COVINGTON

China Privacy Developments in 2018

January 2, 2019

Data Privacy and Cybersecurity

The past year was a particularly significant one for the development of Chinese privacy law. During 2018, the Chinese government systematically established the country's regulatory requirements for cybersecurity and data privacy and continued to implement the Cybersecurity Law, which took effect on June 1, 2017.

Multiple regulators, including the Ministry of Public Security ("MPS"), the Cyberspace Administration of China ("CAC") and the Ministry of Industry and Information Technology ("MIIT"), released regulations and brought enforcement actions against companies in the past year. We expect the overall trend of heightened regulation and increased enforcement to continue in 2019.

Rulemaking Developments in 2018

Ministry of Public Security ("MPS") rules and regulations

MPS is the agency leading the government's effort to implement the Multi-level Protection Scheme ("MLPS"), a cybersecurity framework that classifies information systems physically located in China based on their relative impact on national security, social order, and economic interests in the event of damage or an attack. MPS issued two draft regulations for public comment and finalized one regulation on Internet Security Supervision and Inspection.

Regulation on the Internet Security Supervision and Inspection

On September 30, 2018, MPS released the *Regulation on the Internet Security Supervision and Inspection by Public Security Agencies* (the "Inspection Regulation"), which took effect on November 1, 2018. The Inspection Regulation sets forth detailed procedural guidance on how local Public Security Bureaus ("PSBs") should conduct cybersecurity inspections of companies that provide a broad range of "Internet services" in China. These "Internet services" include:

- Internet access, data centers, content distribution, and domain name services;
- Internet information services;
- Public Internet access services; and
- Other Internet services.

Local PSBs have broad discretion to decide whether a company falls within the Regulation's purview, including the ability to interpret what services are considered "other Internet services." PSBs are also provided wide-ranging powers to conduct both on-site and remote inspections. They are authorized to enter a company's physical premises—including data centers—to

conduct an unannounced on-site inspection, review and copy documents, and interview company executives. PSBs may also conduct remote inspections, provided that the company is informed of the time and scope of the inspection beforehand. In addition, PSBs are allowed to engage qualified third-party vendors to provide technical support for the PSB's inspections.

Even though the Inspection Regulation codifies existing practices rather than imposing new obligations on Internet service companies, it will likely pave the way for more cybersecurity enforcement actions from local PSBs in the future.

Draft Regulations on Cybersecurity Multi-level Protection Scheme

In June 2018, MPS released for public comment a draft of the *Regulations on Cybersecurity Multi-level Protection Scheme* ("the Draft MLPS Regulation"). The Draft Regulation, a binding regulation once finalized, echoes requirements in the Cybersecurity Law and provides guidance for network operators on how to comply with the MLPS.

The Draft MLPS Regulation updates the existing MLPS, a framework dating back to 2007. The original MLPS uses a one-to-five scale to classify information systems physically located in China based on their relative impact on national security, social order, and economic interests, with one being the least critical and five being the most critical. Network operators that are classified (initially self-assessed and proposed by operators, and then confirmed by MPS) at level 3 or above are subject to enhanced security requirements.

Once the Draft MLPS Regulation is finalized, MPS is expected to take more enforcement actions against non-compliance with the MLPS.

MPS Guideline on Protection of Personal Information

On November 30, 2018, MPS released a draft *Guideline for Internet Personal Information Security Protection* ("the Draft Guideline") for public comments. Although it is still unclear whether this Draft Guideline will be legally binding, MPS will likely enforce its requirements when exercising its authority under the Cybersecurity Law.

The Draft Guideline applies to personal information collected through the Internet by "personal information holders," a new concept that covers both data controllers and data processors. Personal information holders are required to adopt organizational and technical measures to protect personal information they hold. This includes detailed requirements on how personal information holders should protect personal information across the life cycle of data, covering collection, retention, usage, deletion, processing by third parties, sharing, transfer and disclosure of personal information. The Draft Guideline also requires personal information holders to have good incident response programs so that they can react quickly to any data breach incidents.

Although the Draft Guideline cross-references the national standard on protecting personal information for some of its definitions and requirements, the Draft Guideline is not completely aligned with the standard.

National Standard on Protection of Personal Information

China's national standard on personal information protection, entitled GB/T 35273-2017 *Information Technology - Personal Information Security Specification* ("the Standard"), came into effect on May 1, 2018. Given that China does not have a separate personal information

protection law, the Standard—though nominally voluntary—effectively sets out the best practices that will be expected by regulators auditing companies and enforcing China's Cybersecurity Law and data protection rules.

Consistent with the general principles of most data protection laws, the Standard requires, for example, transparency, specificity and fairness when processing personal information; proportionality when collecting, using and retaining personal information (use and retention of only the minimum information necessary to achieve the stated purpose); ensuring security for personal information collected; and respecting individuals' rights to control the processing of information about them. It also requires either consent from individuals, or reliance on a limited range of exceptions, for the purpose of collection and processing of personal information.

