Bloomberg Law

Privacy and Security Law Report®

Cybersecurity

Strengthening the Great Cyber-Wall of China—An Effort in Protecting the Masses in Cyberspace or Keeping Out the Foreigners?

China's Cybersecurity Law

China's recent cybersecurity laws have been cited by the government as internet and personal data protection milestones, while being viewed with suspicion by foreign multinationals as potentially increasing compliance costs. The one certain thing is that the Chinese government is succeeding in exercising more control and oversight over cyberspace, the authors write.

By Benjamin Cheong and Terrance Tong

Introduction

The flurry of legislative reforms in China in recent months saw the recurring theme of national security dominating the Chinese cybersecurity agenda. Extending the notion of national security to the cyberspace, recent cybersecurity-related legislative developments set the stage for China's increasingly complex web of cybersecurity regulations and demonstrate the government's resolve to tighten its control over the internet and cyber activities. These laws have been lauded by Beijing as milestones in the protection of China's cyberspace and personal data of Chinese citizens, while being viewed with suspicion by foreign multinational companies as potentially increasing compliance costs, leaving them vulnerable to industrial espionage and giving Chinese companies an unfair advantage.

Benjamin Cheong is a partner as Rajah Tann Singapore LLC in Singapore where he is a member of the technology, media, and telecommunications practice and data protection and cybersecurity practice.

Terrance Tong is a trainee solicitor at PK Wong & Associates LLC in Singapore.

This article will briefly analyse the scope of these newly promulgated laws and their relevant implementing regulations, how they are likely to be implemented and address the impact of these laws and regulations for multinationals operating in or seeking to expand their footprint into China.

The Complicated Web of Cyber-Govenance

The Anti-Terrorism Law The Anti-Terrorism Law (ATL), which came into effect on Jan. 1, 2016, was introduced to ''prevent and punish terrorist activities, strengthen counter-terrorism efforts and to safeguard the security of the state, the public and the lives and properties of the people''. Although the ATL seeks primarily to safeguard against terrorism and prevent terrorist activities generally, certain provisions of the ATL imposes statutory obligations specifically on telecommunications operators and internet service providers.

At the outset, it should be noted that the terms ''telecommunications operators'' and ''internet service providers'' are not defined within the ATL, and can potentially take on a wide enough interpretation to include any companies or businesses providing telecommunications, internet or any ancillary services.

Under Article 18 of the ATL, telecommunications operators and internet service providers have a specific

obligation to ''provide technical support assistance to public security organs and state security organs'' in the course of prevention and investigation of terrorist activities.

Article 19 of the ATL also requires these companies to implement network security and information content monitoring systems, so as to actively monitor and prevent the dissemination of information with terrorist or extremist content. This is coupled with the obligation to disclose such content to the relevant state authorities and to conduct user identifications before provision of services.

Non-compliance with the ATL could also attract stiff fines of up to 500,000 RMB ($75,270) and even personal liabilities for managers or personnel who are responsible for their companies' contravention of the ATL, which may result in such persons being detained.

In light of the broad requirements of the ATL, there are wide ranging implications beyond the potential cost of compliance. One such implication would be that multinational companies operating in China will have to bear the risk of their valuable intellectual property rights being compromised when compelled under the ATL to provide technical assistance in the form of disclosure of technical data and decryption technology. The Chinese government has, however, given the reassurance that this legislation ''accords with the actual work needed to fight terrorism which is basically in line with what other major countries in the world do. This will not affect the normal operation of tech companies and they have nothing to fear in terms of having ''backdoors'' installed or losing intellectual property rights''. This will remain to be seen once the Chinese authorities start enforcing the ATL.

The National Intelligence Law In the same vein, the National Intelligence Law (IL), which came into effect on June 28, 2017, seeks to bolster national intelligence efforts for the purposes of preserving national interests and security. However, unlike the ATL which imposes statutory obligations on telecommunications operators and internet service providers in China, the IL gives the relevant authorities sweeping powers to monitor both foreign and domestic individuals and companies.

