COVINGTON

Data Privacy in China
2015 Year in Review

January 2016

Data Privacy and Cybersecurity

Important new trends emerged in 2015 as Chinese regulators continued to focus greater attention on data privacy and security issues. Notably, data protection issues became increasingly linked to laws and regulations related to China's emerging national security and cybersecurity regime. The nexus between data protection and national security also indicates that the government may begin to play a greater role in the enforcement of data-related obligations.

Government concerns have been amplified by a number of highly publicized actual or potential data security breaches, including: the potential leak of millions of users' sensitive personal information through security loopholes in social security systems in over 30 provinces; allegations of potential exposure of email accounts and passwords run by a major Chinese Internet company; and a public admission of a security flaw in mobile software of a major Chinese messaging and social media platform.

Multinational companies with operations in China should understand Chinese data protection laws and regulations that may affect their businesses in two main ways. First, they should ensure that they are in full compliance with Chinese laws and regulations, particularly because of heightened scrutiny by regulators. Second, multinational companies should ensure that their compliance with Chinese laws and regulations, including those pertaining to cybersecurity and government access, does not conflict with privacy policies and legal obligations in other jurisdictions.

This year-end review briefly summarizes a number of notable developments for data privacy professionals and multinational companies with interests in China.

If you would like to learn more about these developments, you may contact our China data privacy and cybersecurity team using the information below and join our China privacy mailing list here.

Eric Carlson	+86 21 6036 2503	ecarlson@cov.com
Ashwin Kaja	+86 10 5910 0506	akaja@cov.com
Kurt Wimmer	+1 202 662 5278	kwimmer@cov.com
Daniel Cooper	+44 20 7067 2020	dcooper@cov.com
Jetty Tielemans	+32 2 549 52 52	htielemans@cov.com

January 5

China Clarifies Requirements for Companies Regarding Consumers' Personal Information

On January 5, the State Administration of Industry and Commerce ("SAIC") issued measures to implement China's *Consumer Rights Protection Law* ("CRPL"), which was amended effective March 15, 2014 to include, among other things, provisions on the protection of personal information of consumers and administrative penalties for the misuse of personal information. The newly promulgated measures, entitled *Measures on Penalties for Infringing Upon the Rights and Interests of Consumers* ("Implementing Measures"; Covington's translation available here) flesh out the CRPL by addressing a range of consumer protection issues. From a privacy perspective, the Implementing Measures (1) clarify the definition of "personal information of consumers"; (2) provide more detail on the CRPL's requirements for the collection, use, and protection of consumer personal information; and (3) provide for significant penalties for violations. The Implementing Measures took effect on March 15, 2015, China's Consumer Protection Day.

For more information, see our post on Covington's InsidePrivacy blog here.

February 2

Internet Gatekeeper Announces Legislation to Enhance Personal Information Protection

China's principal Internet regulator, the Cyberspace Administration of China ("CAC"), announced in February 2015 that China would advance new legislation to combat the improper collection, use, and sale of personal information—a *Personal Information Protection Law*. The new legislation, announced during an interview of a senior CAC official by state-owned Xinhua News, was reportedly being drafted by the CAC, the Ministry of Industry and Information Technology ("MIIT"), and the Ministry of Public Security ("MPS").

A draft has not yet been released, but if the announcement is accurate, it may lead to the most significant piece of data privacy legislation under consideration since a scholarly draft proposing a more comprehensive framework for protecting personal information, apparently abandoned, was submitted to the State Council in 2008.

May 19

China Clarifies Requirements for Marketing via SMS

On May 19, MIIT published measures to implement various high-level provisions related to SMS marketing in several different laws that, taken together, require companies to (1) comply with express requests from consumers not to send such communications; (2) disclose the identity and contact information of the advertiser in electronic advertising; and (3) provide a way for consumers to refuse future electronic advertisements.

