Hogan Lovells

The grand “finale” of China’s Encryption Law

November 2019

The grand "finale" of China's Encryption Law

Introduction and overview

After a wait of more than two years since the first draft, the long-awaited *People's Republic of China Encryption Law* (the "**Encryption Law**") was finally promulgated by the People's Republic of China ("**China**" or "**PRC**") National People's Congress ("**NPC**") Standing Committee on 26 October 2019, and will take effect on 1 January 2020. The State Commercial Cryptography Administration ("**OSCCA**") had issued two prior drafts for public comment the first draft on 13 April 2017 (the "**2017 Draft**"), followed by the second draft on 5 July 2019 (the "**2019 Draft**").

The final text of the Encryption Law seems to have gone some way to taking on board some of the bigger concerns expressed by the business community in relation to the 2017 Draft: (i) whether mass-consumer products whose main function is not encryption (for example, anti-virus software) may be imported and used in China without restriction; and (ii) the potential for abuse of the wide and intrusive powers (including power to require decryption of traffic or supply of decryption keys) given to the Chinese regulators in relation to the administration of encryption products and services. However, some of the other concerns remain, for instance, uncertainty over whether imported encryption products are still off limits to domestic entities and individuals, and whether imported encryption products are still subject to internal use restrictions when imported by foreign invested enterprises ("**FIEs**"), meaning overseas encryption technology providers remain shut out of the Chinese domestic cryptography products market; and whether critical information infrastructure ("**CII**") operators, once designated as such, can continue using existing imported encryption products and services.

Overall, the Encryption Law follows the same format as the 2017 Draft and the 2019 Draft by setting out a generic set of principles and basic rules on the regulation of the three types of encryption products, namely:

- core encryption products, technologies and services ("**Core Encryption**");
- general encryption products, technologies and services ("**General Encryption**"); and
- commercial encryption products, technologies and services ("**Commercial Encryption**").

Please see our earlier briefing on the 2017 Draft *here* (the "**Earlier Note**").

Also in common with the approach in the 2017 Draft and the 2019 Draft, Core Encryption and General Encryption Products are still being used as an umbrella term for products designed to protect state secrets (and are deemed to be state secrets themselves in the Encryption Law), but for the most part are not particularly relevant to multinational companies. As such, this briefing will focus on the regulation of Commercial Encryption products.

Highlights of the Encryption Law

Import permit and export control

As was the case under the 2017 Draft, the import and export of Commercial Encryption products will remain subject to government approval. Article 28 of the Encryption Law provides that:

- Import permit: applies to Commercial Encryption products that may affect national security, the public interest and that have encryption-based protective functions; this suggests that no import permit will be required for imported Commercial Encryption products that do not fall under one of these categories and that China may issue a new Import Catalogue listing out which classes or

specific imported products require an import permit;
- Export controls: apply to Commercial Encryption products that may affect national security, the public interest or are used to fulfil China's international obligations.

Again, the Ministry of Commerce (the "**MOFCOM**") together with the OSCCA and the GAC will issue catalogues of Commercial Encryption products that are subject to the above import permit and export controls, respectively.

As set out in our Earlier Note, MOFCOM has, for the first time, been brought into the encryption field and appears to play a leading position in the administration of the import and export of Commercial Encryption products. It is unclear to us as to what extent MOFCOM will continue to play this role going forward, although it is a natural extension of its duties as the cross-border commerce regulator.

As was the case under the 2017 Draft and the 2019 Draft, the Encryption Law still does not address the point of whether imported Commercial Encryption products will still be limited to internal use, i.e., for internal communications with the parent company or other offshore affiliates (see further analysis below).

"Core function" test "fortified"?

The current *Catalogue for the Administration of the Importation of Encryption Products and Equipment Incorporating Encryption Technologies* (the "**Import Catalogue**") was issued by the OSCCA and the General Administration of Customs (the "**GAC**") on 31 December 2013. It provides for 9 categories of encryption products[1] that are subject to OSCCA approval when imported into China. The Import Catalogue is non-exhaustive. As a matter of current practice[2], even if a product is not included in the Import Catalogue, as long as the product is caught under the general "core function" test (meaning that such product has encryption as its main function), the importation of hardware products meeting the test must be approved by OSCCA prior to importation (which essentially makes having a list of specified products redundant).

