as well as efforts towards a broader network security review regime that will likely affect international IT product suppliers and IT service providers. It also witnessed issuance of a draft Anti-Terrorism Law that contemplates broad access to voice and data traffic by People's Republic of China (PRC) authorities.

Paul D. McKenzie is a member of Morrison & Foerster LLP's Global Privacy and Data Security practice and managing partner of the firm's Beijing office.

Jing Bu is formerly of Morrison & Foerster's Beijing office.

The authors would like to thank colleagues Gordon Milner and Cynthia Rich for valuable comments on an earlier draft.

CONSUMER PROTECTION LAW

Data Privacy Provisions of Consumer Protection Law Come Into Force

The amended Law on the Protection of the Rights and Interests of Consumers[1] (Consumer Protection Law), which was promulgated Oct. 25, 2013, by the Standing Committee of the National People's Congress (NPC), came into effect Mar. 15, 2014. The amended Consumer Protection Law includes a number of privacy-related provisions.

The Consumer Protection Law recognizes that consumers have a right to dignity and the right to have their personal information protected when purchasing or using a good or receiving a service.

The Consumer Protection Law also provides as follows:

- The collection and use of consumers' personal information should be on the basis of informed consent, and consumers should be notified about the purpose, method and scope of the data collection.
- Business operators should adhere to the principles of legality, legitimacy and necessity when collecting or using consumers' personal information.
- Business operators should publish policies governing their collection and use of the personal information.
- Business operators and their staffs should keep consumers' personal information in strict confidence and may not divulge, sell or provide such information to third parties without consent.
- Business operators should adopt technological and other measures as necessary to secure the

[1] The Consumer Protection Law is available, in Chinese, at http://www.npc.gov.cn/npc/xinwen/2013-10/26/content_1811773.htm (12 PVLR 1879, 11/4/13).

 ISSN 1538-3423

safety of the information and prevent it from being divulged or lost. In the event that personal information has been or could be divulged or lost, the business operator should immediately take remedial actions.

- Without a consumer's consent or request or if a consumer has expressly refused, business operators may not engage in direct marketing by sending commercial information to the consumer.

The Consumer Protection Law provides consumers with various civil remedies. A business operator who infringes a consumer's rights to dignity or privacy must cease such infringement, rehabilitate the user's reputation, take actions to mitigate adverse consequences, apologize and indemnify the user for losses.

The Consumer Protection Law also contemplates a number of administrative penalties. It states that industrial and commercial authorities and other relevant administrative authorities may issue rectification orders and, based on the circumstances, impose penalties that include a warning, confiscation of unlawful income and fines of (i) between one and 10 times the unlawful income or (ii) where there is no unlawful income, up to 500,000 yuan (about $80,645). Where laws and regulations are seriously violated, the business operator can be ordered to cease business until the problem has been rectified or have its business license revoked.

The Consumer Protection Law itself offers no definition of ''personal information.'' However, after the amendments to the Consumer Protection Law came into force, Jan. 5, 2015, the State Administration for Industry and Commerce (SAIC) issued Measures for Punishment of Infringements of Consumer Rights and Interests[2], which provide a definition. ''Consumer personal information'' is defined to mean information such as ''name, gender, occupation, birthday, identification number, domicile, contact information, income, financial condition, health condition and consumption history'' of a consumer ''that individually or in conjunction with other pieces of information can identify the consumer.'' These measures came into effect Mar. 15, 2015.

CRIMINAL LAW

ChinaWhys Case

The year 2014 witnessed the conclusion of the most high-profile prosecution[3] to date under the privacy-related provisions of the Criminal Law.

As amended in 2009, Article 253 of the Criminal Law imposes criminal liability on employees of government institutions and companies in the financial, telecommunications (telecom), transportation, educational and medical sectors who sell or otherwise unlawfully provide to third parties the personal data of any citizen that have been obtained in the course of employment and also on any person who has obtained such information by means of theft or other unlawful means, in either case where the associated circumstances are ''serious.''