More specifically, Articles 10 to 17 of the IL confers upon Chinese intelligence institutions extensive powers in the course of carrying out intelligence efforts. These institutions are authorized to use all necessary means to carry out espionage, domestically and abroad, and to compel relevant organizations or citizens to provide necessary assistance in the course of carrying out such efforts.

The IL further empowers relevant intelligence institutions to, amongst other things:

(i) enter relevant restricted areas and venues, learn from and question relevant institutions, organizations, and individuals;
(ii) use or lawfully request, the use of transportation, communications tools, premises and/or buildings belonging to any state organs, organizations or individuals; and
(iii) when necessary, set up relevant work sites, equipment, and facilities.

As with the ATL, there is a real risk that valuable intellectual property rights such as trade secrets belonging to companies operating in China may be compromised if it is assessed by the authorities to be necessary for the purposes of carrying out espionage. Individuals who are in violation of the IL or found to have obstructed national intelligence efforts may, under Article 28, be detained up to 15 days.

Companies operating in China may find it a relief to note that Articles 26 and 27 of the IL provide for measures that aim to safeguard against the abuse of powers, requiring intelligence institutions to put in place proper procedures and channels for anonymous complaints of abuses of power. However, the practical effect of the measures will in a large part also depend on its implementation, and it remains to be seen if it will in fact achieve its stated purpose.

The Cybersecurity Law The Cybersecurity Law (CSL), which came into effect on June 1, 2017, is one of the most important and comprehensive piece of legislation that seeks to consolidate China's regulation of cyber activities. The primary purpose of the legislation is to safeguard China's cyberspace sovereignty, national security and the societal public interest. This is to be achieved through the CSL's focus on ''personal'' and ''critical'' data, and a tiered system of network security provisions.

Various data privacy and cybersecurity obligations are imposed on ''network operators,'' which is broadly defined as ''network owners, managers, and network service providers'' of ''systems comprised of computers and other information terminals and related equipment'' that gather, store, transmit, exchange, and process information''. This definition not only covers telecommunication, wireless communication, and internet service providers but could ostensibly cover every organization or business that owns or operates IT networks in China.

The general cybersecurity obligation is found under Article 21 of the CSL which stipulates key duties that network operators are to perform. This includes formulating internal security management systems, adopting appropriate technological measures to prevent viruses and malwares, monitoring of network operational status, and storage of network logs for at least six months. Chapter IV of the CSL also governs and sets out the rule on usage, collection and transfer of personal data belonging to Chinese citizens.

In addition, the CSL imposes three specific sets of obligations:

(i) Restrictions on network products and services;
(ii) Obligations imposed on Network Operators; and
(iii) Obligations imposed on Critical Information Infrastructure Operators (CII Operators).

Restrictions on Network Products and Services

All ''critical network equipment'' and ''specialised network security products'' must comply with government-issued standards of security. Further, under Article 23, these network products and services must be subject to an inspection and certification process before the sale or provision of the products or services.

These terms are not specifically defined in the CSL. However, a catalogue detailing specifically which products and services would be subject to Articles 22 and 23 was published jointly on June 9, 2017 (the Catalogue) by the Cyberspace Administration of China (CAC), the Ministry of Industry and Information Technology (MIIT), the Ministry of Public Security (MPS), and the Certification and Accreditation Administration (CNCA).

   ISSN 1538-3423

The Catalogue sets out the first batch of equipment and products that are covered, which includes very common items such as ''routers, switches, servers (rack-mounted), and the dedicated products for cybersecurity include integrated data backup, firewall (hardware), web application firewall, intrusion detection system, intrusion defense system, security isolation and information exchange products (gatekeepers), anti-spam mail products, network audit systems, network vulnerability scanning product, security data system, and website recovery products (hardware)''.

Such requirements, however, have raised legitimate concerns regarding (a) the extent to which information technology (hardware and software) products must be ''certified'' for security by the Chinese authorities before they can be sold in China; (b) whether the certification would require companies to provide the source code and other intellectual property relating to their products; and (c) whether these requirements would create market barriers to entry for products offered by non-Chinese companies.