The above-mentioned "core function" test seems to have become the prevailing view after the OSCCA began to realize that the current import restrictions were, if strictly followed, basically unworkable. However, there has not been any corresponding repeal of, or amendments to, current laws and regulations, so we consider the "core function" test to only be an unofficial administrative policy within OSCCA as opposed to black letter law.

Nowadays, virtually all electronic communication products and software products (mobile telephones, laptops, email systems) use encryption technology to a greater or lesser extent in order to protect their source code, or for other security and privacy-related reasons.

---

[1] (i) electrostatic photosensitive multi-functional integrated encrypted fax machines (which can be connected to automatic data processing equipment or networks);
(ii) other multi-functional integrated encrypted fax machines (with one or more of printing and copying functions);
(iii) other encrypted fax machines (which can be connected to automatic data processing equipment or networks);
(iv) cordless encrypted telephones;
(v) other encrypted telephones;
(vi) optical communication encrypted routers;
(vii) non-optical communication encrypted Ethernet switches;
(viii) non-optical communication encrypted routers; and
(ix) encryption machines and encryption cards (not including digital TV smart cards, Bluetooth modules, or dongles used for the protection of intellectual property rights).

[2] Based on the responses consistently received to our no-names telephone inquiries with the central-level OSCCA, and its Shanghai, Beijing, Guangdong, and Jiangsu counterparts.

The business community therefore needs urgent clarification on this point, given how widely encryption technologies are used for securing electronic products in daily use.

The Encryption Law takes one further step towards trying to address these concerns. For the first time, Article 28 of the Encryption Law clarifies and confirms, in legislation with the status of a law, that Commercial Encryption that is used on mass-market consumer products is exempted from the import permit and export control requirements. With only one general sentence to rely on, it only provides very high-level conceptual guidance, and leaves practical questions, such as the definition or scope of "mass-market consumer products" and whether this is, in fact, a "core function" test by any other name unanswered.

Link to the cyber security regime

The Encryption Law has two articles (Article 26 and Article 27) which apparently were drafted with the existing cyber security regime under the *PRC Cyber Security Law*, effective 1 June 2017 ("**Cyber Security Law**") in mind:

- Commercial Encryption products that involve national security, the national economy and people's livelihoods or the public interest shall be listed in the key network equipment and specialized cyber security products catalogue, and must pass testing and certification (which the Encryption Law helpfully confirms is, in fact, the same testing and certification required under the Cyber Security Law, so as to avoid repetitive testing and certification);
- Those engaging in the provision of Commercial Encryption services using any key network equipment and specialized cyber security products must pass certification conducted by Commercial Encryption certification institutions;
- Where required under applicable PRC laws to use Commercial Encryption products to protect critical information infrastructure ("**CII**"), CII operators must carry out a security assessment on the use of such Commercial Encryption products either through self-assessment or through Commercial Encryption testing institutions. Such security assessment shall be in sync with those security assessments required for CII and for classification-based protection of cyber security systems under the Cyber Security Law, so as to avoid repetitive testing and certification;
- Where CII operators wish to purchase Commercial Encryption products which may potentially have an impact on national security, such purchases shall be subject to a national security review by the Cyberspace Administration of China ("**CAC**"), the OSCCA and other relevant authorities as provided under the Cyber Security Law. The reference to products impacting on national security is a reference to the current *Network Products and Services Security Review Measures* effective 1 June 2017, which are expected to be replaced when the draft *Cybersecurity Review Measures* (please see our earlier briefing *here*) are finally issued. The latter set out general guidance on the review process.

