Decrypting China's first crack at a Cryptography Law

May 2017

Hogan Lovells

Decrypting China's first crack at a Cryptography Law

On 13 April 2017, the Office of the State Commercial Cryptography Administration ("**OSCCA**") published the *People's Republic of China Cryptography Law* (draft for seeking comments) ("**Draft Cryptography Law**") on its website. The Draft Cryptography Law marks a clear stepping up of the regulatory emphasis in the area of encryption and will, once passed, serve as the most authoritative source of law in the area of cryptography in China.

Prior to the newly released Draft Cryptography Law, the main PRC rules governing encryption equipment and technology in the People's Republic of China ("**China**" or the "**PRC**") were the *Commercial Encryption Administration Regulations* (the "**Commercial Encryption Regulations**"), which are now 18 years old, and four major relevant sets of rules passed by OSCCA between 2005 and 2007 governing commercial encryption manufacturing, sales, use and scientific development, respectively.

Since then, the need for further legislation has been recognized, and this year the State Council listed the promulgation of a Cryptography Law in its 2017 legislative work plan as one of the "items with an immediate and urgent need for comprehensively deepening reform". In other words, a high strategic priority.

The Draft Cryptography Law defines "cryptography" as the items and technologies which are used to encrypt or certify the data and other information through the application of certain algorithms. The scope of the law is broad, covering all aspects of the development and supply chain for cryptographic products and services, from scientific research, manufacturing, use in business operations, importation and export, testing, certification, supervision and management and other such like activities.

OSCCA and its respective local branches are tasked with administering all aspects of cryptography related work under a system of unified leadership, which the Draft Cryptography Law makes a specific point of stating is ultimately vested with the Chinese Communist Party, underscoring the somewhat heavy political and state security overtones of this area.

Classifications of cryptography

The Draft Cryptography Law categorizes cryptography products and services into three types:

- core cryptography products and services ("**Core Cryptography**")
- general cryptography products and services ("**General Cryptography**"), and
- commercial cryptography products and services ("**Commercial Cryptography**").

Each category of cryptography products and services is subject to different use restrictions and regulation, with some of the key differences discussed below.

State secrets

The former two types can be used to protect state secrets, while the latter can only be used to protect information not deemed to constitute state secrets. The restriction on commercial encryption devices being used to protect state encryption technologies secrets is not a new concept. Presumably, the concern is that commercial encryption technology is less reliable and decryption keys may be more readily available. Article 2 of the Commercial Encryption Regulations expressly defines commercial encryption as technologies not used for protection of state secrets.

Import and export

Core Cryptography and General Cryptography cannot be exported.

Commercial Cryptography may be imported or exported, subject to having obtained government approvals. Under the current Commercial Encryption Regulations, such approvals have to be obtained from OSCCA, with the importation of foreign Commercial Cryptography further regulated by the *Catalogue for the Administration of the*

Importation of Encryption Products and Equipment Incorporating Encryption Technology ("**Import Catalogue**") issued by OSCCA and the General Administration of Customs (the "**GAC**"). The latest version of the Import Catalogue is dated 31 December 2013 and lists the following 9 categories of products and equipment as being regulated under it: (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 (can be connected to automatic data processing equipment or network); (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).

The Draft Cryptography Law provides a slightly different regime, bringing into play one more government authority, i.e. the Ministry of Commerce ("**MOFCOM**"), whereby both the export and importation of Commercial Cryptography will be subject to a permit from MOFCOM and OSCCA. MOFCOM, together with OSCCA and GAC will publish a list of Commercial Cryptography products and services which are subject to restrictions in relation to imports and exports.

Currently, imported Commercial Cryptography products cannot be sold in the China market and can only be imported for restricted use by foreigners, representative offices, and foreign invested enterprises (the "**FIEs**") for internal communications with their parent companies with an import permit and approval from OSCCA. The Draft Cryptography Law does not address this point. Presumably, the restrictions on sale found in existing legislation will remain in place or will otherwise be carried forward.

Sale and usage of domestic Commercial Cryptography

Article 11 of the Draft Cryptography Law sets out the rules with respect to domestic sales and use of Commercial Cryptography, such that the sale of and use of Commercial Cryptography products as well as the provision of Commercial Cryptography services by an entity in China (e.g. repairs) will require a permit from OSCCA. OSCCA will formulate and publish a catalogue of (domestic) Commercial Cryptography products and services. The *Catalogue of (Domestic) Commercial Encryption Products* ("**Domestic Products Catalogue**") previously issued by the OSCCA dated 22 March 2017 contains 1817 products approved for sale in the Chinese market. It is unclear, given how recent in origin this is, whether the plan is to replace this with a new catalogue. Chinese citizens and legal persons are currently allowed to use Commercial Cryptography products as long as such use is not for protecting information relating to state secrets.

What is very clear from the above two catalogues is that the distinction between imported and domestically produced encryption products is likely to remain under the Draft Cryptography Law, with no relaxation on the heavy restrictions on imported products in sight.