Obligations Imposed on Network Operators

Whilst a slew of obligations is imposed on network operators, it is Article 28 of the CSL which raises the red flag. The provision compels network operators to provide ''technical support and assistance'' to state authorities. As with both the ATL and IL, this may potentially include the granting of state access to confidential data, in the course of the preservation of national security or investigations of crimes. The circumstances under which network operators may be compelled to provide technical assistance remains largely unclear.

On the other hand, one of the most important improvements to the overall legal protection of personal information is brought about by the CSL. This is because China does not have an overarching data protection law, and the CSL contains very detailed data protection obligations which bind network operators. In particular, network operators are required:

(i) to inform and obtain consent from the users when collecting their personal information;

(ii) to collect and use personal information in a legal and proper manner;

(iii) not to steal or use other illegal means to obtain personal information;

(iv) to gather and store personal information in accordance with the law, administrative regulations and their agreements with users;

(v) not disclose, tamper with or destroy collected personal information;

(vi) to allow users to request that their personal information is destroyed in circumstances where the network operator has violated the laws; and

(vii) ensure that all personal information obtained is kept confidential.

Additional Obligations Imposed on CII Operators

The CSL adopts a tiered regulatory approach, which means that all obligations imposed on CII Operators will be in addition to the obligations generally imposed on network operators. CII Operators are defined broadly as operators that provide services that, if lost or destroyed, would endanger China's national security and national welfare. The CSL elaborates CII as companies operating, or providing services, in the following sectors: public telecommunications and information services, power and energy, transportation, irrigation, finance, public services, and e-government.

Specific operational security obligations are set out in Articles 31 to 39 and are mandatory for CII Operators. The Chinese government also actively encourages all network operators to voluntarily comply with these additional obligations. Article 34, for instance, requires the establishment and maintenance of a higher level of data security measures. This includes, amongst others, obligations such as the setting up of specialised security management bodies, periodically conducting network security technical training and education, and conducting disaster recovery backups. However, the specific scope of these measures is contemplated to be set out by implementing regulations, which have not yet been released.

Penalties

Chapter VI of the CSL sets out in detail the penalties for contravention and non-compliance. Network operators and CII Operators in breach of their obligations may be liable for a fine of up to 100,000 RMB ($150,540) and directly responsible managers or personnel may also be personally liable for a fine of up to 100,000 RMB ($150,540). Article 67 of the CSL also criminalises the establishment of website or communications group for the commission of unlawful and criminal activities, allowing detention of up to 5 days and/or a fine of up to 15,000 RMB ($2,258), and where circumstances are deemed serious, a detention period of up to 15 days and/or a fine of up to 500,000 ($75,270).

Measures on Security Review of Network Products and Services CII Operators who are procuring services or network products that could potentially have an impact on China's national security will also have to undergo a separate procurement-related cybersecurity review as mandated under Article 35 of the CSL.

The Measures on Security Review of Network Products and Services (the Security Review Measures), which took effect from 1 June 2017, offering guidance on how a security review will be conducted has been published by the CAC. The Security Review Measures stipulate that all important network products and services which are procured for use in network systems that concern national security will be subject to a security review.

Draft Measures on Security Assessment of Outbound Transmission of Personal Information and Important Data Additionally, CII Operators are subject to a data localisation obligation to store personal information of Chinese citizens or other important data gathered as a result of operations conducted within Chinese territories. Article 37 of the CSL further restricts data export and stipulates that such data shall not be transferred out of China unless ''truly necessary'' for business needs, and subject to appropriate security assessment by the relevant state departments.

On May 19, 2017, the CAC released a further revised draft Measures on Security Assessment of Outbound Transmission of Personal Information and Important Data (Draft Outbound Transmission Measures).

In the Draft Outbound Transmission Measures, ''personal information'' is defined very broadly as ''all the information recorded in electronic form or otherwise, which can be used, solely or together with other information, to determine the identity of a natural person,

including but not limited to the name, date of birth, ID card number, personal biometric information, address and phone number of the natural person''. ''Outbound Transmission'' is defined as ''providing overseas institutions, organizations and individuals with the personal information and important data generated or collected by network operators during their operation within the territory of China''.