The requirements in relation to key network equipment and specialized cyber security products passing security certification or security testing originate from Article 23 of the Cyber Security Law. On the same day as the Cyber Security Law took effect, the CAC, the Ministry of Industry and Information Technology ("**MIIT**"), the Ministry of Public Security ("**MPS**"), and the Certification and Accreditation Administration jointly issued a circular reiterating such certification/testing requirements, together with a *Key Network Equipment and Specialized Cyber Security*

Products (Batch No. 1) Catalogue ("**Batch No. 1 Catalogue**"). Commercial Encryption products were not included in the Batch No. 1 Catalogue, but when the Encryption Law becomes effective, Commercial Encryption products involving national security, the national economy and people's livelihoods or the public interest shall be deemed to be Key Network Equipment and Specialized Cyber Security Products by operation of law.

It is still not clear under the Encryption Law as to when or under what circumstances Commercial Encryption must be used by CIIs. Given the sensitivity of the networks designated as CIIs[3], it appears that all CIIs may be required to be equipped with Commercial Encryption products. Under the draft *Cybersecurity Classified Protection Regulations* issued by the MPS in June 2018 for public comment ("**Draft Classified Protection Regulations**") (see our earlier briefing *here*), encryption-based protection must be established for networks deemed to constitute Level 3 or above. The Draft Classified Protection Regulations create a multi-level protection scheme for networks based on the potential degree of harm to national security, public order, the public interest and the lawful rights and interests of the PRC if the system were breached or disrupted. Based on this, any destruction of a network from Level 3 upwards may jeopardize national security. So based on the definition of CII, the networks designated as CIIs are most likely to be deemed to constitute Level 3 or above networks, triggering the requirement to use Commercial Encryption. Presumably CIIs will still use General Encryption or Core Encryption products for networks involving state secrets.

Removal of compulsory duty to provide decryption support to the Chinese government

Following the approach in the 2019 Draft, the Encryption Law has removed the compulsory duty on telecommunications operators and Internet services providers to cooperate with the Chinese authorities in relation to investigations by providing decryption technical support, which, as set out in our Earlier Note, was the most worrying aspect of the 2017 Draft. The Encryption Law further eliminates OSCCA's sweeping and intrusive investigatory powers by deleting the entire supervision and administration chapter of the 2017 Draft. Against the backdrop of trade tensions with the United States, the Encryption Law could be seen as an attempt to seek a balance between the need to safeguard national security and the protection of the interests of business participants in China. Please note that notwithstanding this welcome revision, as network operators are still generally required to cooperate with supervisory and investigatory bodies under Article 49 of the Cyber Security Law, the extent of cooperation which will be called upon by the Chinese government in practice still remains to be seen. The Chinese government still has tremendous leverage over telecommunications and internet service providers given the fact that they rely on licences issued by MIIT for their continued existence.

The Encryption Law purports to establish an administration regime combining daily supervision with random inspections, with the results of such supervision and random inspections linked to the social credit system (see our earlier briefing *here*).

[3] CII is stated in the Cyber Security Law to be critical infrastructure relating to critical industries, being public communications and information services, energy, transportation, water conservancy, finance, public services, e-government affairs and other significant industries and sectors, as well as any other infrastructure that may jeopardise national security, the national economy, people's livelihoods or the public interest were it to be destroyed, experience a loss of functionality or data leakage.

Promoting the standards of Commercial Encryption

Given that Commercial Encryption products are highly technical in nature, the Encryption Law emphasizes the importance of establishing national and industry standards as well as promoting the internationalization of the standards in the Commercial Encryption field.

Based on the information on the official website of OSCCA, there are already approximately 90 standards focusing on encryption products and technologies. The latest standard was issued in 2016. With the issuance of the Encryption Law, we anticipate that there will be more standards issued in this area. The question is whether the very close connection between encryption and China's national security needs mean that it remains to be seen whether other countries will be willing to incorporate domestic standards into international standards, and make international standards interoperable with them.

What questions remains unanswered?

Will restrictions on the sale of imported Commercial Encryption be lifted?

Prior to the promulgation of the Encryption Law, only domestic Commercial Encryption products were allowed to be sold and used in China, and then subject to such domestic Commercial Encryption products having obtained a type certificate issued by the OSCCA. The law as it currently stands in relation to imported Commercial Encryption products provides that only FIEs, foreign organizations (such as representative offices of overseas companies) and foreign nationals may use imported Commercial Encryption products. While the previous requirement to get approval for the use of Commercial Encryption products has gone they must still obtain an import permit from the OSCCA on a case-by-case basis before they may import and use such imported Commercial Encryption products. For FIEs, there are two additional requirements: there must be a genuine business need to use such products, and such products can only be used for the purpose of internal communications with foreign parties, e.g. offshore affiliates of the importer ("**Internal Use Restriction**").