Supreme People's Procuratorate Guidelines

On November 9, the Supreme People's Procuratorate of China released the *Guidelines for Handling Criminal Cases Involving the Infringement of Citizen's Personal Information* ("the Procuratorate Guideline").

China's Criminal Law prohibits illegally disclosing personal information, as well as illegally obtaining personal information through theft or other means. If the offense of individuals or companies falls within the scope of "serious circumstances" or "particularly serious circumstances", criminal liability may be triggered. "Serious circumstances" include, for example, when personal information is used to commit a crime, or when a defendant obtains, provides, or sells personal information above a threshold amount. "Particularly serious circumstances" include cases where the infringement of personal information causes death, serious injury, significant economic loss, or adverse social effects.

The Procuratorate Guideline addresses some key issues raised by the *Interpretation of Applicable Laws on Handling Criminal Cases Involving Infringement of Citizens' Personal Data* ("Interpretation"), a judicial interpretation jointly released by China's Supreme People's Court and Supreme People's Procuratorate on June 1, 2017. Notably, the Procuratorate Guideline provides detailed instructions for when and how prosecutors should investigate and prosecute the infringement of citizens' personal data. For instance, where there is a theft of personal information, procuratorates must carefully review the evidence that is used to prove that the offender was responsible, including the offender's IP address, MAC address and other offender's records discovered in the victim's computer system.

The Procuratorate Guideline also clarifies the scope of information that is considered "personal" for the purposes of prosecuting the infringement of citizens' personal information. Under the Procuratorate Guideline, phone numbers and information used to register a company do not fall within the scope of personal information so long as the phone was purchased and used by the company. Procuratorates are instructed to distinguish between phones purchased and used exclusively by a company, and personal phone numbers used by a company representative to register a business.

Enforcement Actions in 2018

In 2018, two sectoral regulators, the Ministry of Science and Technology (MOST) and the MITT, took additional steps to enforce sectoral regulations, some of which pre-dated the Cybersecurity Law.

Ministry of Science and Technology (MOST) Action on Genetic Data

On October 25, 2018, the Ministry of Science and Technology ("MOST") announced that six entities were fined for violating the *Interim Administrative Measures on Human Genetic Resources* ("Interim Measures", effective June 10, 1998) on the grounds that the violators failed to obtain prior approval from the MOST before they initiated cross-border transfers of genetic data collected in China.

According to the Interim Measures, human genetic resources associated with international collaborations (i.e. clinical trials) may be transferred abroad only if the international collaboration receives prior approval from MOST, and the entity transferring offshore human genetic resources first obtains a cross-border transfer certificate.

Although the Interim Measures predated the Cybersecurity Law and are not a dedicated data protection regulation, this enforcement action highlights the concerns of the Chinese government that foreign companies were procuring and transferring offshore a large amount of Chinese genetic material without approval. Cross-border transfers of healthcare data may remain an enforcement priority for Chinese agencies going forward.

MIIT enforcement action related to personal information protection

On November 26, 2018, MIIT announced that a cybersecurity inspection revealed that seven companies had failed to fulfill their obligations under the Cybersecurity Law and MIIT's sectorial regulations, including the *Measures for the Administration of Communication Cybersecurity Protection* (effective March 1, 2010) and the *Provisions on Protecting the Personal Information of Telecommunications and Internet Users* (effective September 1, 2013). These violations included failing to file for an MLPS classification, failing to establish internal policies and procedures for the collection and use of personal information, and failing to launch the security assessment process for new services, among others.

Key Developments Expected in 2019

Regulation for the Protection of the Critical Information Infrastructure

We expect the final version of the *Regulation for the Protection of the Critical Information Infrastructure* ("CII Regulation") to be released in the first few months of 2019. The draft CII Regulation was released by the Cyberspace Administration of China ("CAC") on July 11, 2017. Once finalized, the CII Regulation will clarify the scope of CII and elaborate on the regulatory requirements imposed on CII operators. The CII Regulation may also provide further detail about how CII operators should interact with agencies on information sharing, threat monitoring, and cybersecurity inspections.

Measures on Cross-border Data Transfer

On April 11, 2017, CAC released a draft of the Measures on Security Assessment of Cross-border Data Transfer of Personal Information and Important Data ("the Draft Measures"). One month later, another draft was released to several international stakeholders that were invited to attend a seminar held by CAC. The Draft Measures will be finalized in 2019. Once finalized, the Draft Measures will play a key role in creating China's comprehensive framework for regulating cross-border data flows.

Under the Draft Measures, network operators in China may face a general obligation to assess the security of their cross-border data transfers and potentially undergo security assessments for such transfers by the Chinese government. To avoid any disruption of data transfers, companies with operations in China should consider closely following the development of these Draft Measures and consider taking steps to comply with relevant security assessment requirements once the Draft Measures are finalized.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Data Privacy and Cybersecurity practice:

Yan Luo	+86 10 5910 0516	yluo@cov.com
Jetty Tielemans	+32 2 549 52 52	htielemans@cov.com
Kurt Wimmer	+1 202 662 5278	kwimmer@cov.com