A two-tier assessment procedure is envisaged under the Draft Outbound Transmission Measures: self-assessment and regulatory assessment.

Article 12 of the Measures requires the network operators to conduct security assessment on the outbound transmission of data at least once a year. In case of any changes to the data receiver, any major changes to the purpose, scope, quantity and type of the outbound transmission of data, or any major security events of the data receiver or the outbound transmission of data, another security
assessment shall be conducted without delay.

The following issues should be considered when conducting such security assessment:

(i) necessity of the outbound transmission of data;

(ii) personal information involved, including the quantity, scope, type and sensitivity of personal information, as well as whether the owner of personal information agrees to transmit his personal information abroad;

(iii) important data involved, including the quantity, scope, type and sensitivity of important data;

(iv) security protection measures and capability of the data receiver, as well as the network security environment of the country or region where the date receiver is located;

(v) risks of leakage, damage, tampering and abuse of the data after being transmitted abroad and further transferred;

(vi) risks to national security, social and public interests, and personal legitimate interests arising from the outbound transmission of data and gathering the outbound data; and

(vii) other important matters to be assessed.

The Draft Outbound Transmission Measures provide that a network operator shall report to its industrial authority or regulator to arrange for security assessment to determine whether the data shall be allowed to transmitted abroad in the following circumstances:

(i) the data to be transmitted abroad contains or contains in aggregate more than 500,000 users' personal information;

(ii) the quantity of the data to be transmitted abroad is more than 1,000 gigabytes;

(iii) the data to be transmitted abroad contains data relating to nuclear facilities, chemical biology, defense industry, population and health, as well as the data of large-scale project activities, marine environment and sensitive geographic information etc.;

(iv) the data to be transmitted abroad contains system vulnerabilities, security protection and other network security information of critical information regarding to the infrastructure;

(v) an infrastructure operator of the critical information provides personal information and important data abroad; or

(vi) other data which may affect national security, and social and public interests, and are necessary for assessment as determined by the industrial authority or regulator.

Under the following three circumstances, the data shall not be transmitted abroad:

(i) the outbound transmission of personal information fails to be approved by the owner of personal information, or may jeopardise personal interests;

(ii) the outbound transmission of data causes security risks to the nation's politics, economy, technology and national defense, which may affect national security and jeopardise social and public interests; or

(iii) other data which are prohibited from being transmitted abroad as determined by relevant authorities.

While the Draft Outbound Transmission Measures are helpful to clarify that outbound transmission of data is allowed if such data transmission is approved by the user, and if it is necessary and carries no harm to the national security and social and public interests, the fact that the ambiguous terms ''other data which may affect national security, and social and public interests'' and ″ other data which are prohibited from being transmitted abroad as determined by relevant authorities'' contained in these measures still give rise to unpredictability and business uncertainty.

Critiques of the Laws

Generally, the laws grant extensive regulatory powers to the Chinese government and its organs. The sheer scope of the law, coupled with the vague and ambiguous drafting, renders compliance incredibly difficult. The broad drafting of the laws has been raised as a key concern for business risk and uncertainty, particularly for foreign multinational companies operating in China.

Firstly, the invasive measures and vague wording of the laws sparks fear that the Chinese authorities may compel foreign multinational companies to hand over confidential data or open back doors within their product offerings in the name of ''national security'' or ''counter terrorism''. It is submitted that the law goes beyond what is necessary to secure the internet and further tightens China's already heavily regulated cyber space.

Each of the laws discussed above contains provisions allowing state authorities to compel specified entities to allow state access to confidential data and provide technical assistance (presumably such as decryption) to state authorities, subjecting companies to close monitoring and surveillance. While the laws will undoubtedly strengthen cybersecurity, the risk of the laws being used as a tool for achieving objectives that are merely tangential to cybersecurity remains real.

Secondly, the CSL and its implementing regulations present an indirect form of protectionism in favor of local Chinese companies. The restriction on network products and services entail high compliance cost requiring foreign companies and manufactures seeking to provide such products and services to modify existing offerings to comply with the government issued standards. There is also significant risk that foreign products or services that are uncertified or unable to meet the issued standards could be completely cut off from the Chinese market, in favor of local companies.