Article 21 of the Encryption Law provides that all Commercial Encryption operators including domestic companies and FIEs carrying out R&D activities, manufacture, sales, services, import and export shall be treated equally in accordance with the law. Furthermore, Article 21 goes on to say that the Commercial Encryption technology cooperation during foreign investment shall be encouraged. In a silent nod to similar provisions on forced intellectual property transfers in return for market access in the *Foreign Investment Law* which takes effect on the same date as the Encryption Law (see our two separate notes: *The foreign investment law: A new chapter opens for foreign direct investment in China* and *The Foreign Investment Law gets wings: draft implementation regulations released for public consultation*), no forced Commercial Encryption-related technological transfer may be imposed by administrative organs and their officers.

Due to the general nature of the provision, it is still unclear to us whether (i) the "equal treatment" principle will mean both domestic capital and foreign entities and individuals will be permitted to import foreign-made Commercial Encryption products or services; and (ii) whether the Internal Use Restriction will be lifted, meaning imported Commercial Encryption products and services may be sold to third parties. We made telephone enquiries with the OSCCA but the officials we spoke to were unwilling to provide any interpretation of Article 21.

Effect of designation of CII on existing Import Permit

The Encryption Law is still silent on whether any FIE in China that is currently using a foreign manufactured Commercial Encryption products (with an import permit issued by the OSCCA) will be allowed to continue to use it after it has been designated a CII operator or whether a new import permit will be required.

Conclusion

The Encryption Law clearly represents a step in the right direction in terms of putting in place a comprehensive law in the encryption field. It appears to show that China is listening to some of the concerns expressed in comments on the prior drafts in that it no longer requires telecommunication operators and Internet content providers to provide the Chinese government with decryption support. However, the Encryption Law still has a strongly political flavour, as it continues to emphasize that the leadership of the Chinese Communist Party over encryption work must be upheld.

Undoubtedly, this version of the Encryption Law has, to some extent, been influenced by trade tensions and ongoing trade discussions. However this sensitive area, which China links so closely to state security and secrecy, is not one where we think China will be willing to compromise on or liberalise readily. Even if the parameters of the exemption for mass market consumer products in Article 28 are far from clear, this is a step forward in terms of defining which products are regulated, thereby potentially saving costs being incurred by FIEs in China in trying to understand which products do or do not require an import permit. The full meaning of the provision on equal treatment in Article 21 of the Encryption Law may only be revealed in subsequent implementing legislation and practice, but it can be seen as the best hope for opening up of the Commercial Encryption area which has remained closed to foreign investment to date.

As mentioned in the official news report regarding the promulgation of the Encryption Law on the next day of its promulgation, implementing rules are expected to be issued in the coming months to supplement the general concepts under the Encryption Law and to bring rules issued earlier in line with the Encryption Law. Commercial Encryption businesses need to keep a close eye on legislative developments on this front, as the Encryption Law remains very much a high-level framework document, and details of how the Encryption Law will work, as well as clarification on the questions it fails to answer, is only likely to be found in the forthcoming implementing rules, which may explain why OSCCA is unwilling to provide interpretations of certain key provisions at this point in time.

Contacts

Hong Kong

Andrew McGinty
Partner, Hong Kong
andrew.mcginty@hoganlovells.com

Beijing

Roy Zou
Partner, Beijing
roy.zou@hoganlovells.com

Sherry Gong
Partner, Beijing
sherry.gong@hoganlovells.com

Shanghai

Maggie Shen
Senior Associate, Shanghai
maggie.shen@hoganlovells.com

Jia Zhan
Associate, Shanghai
jia.zhan@hoganlovells.com

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest*
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta*
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Riyadh*
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ*
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar*
Warsaw
Washington, D.C.
Zagreb*

*Our associated offices
Legal Services Center: Berlin

www.hoganlovells.com