In August, Peter Humphrey (a British national) and Yu Yingzeng (an American citizen) were convicted for their purchase of personal information about Chinese citizens in the course of operating their ChinaWhys investigations business. The case received prominence (and some sources believe the prosecution was pursued in the first instance) due to rumored connections between ChinaWhys and GlaxoSmithKline Plc. At the time of Humphrey's and Yu's arrests, GlaxoSmithKline was itself being investigated by Chinese authorities for corruption. Some media reports suggest GlaxoSmithKline was a ChinaWhys client that had asked ChinaWhys to conduct investigative work associated with the corruption allegations.

Factors considered by the court in determining that the circumstances were ''serious'' included the frequency of the breaches, the volume of personal information involved and the amount of associated illegal profits. Penalties imposed on Humphrey included a two-and-a-half-year prison sentence, a 200,000 yuan ($32,279) fine and an order that he be deported from China upon completion of his prison term. Yu was penalized with a two-year prison term and a 150,000 yuan ($24,209) fine.

Draft Amendment to Criminal Law

On Nov. 3, 2014, the NPC circulated for public comment Amendment 9 to the Criminal Law of the People's Republic of China (Draft),[4] which contemplates, among a variety of other proposed changes to the law, a significant broadening of the scope of criminal liability under Article 253 of the Criminal Law for the misuse of personal information. Specifically, it calls for:

- a broadening of the scope of the current data privacy offense under Article 253. The NPC is proposing that criminal liability would attach to an employee of any organization selling or illegally providing personal information obtained in the course of employment and not just government employees and employees of companies in specified sectors; and

- an additional, lesser offense under Article 253 of ''selling or illegally providing a citizen's personal information to third parties without the consent of such citizen,'' which would be subject to a prison term of up to two years (as opposed to three years for the existing offense). A company may also be subject to a fine for committing this offense and responsible individuals within the company may also be subject to criminal liability.

Promulgation of this amendment would represent a significant broadening of potential criminal liability associated with personal data breaches. The necessary element under Article 253 that the circumstances be ''serious'' in theory protects individuals and companies from prosecution for trivial breaches. However, the Criminal Law does not stipulate what circumstances count as serious, leaving courts with significant discretion to apply the test to specific cases.

[2] These measures are available, in Chinese, at http://www.saic.gov.cn/zwgk/zyfb/zjl/xfzbhj/201501/t20150114_151320.html (14 PVLR 485, 3/16/15).

[3] No official case report has been issued. A news report published by Xinhua, China's state-owned media outlet, can be found, in Chinese, at http://news.xinhuanet.com/2014-08/09/c_1112002618.htm.

[4] These draft amendments are available, in Chinese, at http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2014-11/03/content_1885029.htm.

  PVLR ISSN 1538-3423

SECTOR-SPECIFIC PRIVACY DEVELOPMENTS

Telecom/Internet

Online privacy continued to be one of the main focuses of regulations in 2014, following issuance in 2013 by the Ministry of Industry and Information Technology (MIIT) of standalone provisions governing the protection of personal information online.

Online Tort Provisions

On Aug. 21, 2014, the Supreme People's Court issued the Provisions on Several Issues Concerning the Application of Law to Adjudicate Civil Disputes Involving Infringement of Personal Rights Via Information Networks (the Supreme Court Provisions),[5] which came into effect Oct. 10, 2014.

The Supreme Court Provisions direct courts to support tort claims associated with disclosure by network users and network service providers of private information and other personal information, such as genetic information, medical records, health examination materials, criminal records, home addresses and information regarding private activities. At the same time, the Supreme Court Provisions stipulate a number of circumstances where a disclosure of information should not serve as the basis of a tort claim, including:

- disclosure with the written consent of the relevant individual and within the agreed scope;
- disclosure for the public interest to the extent necessary; and
- disclosure by an educational or scientific entity for public interest in connection with academic research or statistical analysis, provided that the relevant individuals have provided written consent and the method of disclosure is not sufficient to identify any individual.

Additional ''safe harbors'' contemplated by the Supreme Court Provisions include:

- disclosure where the relevant personal information has already been publicly disclosed by the relevant individual himself or herself online, or has already become public via other lawful means; or
- disclosure of personal information obtained through lawful means.

The Supreme Court Provisions limit the scope of these last two safe harbors by stipulating that network users and network service providers may still be liable if the method of disclosure violates the public interest or social morals or if the disclosure harms a material interest of the individual whose personal information is publicly disclosed.