Similarly, the data-localisation and data export obligation effectively forces foreign companies to store data in China, which can result in a duplication of services

   ISSN 1538-3423

and high operational cost. The importance of data in this global economy is indubitably clear. Global companies are increasingly using such data analytics to understand customers' preferences, streamline internal business processes and increase efficiency. Restrictive data policies will make data analytics more expensive, putting foreign companies at a disadvantage as compared to local companies, since these companies will no longer be able to conduct data analytics cost-effectively on a global basis. In order to comply, foreign companies have the option of contracting with local cloud service providers in China or build their own data centers, either of which involves high outlays. This requirement benefits largely local Chinese companies offering cloud and storage services such as Alibaba Group Holding Ltd.'s AliYun, but is particularly onerous for small-medium sized enterprises that do not possess the deep pockets to comply.

Thirdly, from a human rights perspective, elements of the laws are said to further solidify the government's control over the Internet, which is already subject to the country's Great Firewall. Elements such as the criminalisation of the use of the Internet for unlawful or criminal activities, and the obligation on operators to prevent the dissemination of ''terrorist'' or ''extremist'' content are likely to further restrict online freedom in China. Noting that the laws also provide for personal liabilities to be imposed on directly responsible managers or personnel in a wide array of circumstances, the Chinese government would effectively have another tool to suppress and crack down on dissidents.

Compliance With These Laws Moving forward, foreign companies will have to conduct a cost and benefit analysis to decide whether it is worthwhile to continue operating in, or expand operations into, China. Notwithstanding the seemingly insurmountable task of compliance, the Chinese market and its promise for growth is far too huge to be ignored.

At the outset, it would be prudent for foreign companies operating in China to assess whether they are subject to the relevant laws and ancillary regulations, and determine the extent of compliance required. This will require foreign companies to consider whether they fall under an enforcement priority. As a rule of the thumb, given the broad drafting and vague definitions employed in the laws, companies in the technology-related sectors should take the stance that it will more likely than not be subject to the obligations.

Preparing for compliance will require a review of current business practices and internal processes, including data localisation, and a security review. Foreign companies already operating in China should have been accustomed to restrictive internet controls given the requirements imposed under the Golden Shield Project (known as China's Great Firewall). These companies should also take the opportunity to assess potential gaps in their existing cybersecurity policies and procedures. This may include taking further measures for data categorisation and segregation, server localisation, review of its existing standard terms and conditions of service offerings, and putting in place appropriate internal cybersecurity policies amongst others. The compliance route will inevitably involve foreign companies incurring significant cost outlays, particularly if the company requires major overhaul to its practices and processes.

Large multinational companies are already moving to comply with the laws with Apple announcing its plans to build its first Chinese data center in partnership with a local Chinese data management company, while Amazon.com Inc. and Microsoft Corp. already have data centers in China. Other companies such as Airbnb Inc. and South Korean company, AmorePacific Corp., are either shifting data collected from its Chinese operations to local Chinese servers, or relocating its e-commerce systems to China.

Foreign multinational companies should also be minded to recognise that the Chinese legal systems are fundamentally different from the Anglo-Saxon legal system familiar to most in the Western world. A plain reading of the relevant laws and implementing regulations will not be sufficient to understand or determine the precise ambit of the obligations. Rather, the key to compliance is to understand the government's motivations and regulatory approach. This will require constant strategic engagement with the relevant state authorities to help understand and mitigate the impact of the laws.

Conclusion

Short of the detailed implementing regulations that have yet been fully released by the relevant state authorities, the true overall impact of the laws remains to be seen. Guidelines and implementing regulations will continue to be rolled out as state authorities look towards facilitating the implementation of cybersecurity measures. While the state of cybersecurity regulation in China remains in a flux, one thing that is certain is that the Chinese government is succeeding in its desire to exercise more control and oversight over the cyberspace.

By Benjamin Cheong and Terrance Tong

To contact the editor responsible for this story: Donald Aplin at daplin@bna.com