The newly promulgated measures, entitled the *Administrative Rules for Short Message Services* (official Chinese version available here; Covington's translation available here) flesh out these general rules related to SMS marketing. In addition to the general consent and disclosure requirements in the laws listed above, the new SMS rules, effective June 30, 2015, (1) define commercial SMS messages; (2) provide more detailed rules regarding

consent and refusal in the commercial SMS context; (3) impose SMS and mobile subscription data retention requirements on SMS service providers (e.g., mobile operators such as China Mobile and China Unicom); and (4) outline penalties for violations.

For more information, see our post on Covington's InsidePrivacy blog here.

July 1

Draft Regulations Preview Stricter Rules on Internet Advertising

On July 1, SAIC published a draft of the *Interim Measures on the Supervision of Internet Advertising* ("Draft Internet Advertising Measures"; original Chinese available here) for public comment. If adopted as drafted, the Draft Internet Advertising Measures would (1) require advertisements in email and instant messaging to contain conspicuous options for the user to agree to, refuse, or unsubscribe from advertisements; (2) require websites to allow users to block pop-ups for certain repeat visitors; and (3) require advertisements sent via email or instant message to identify senders and be marked as advertisements.

The Draft Internet Advertising Measures, once finalized, would be the first to focus specifically on Internet advertising, and primarily serve to implement China's recently revised *Advertising Law*, amended in April 2015 and effective September 1, 2015. The amended *Advertising Law* prohibits sending electronic advertising without prior consent or request by recipients. Senders are required to disclose their true identities and contact information, and provide a choice to unsubscribe from the advertisements. The amended *Advertising Law* also requires that the "close" button on Internet advertisements must be prominently visible, and that users can close advertisements with a single action. The Draft Internet Advertising Measures provide more details on these requirements.

Although it was reported in November that the Draft Internet Advertising Measures would be adopted by the end of calendar year 2015, no such announcement has been made to date.

For more information, see our post on Covington's InsidePrivacy blog here.

July 1

China Enacts Sweeping National Security Law

Although mostly focused on national security issues, the scale and scope of China's new *National Security Law* merits mention here due to certain provisions related to data protection. On July 1, the Standing Committee of the National People's Congress passed a sweeping new *National Security Law* (official Chinese version available here). The scope of the law, China's most comprehensive piece of national security legislation to date, is broad. It covers issues of political security, military security, economic and financial security, social and cultural security, nuclear security, ecological security, and more.

One chapter of the law lays out obligations for citizens and corporations to assist the government in protecting national security. Article 77 requires that citizens and corporations "timely report information on activities that may damage national security"; "provide (to the authorities) accurate evidence on activities that may damage national security"; "protect national secrets"; and *"provide necessary support and assistance to national security, public security, and relevant military agencies."* The italicized text reflects general language in the final version of the law that has replaced more specific language included in the draft version stating that citizens and corporations must provide data, information, and technical support or assistance.

As is generally the case with high-level laws in China, details of these obligations will begin to take form in the coming months and years through implementing measures issued by regulating agencies.

For a general discussion of the new *National Security Law*, see our post on Covington's GlobalPolicyWatch blog here. You can read our more detailed alert on the topic here.

July 6

China Issues Draft Network Security Law

On July 6, China's National People's Congress ("NPC") released a draft of the *Network Security Law* (also referred to as the draft *Cybersecurity Law*). If enacted as drafted, this draft law would apply broadly to entities or individuals that construct, operate, maintain, and use networks within the territory of China, as well as those who are responsible for supervising and managing network security.

The draft law would impose a series of obligations on network operators, defined to include operators of basic telecommunications networks, Internet information service providers, and key information system operators. Some of these obligations are restatements of rules set out in existing laws and regulations, but consolidated and elevated due to the higher-level legal authority of the draft law if enacted. There are also several new privacy-related rules relating to (1) required notification in cases of data breach; (2) data localization requirements and potential security assessments for the transfer of data across borders; and (3) a broader definition of "personal information" to include "personal biometric information."

