Significant changes to data and cybersecurity practices in China

Intellectual Property Update

11 NOV 2016
By: Scott Thiel | Carolyn Bigg | Paula Cao

PRC Cybersecurity Law to come into effect in June 2017 requiring significant changes to data and cybersecurity practices in China.

After a third deliberation, the Chinese government passed the new PRC Cybersecurity Law on 7 November 2016. The new law will come into force on 1 June 2017 and has significant implications for the data privacy and cybersecurity practices of both Chinese companies and international organisations doing business in China.

The new PRC Cybersecurity Law intends to combat online fraud and protect China against Internet security risks. In short, it imposes new security and data protection obligations on "network operators"; puts restrictions on transfers of data outside China by "key information infrastructure operators"; and introduces new restrictions on critical network and cybersecurity products.

The new law has been widely reported in both the local and international press. While Chinese officials maintain that China is not closing the door on foreign companies with the introduction of this new law, there has been widespread international unease since the first reading. Commentators have expressed concern that competition will be stifled; regarding the handover of intellectual property, source codes and security keys to the Chinese government; as to perceived increased surveillance and controls over the Internet in China; and in relation to the data localisation requirements. Other new obligations, including increased personal data protections, have been less controversial, but are a clear indicator of the increased focus within the Chinese authorities on data protection, and could signal a change to the data protection enforcement environment in China.

Some of the key provisions of the final law (which contains some changes to earlier drafts of the law) include (*inter alia*):

- Chinese citizen's personal information and "important data" gathered and produced by "key information infrastructure operators" (KIIO) during operations in China must be kept within the borders of the PRC. If it is "necessary" for the KIIO to transfer such data outside of China, a security assessment must be conducted pursuant to the measures jointly formulated by the National Cyberspace Administration and State Council unless other PRC laws permit the overseas transfer. While the final version of the law provides some guidance as to the industry fields that will be acribed greater protection, such as public communications and information service, energy, transportation, water conservancy, finance, public service and e-government, the definition of KIIO remains vague and could potentially be interpreted to cover a broader range of companies and industry sectors. "Personal information" is defined as including 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. However, the types of information that might constitute "important data" is currently unclear. In any case, these data localisation rules are likely to create practical issues for international businesses operating in China.

- A range of new obligations apply to organisations that are "network operators" (ie network owners, network administrators and network service providers). A "network" means any system comprising computers or other information terminals and related equipment for collection, storage, transmission, exchange and processing of information. Some commentators are suggesting that these broad definitions could catch any business that owns and operates IT networks/infrastructure or even just websites in China.

  In terms of data protection, network operators must make publicly available data privacy notices (explicitly stating purposes, means and scope of personal information to be collected and used); and obtain individuals' consent when collecting, using and disclosing their personal information. Network operators must adopt technical measures to ensure the security of personal information against loss, destruction or leaks, and in the event of a data security breach must take immediate remedial action and promptly notify users and the relevant authorities. They must also comply with principles of legality, propriety and necessity in their data handling, and not be excessive; not provide an individual's personal information to others without the individual's consent; nor illegally sell an individual's personal data to others. The rules do not apply to truly anonymised data. There are also general obligations to keep user information confidential and to establish and maintain data protection systems. Data subject rights to correction of their data, as well as a right to request deletion of data in the event of a data breach, are also provided. While an earlier draft specifically provided protection to personal information of "citizens", the final law does not make this distinction, and so seemingly offers a broader protection to all personal information. These requirements formalise as binding legal obligations some data protection safeguards that were previously only perceived as best practice guidance in China.

  As regards network security, network operators must fulfil certain tiered security obligations according to the requirements of the classified protection system for cybersecurity, which includes (amongst other things): formulating internal security management systems and operating instructions; appointing dedicated cybersecurity personnel; taking technological measures to prevent computer viruses and other similar threats and attacks, and formulating plans to monitor and respond to network security incidents; retaining network logs for at least six months; undertaking prescribed data classification, back up, encryption and similar activities; complying with national and mandatory security standards; reporting incidents to users and the authorities; and establishing complaints systems.

  Network operators must also provide technical support and assistance to state security bodies safeguarding national security and investigating crimes, and will be subject to government and public supervision. The form and extent of such cooperation is not currently clear, and international businesses have expressed concerns over the extent to which this may require them to disclose their IP, proprietary and confidential information to the Chinese authorities.

  More general conditions on network operators carrying out business and service activities include: obeying all laws and regulations, mandatory and industry national standards, social mores and commercial ethics; being honest and credible; and bearing social responsibility. There are also requirements on network operators to block, delete and report to the authorities prohibited information and malicious programmes published or installed by users.

  Network operators handling "network access and domain registration services" for users, including mobile phone and instant message service providers, are required to comply with "real identity" rules when signing up or providing service confirmation to users, or else may not provide the service.

- Additional security safeguards apply to KIIOs, including: security background checks on key managers; staff training obligations; disaster recovery back ups; emergency response planning; and annual inspections and assessments. Further, strict procurement procedures will apply to KIIOs buying network products and services.

- Providers of "network products and services" must comply with national and mandatory standards; their products and services must not contain malicious programs; must take remedial action against security issues and report them to users and relevant authorities; and must provide security maintenance for their products and services which cannot be terminated within the contract term agreed with customers. These new conditions will require providers of technology products and services to review and update their product and related maintenance offerings and, in particular, the contractual terms on which they are offered to customers.

- Critical network equipment and specialised cybersecurity products must obtain government certification or meet prescribed safety inspection requirements before being sold or provided. This potentially catches a wide range of software, hardware and other technologies being sold - or proposed to be sold - byl international companies in the China, since the definitions used in the law are drafted very broadly. Further guidance by way of a catalogue of key network products is expected in due course. There are concerns that this may create barriers to international businesses looking to enter the Chinese market.

- Each individual and organisation shall be responsible for its own use of websites, and may not set up websites or communication groups for the purpose of committing fraud, imparting criminal methods, producing or selling prohibited items, or engaging in other unlawful activities. Again, there is scope for this to be interpreted and applied broadly.

- Institutions, organisations and individuals outside China that cause serious consequences by attacking, interfering or destructing key information infrastructure of China shall be responsible for any damage, and the relevant public security department of the State Council may freeze assets and impose other sanctions against them. While these provisions would appear to have an extra-territorial effect, and could be interpreted very broadly, it is unclear what sanctions could in practice be enforced against organisations without a presence in China.

- Other new rules relate to: network/online protections for minors; the establishment of schemes for network security monitoring, early warning and breach notification to relevant authorities and the public, as well as rights for individuals and organisations to report conduct endangering network security; opening of public data resources; and prohibitions on hacking and supporting activities.

While criminal sanctions, administrative penalties and civil liabilities potentially await those (both organisations and, in some circumstances, individual employees and officers) who violate the new law, unfortunately great uncertainties remain as to how the new legislation will be enforced, who exactly is caught by the various new rules, and the precise steps that organisations must take to comply with them. It is hoped that the Chinese authorities will publish more detailed, practical guidance in the coming months. In the meantime, organisations are strongly advised to review their data privacy and cybersecurity practices in China to ensure compliance with the new law before it comes into force on 1 June 2017, and to keep these under review as further guidance becomes available.

AUTHORS

Scott Thiel
Partner
Hong Kong | T: +852 2103 0808

Carolyn Bigg
Partner
Hong Kong | T: +852 2103 0808