The language of the Supreme Court Provisions summarized above leaves some uncertainty as to whether tort liability will arise in particular cases involving online data, and it will be interesting to see how judicial practice applying the Supreme Court Provisions develops.

[5] The Supreme Court Provisions are available, in Chinese, at http://www.chinacourt.org/law/detail/2014/08/id/147944.shtml.

MIIT Standards

After having circulated drafts for public comment[6] Nov. 13, 2014, MIIT formally issued Dec. 24, 2014, two related standards governing the protection of personal information by telecom service providers and Internet information service providers:

- Telecom and Internet service—User personal information protection—Definition and category (Classification); and
- Telecom and Internet service—User personal information protection—Classification guideline (Guideline).

The Classification categorizes personal information into three categories and further into an aggregate of 14 subcategories. The Guideline in turn provides for different levels of protection for the different categories and subcategories of personal information: five different levels, from level 1 to level 5 in ascending order of rigor.

Level 5 protection applies to information such as proof of identification (e.g., photocopies of identification cards), biological identification (e.g., iris scans) and identity and authentication information in relation to transaction services (e.g., account names/numbers and passwords), and it requires

> that strict technology and management measures be implemented; that users' information and choice rights be protected; that the confidentiality and completeness of personal information be preserved; that control and security of access to personal information be ensured; and that strict management protocols and real-time monitoring mechanisms be established in regard to the security of users' personal information.

Level 1 protection applies to information such as information about the service relationship with users—for example, data on when a user registered for service—and requires adoption of measures to control access to the personal information.

The Guideline and Classification list additional standards to be issued governing data privacy:

- Telecom and Internet service—Technical requirements for user personal information protection—Mobile app stores;
- Telecom and Internet service—Technical requirements for user personal information protection—Instant communications services; and
- Telecom and Internet service—Technical requirements for user personal information protection—E-commerce.

MIIT work plans in regard to standards-setting target the end of 2015 for completion of these three standards.

China Law Association/Peking University Standards

Nongovernmental organizations have also been participating in standards-setting efforts.

[6] The MIIT notice circulating the drafts is available, in Chinese, at http://www.miit.gov.cn/n11293472/n11293832/n12845605/n13916913/16249933.html. The texts of the draft Classification and Guideline are no longer available via this link. Copies of the final, Chinese-language Classification and Guideline are available for purchase from Posts & Telecommunications Press.

The China Law Association on Science and Technology and the Internet Law Center of Peking University issued Standards for the Assessment of Internet Enterprises' Protection of Personal Information[7] Mar. 15, 2014.

These standards, as compared with other existing rules, propose certain additional measures to be adopted by Internet service providers, such as encrypting users' personal information, giving users the right to access, and to request correction of, the personal information in the possession of Internet service providers and, where geolocation information is collected, notifying users of the same and providing them with the means to disable the collection.

Having been issued by two research organizations, these standards are not legally binding. However, they do contemplate Internet information service providers be granted ratings based on their practices in handling personal data and may help inform best practices with respect to the protection of personal information in China's quickly evolving regulatory environment.

Health Care

The National Health and Family Planning Commission issued the Administrative Measures on Management of Population Health Information (Trial)[8] May 5, 2014.

They include one of the first examples of an outright prohibition on the export of personal data, stating that medical, health and family planning organizations are prohibited from storing medical information on servers located outside of PRC and from using an escrow server or renting a server located outside of PRC.

Postal/Express Delivery Services

The State Post Bureau issued the Administrative Measures for Security of Personal Information of Postal Service Users[9] (Postal Measures) on Mar. 19, 2014.

The Postal Measures, which govern not only China Post but also express delivery companies, define ''personal information'' of postal service users as personal information disclosed by users during the process of using postal services, including senders'/recipients' names, addresses, identity numbers, telephone numbers, entity names, details of waybills, timing and information regarding items to be delivered. Postal service enterprises, express delivery enterprises and their staffs may not disclose user information to any other entity or individual unless expressly authorized by law or consented to in writing by users.

The Postal Measures also impose numerous technical requirements on postal service and express delivery enterprises to ensure the security of users' electronic information, including, among others, that users' electronic information be encrypted and stored in a separate location.