For more information, see our post on Covington's InsidePrivacy blog here. A more general discussion of the draft *Network Security Law* can be found on Covington's GlobalPolicyWatch blog here, or in our alert on the topic here.

November 16

New Regulation Requires Real-Name Identification for Couriered Packages; Relevant Protections for Personal Information

On November 16, the Legislative Affairs Office of the State Council published a draft *Regulation on Couriers* (official Chinese version available here) for public comment. Increased government attention to the regulation of courier services follows the rapid development of the industry in China and fears that it could be used as a vehicle for terrorism.

The draft regulation requires courier companies to verify the authenticity of information on package waybills (including "identification information, addresses, and contact information" for both senders and receivers) and refuse orders with false information. Concerns regarding the protection of personal information shared with courier companies are reflected in data privacy-related provisions contained in the regulation. Courier companies and their employees may not illegally sell or disclose user information obtained through their operations, and must, in the case of a leak, damage, or loss of user information, promptly implement remedial measures and notify postal authorities. Courier companies are also required to set up a management system for handling courier waybills and electronic data, and regularly destroy waybills in order to ensure the security of personal information.

December 27

New Counter-Terrorism Law Enacted

On December 27, the Standing Committee of the National People's Congress, China's top legislative body, enacted the *Counter-Terrorism Law* (official Chinese version available here; unofficial translation available here), which took effect on January 1, 2016. The *Counter-Terrorism Law* reinforces the government's broad powers to investigate and prevent incidents of terrorism and requires citizens and companies to assist and cooperate with the government in such matters. It imposes additional and specific obligations on companies in certain sectors, including those providing telecommunications, Internet, and financial services. Non-compliance or non-cooperation can lead to significant civil or criminal penalties.

The law's broadly worded requirements create some uncertainty as to their implications for companies' data protection and security policies. The final version of the law removes some of the more controversial requirements of the draft versions, but still imposes new requirements that merit careful attention, such as requirements for telecommunications and Internet service providers to (1) provide technical support and assistance to the authorities as needed, including handing over access or interface information and decryption keys; and (2) establish content monitoring and network security programs—including censorship, storage, and reporting mechanisms—for content related to extremism or terrorism. The law also imposes obligations on companies in other sectors such as freight, transportation, and hospitality.

For more information, see our post on Covington's InsidePrivacy blog here. A more general discussion of the new *Counter-Terrorism Law* can be found in our alert on the topic here.

December 28

People's Bank of China Issues Further Rules for Online Payment Institutions

On December 28, the People's Bank of China ("PBOC") published the *Administrative Measures for Online Payment Business of Non-Bank Payment Institutions* ("NBPI Measures"; official Chinese version available here). These measures supplement the *Administrative Measures for Payment Services of Non-Financial Institutions* ("NFI Measures") that went into effect in September 2010. Compared to the NFI Measures, the new NBPI Measures focus on online payment services such as those facilitating "internet payments, mobile phone payments, landline payments, and digital television payments" offered by NBPIs that have already obtained Payment Business Licenses. Effective July 1, 2016, the NBPI Measures lay out a number of requirements related to real-name identification and authentication—"know your customer" provisions—including the need to use real names, verify identities (storing copies of identification certificates), and keep accurate records of payment activities.

Recognizing the risks associated with handling and storing such sensitive information, the NBPI Measures also incorporate data protection and security requirements. NBPIs must adopt effective protective measures and risk control systems, and may not store sensitive information such as tracking or chip information, verification codes, or passwords. They also may not store dates of effectiveness of bank cards unless required (in which case the data must be encrypted). Generally, the collection, use, storage, and transfer of customer information, unless otherwise authorized by the customer or required by law, is to be conducted on a "minimum extent necessary" principle with customers kept informed. The

NBPI Measures also make NBPIs responsible for the data protection practices of merchants, requiring them to include data protection standards (including a prohibition on storing sensitive information) in relevant agreements and to implement systems for monitoring or periodically checking merchant practices, among other things.

* * *