DATA SECURITY

The year 2014 witnessed significant efforts on the part of MIIT and other parts of the PRC government to improve standards in regard to data security.

MIIT Guiding Opinions

A key document, issued by MIIT Sept. 1, 2014, is the Guiding Opinions on Strengthening Network Security in the Telecommunications and Internet Sectors[10] (MIIT Opinions). The MIIT Opinions call for a coordinated effort by regulators and telecom enterprises to strengthen network security in the telecom and Internet sectors, starting with enhanced enforcement of existing regulations and standards governing network security and including adoption of a formal network MIIT security review mechanism. Further, the MIIT Opinions also:

- require bid invitation documents for the procurement of key software and hardware to expressly stipulate network security requirements;
- regulate the security aspects of the collection, storage, use and destruction of users' personal information; and
- encourage mobile application (app) stores to establish and improve systems to verify the identity of app developers and to test the security of apps in order to identify and blacklist malicious applications.

Banking Rules

It would appear that the banking sector has been chosen by regulators to be at the forefront of efforts to enhance network security.

On Sept. 3, 2014, the China Banking Regulatory Commission (CBRC), the National Development and Reform Commission, the Ministry of Science and Technology and MIIT issued the Guiding Opinions Regarding Application of Secure and Controllable Information Technologies to Strengthen Network Security and Information Construction in the Banking Sector[11] (Banking Opinions).

The Banking Opinions define a number of related goals for the banking sector in relation to data security, promoting the use by banks of ''secure and controllable information technologies'' and calling for implementation of network security review standards for the banking sector. Other key provisions include the following:

- Individual banks are exhorted to utilize secure and controllable technologies, with the goal that utilization will increase starting in 2015 at a rate of no less than 15 percent, with aggregate utilization of no less than 75 percent in 2019.
- The Banking Opinions include general policy language suggesting that development of local technology is encouraged. At the same time they call for ''open cooperation,'' which might be read to

[7] These standards are available, in Chinese and English, at http://www.pkunetlaw.cn/news_info.aspx?id=2441.

[8] These measures are available, in Chinese, at http://bit.ly/1N4lTsR.

[9] These measures are available, in Chinese, at http://www.spb.gov.cn/zcfg/gfxwj/201403/t20140326_301910.html.

[10] The MIIT Opinions are available, in Chinese, at http://www.miit.gov.cn/n11293472/n11293832/n12843926/n13917072/16121158.html.

[11] The Banking Opinions are available, in Chinese, at http://www.cbrc.gov.cn/govView_115696B8621049099A0B880DAB133A33.html.

  PVLR ISSN 1538-3423

mean that foreign participation is not intended to be restricted. However, this open cooperation is subject to conditions that priority be given to technologies and solutions that are ''highly open, highly transparent and of a broad application scope'' and to suppliers who are willing to work on a cooperative basis in relation to key knowledge and critical technologies. The Banking Opinions state that reliance on a single product or technology should be avoided.

The Banking Opinions were followed by issuance by the CBRC and MIIT on Dec. 29, 2014 of the following:

- the Notice Regarding Implementing Guideline for Printing and Circulating Application of Secure and Controllable Information Technology (2014–2015) (2014–2015 Guideline), which is appended with
- the Classification Catalog of Banking Information Technology Assets and Indexes of Security and Controllability (Catalog).[12]

The Guideline and Catalog implement the Guiding Opinions by confirming the scope of institutions covered by the requirements (broadly, including commercial banks and various categories of other financial institutions) and by defining specifically what ''security and controllability'' require in regard to stipulated categories of IT products and services. They also set minimum utilization rates for ''secure and controllable'' technology specific to each category of products and services, including various categories of software products.

Specific requirements regarding security and controllability, as well as specific utilization rates, vary with the particular type of software at issue. A general requirement applicable to all categories of software covered by the Catalog, as well as software embedded in specified hardware, is that related source codes must be filed with CBRC.

The Guideline sets out a relatively demanding work plan for banks in order to comply with the various requirements.

The period following issuance of the Guideline and Catalog have witnessed significant efforts by the U.S. and European Union to secure the Chinese government's agreement to shelve them. As of the time of writing, it appears the Chinese government may have agreed to delay their implementation.[13]

Formation of CAC; Formulation of Network Security Review Process

At the beginning of 2014, a major administrative restructuring was implemented that involved the separation of the State Internet Information Office (SIIO) from the State Council Information Office through establishment of SIIO as a separate government department under the oversight of the Central Leading Group for Cyberspace Affairs under the direct leadership of the Communist Party Chairman Xi Jinping. The English name now used by SIIO is the Cyberspace Administration of China (CAC) and www.cac.gov.cn was launched as its official website on Dec. 31, 2014. While the formal structure and authorities of the CAC have not been publicly disclosed, industry sources anticipate that CAC will have significant authority over network security issues.

Various existing regulations and standards contemplate implementation of a formal network security review process affecting IT products and services, and one priority task of the CAC appears to be formulation of such a mechanism.

Media reports suggest work is underway to formulate a mandatory network security review process, with the Xinhua state-owned news agency, in a Jan. 19, 2015, news report, quoting a CAC official as saying that CAC had finalized draft network security review measures and would submit them for review to the Central Leading Group for Cyberspace Affairs, the Communist Party organization that oversees CAC operations in February.[14]

Draft Anti-Terrorism Law

On Nov. 3, 2014, the NPC issued the Anti-Terrorism Law (First Review Draft) for public comments.[15]

The first draft of the law caused significant concerns on various fronts due to the following requirements:

- In their design, construction and operation of telecoms and Internet networks, telecom network operators and Internet service providers must ''preset'' a technical interface and submit the encryption scheme with the authority responsible for encryption—vague language that commentators understand to mean that PRC government authorities would have broad rights to monitor network use.
- Telecom services providers and Internet service providers must keep relevant equipment and data with respect to local users within the territory of China. The relevant provision suggests that the data may be exported as long as the same data have also been retained in China.

According to Mar. 9, 2015, comments[16] made by a representative of the legislative drafting committee of the NPC Standing Committee, a review of a second draft of the law was completed in February and, while the law was not on the agenda for the annual NPC session held on Mar. 5, 2015, the law may undergo third reading and promulgation later in 2015.

The draft law has been criticized by the U.S. government and other parties for the overbroad monitoring rights that Chinese government authorities would have. In responding to questions about the draft law, spokesperson for the NPC, Fu Ying, is quoted by Xinhua news agency[17] as stating that the second draft of the law

[12] The Guideline and Catalog have not been made publicly available, having been issued by the CBRC or its local branches to affected financial institutions.

[13] Len Bracken, *China Delays Cybersecurity Rule, as Requested by U.S., EU, Japan*, 14 Bloomberg BNA Privacy & Sec. L. Rep. 618 (Apr. 6, 2015) (14 PVLR 618, 4/6/15).

[14] A news report published by Xinhua, China's state-owned media outlet, is available, in Chinese, at http://news.xinhuanet.com/2015-01/19/c_1114042721.htm.

[15] The draft text of the Anti-Terrorism Law is available, in Chinese, at http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2014-11/03/content_1885027.htm.

[16] As reported on People's Daily Online, in Chinese, at http://politics.people.com.cn/n/2015/0309/c70731-26663531.html.

[17] The quotes are available, in Chinese, at http://news.xinhuanet.com/politics/2015-03/04/c_1114517556.htm.

stipulates that use of the technical interface (1) is limited for purposes of investigating and preventing terrorist activity; (2) is limited to public and state security agencies; and (3) is subject to a strict review and approval process.

WHAT TO WATCH FOR IN 2015

If 2014 is any indication, China will be an interesting jurisdiction for data privacy and security practitioners in 2015.

Look for:

- continued issuance of sector-specific data privacy rules in various sectors;
- increased enforcement of data privacy rules, particularly online rules and rules governing consumer information;
- further criminal prosecutions in regard to data privacy breaches and, potentially, broadening of criminal law provisions;
- enhanced enforcement of existing data security regulations and, likely, implementation of a formal network security review process affecting both IT product suppliers and service providers; and
- developments in regard to promulgation of the Anti-Terrorism Law incorporating provisions that broaden government access to data traffic on information and telecommunications networks.

  PVLR ISSN 1538-3423