The link to the Cyber Security Law and Critical Information Infrastructure operators

The *People's Republic of China Cyber Security Law* which was adopted on 7 November 2016 and takes effect on 1 June 2017 (the "**Cyber Security Law**") (see our client notes here) designates certain systems as "Critical Information Infrastructure" ("**CII**"), which are subject to a number of specific requirements under the Cyber Security Law, notably the obligation under Article 35 to submit purchases of network products and services which may potentially have an impact on national security to a national security review before purchase by a CII.

The ultimate definition of what constitutes a CII operator will be issued by the State Council, but 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.

The *Network Products and Services Security Review Measures* which take effect on the same date as the Cyber Security Law (the "**Network Products Review Measures**") state that "networks which relate to national security and important network products and services purchased for information systems" are subject to a network security review, which leaves it open as to what are "networks which relate to national security" and, more worryingly, "important network products and services".

Cryptography will undoubtedly play an important role in security systems for CIIs. Article 12 and Article 18 of the Draft Cryptography Law relate directly to the use of cryptography by CIIs. They state that CIIs must use cryptography to protect their systems and must plan, build and operate cryptology protection systems in accordance with laws, regulations and mandatory provisions in standards relating to cryptography in tandem. Article 18 goes on to say that the state will use a tiered review system to categorize the security status of cryptography products used in CIIs, and where they impact, or are likely to impact state security, and will carry out security reviews of cryptography products and services and systems based on state review requirements. This is clearly a reference to the Network Product Review Measures.

In short, it seems almost a given that even domestically manufactured cryptography products are going to be subject to the security review process under the Network Product Review Measures where these is a potential impact on national security (or even where classified as "important network products"), and thus it seems highly unlikely that any foreign-made Commercial Cryptography product will be permitted to be used in the systems of any CII, as they are currently banned from sale in China in any event. What remains to be seen is whether any FIE in China that is currently using a foreign manufactured Commercial Cryptology product (with an import permit and OSCCA approval to use) will be allowed to continue to use it after it has been designated a CII. Instinctively the answer would appear to be "no", as the Chinese government has remained very wary and mistrusting of foreign cryptography products, particularly as it has no access to the source code and decryption keys and the CII designation also provides a link to national security concerns.

Link to the "secure and controllable" concept

The Draft Cryptography Law has come out amongst a backdrop of various efforts by China to tighten the regulation of overseas-originated technology on several fronts with the stated objective of making technology "secure and controllable". The term "secure and controllable" has found its way into the *People's Republic of China National Security Law* ("**National Security Law** ") adopted on 1 July 2015, which pre-dated the Cyber Security Law. Already the rolling out of the concept has had a very significant impact on FIEs in sectors providing equipment and services to the banking industry in particular, which previously were not subject to policy restrictions. The national security review procedures under the Network Product Review Measures, with their open-ended and ambiguous formulation "important network products and services purchased for information systems" may become the legal basis for the Chinese government to wade into the overseas-sourced technology and equipment supply sectors in an

even more intrusive manner. The Draft Cryptography Law provides no evidence to the contrary and, in fact, points clearly in that direction.

Compulsory duty to cooperate with the Chinese authorities on investigations

Article 20 provides that Chinese authorities including the People's Procuratorate, the Ministry of Public Security (the "**MPS**") and Ministry of National Security (the "**MNS**") are authorised to require telecommunications operators and Internet services providers[1] to cooperate and provide decryption technical support where required due to national security concerns or investigations into criminal offences, and the latter must keep such cooperation confidential. This provision adds to the already fulsome set of powers the Chinese government authorities have to investigate information transmitted through telecom services and the Internet.[2] The respective industry regulators may impose a monetary fine (the amount is not stated) on the operators or providers and the persons directly in charge and other directly responsible persons for failure to cooperate or provide decryption technological support or for "disclosing the relevant circumstances"; in serious cases, the MPS or the MNS may impose criminal detention ranging from five to fifteen days on persons directly in charge and other directly responsible persons. Unlike some of their overseas counterparts, telecoms operators and Internet services providers in China do not have the right or option of challenging or refusing to cooperate in China. Article 27 seems to go even further, providing that relevant organisations and individuals must cooperate when the cryptography administrative departments are carrying out their regulatory and administrative duties.

[1] This is thought to be much wider a concept than the Internet Service Provider concept, which in Chinese translates as "Internet access provider".

[2] See for example the content controls set out in Article 57 et seq. of the *People's Republic of China Telecommunications Regulations* passed by the PRC State Council with effect from 25 Septermber 2000, for example.

Clarifying and strengthening of OSCCA's surveillance

The Draft Cryptography Law grants the OSCCA sweeping and intrusive investigatory powers. Under Article 29, the OSCCA may:

- conduct on-site investigations in places where cryptology products or services are manufactured, sold, imported or exported, examined, certified or used
- make enquiries of the main persons in charge or other relevant persons in enterprises or institutions manufacturing, selling, importing and exporting, examining, certifying and utilizing encryption products or services
- access and copy relevant contracts, bills of exchange, accounting books and other materials
- seal up or confiscate unlawful facilities for manufacturing, operating, importing and exporting, examining, certifying or using cryptography products or services, and
- seal up places used for the unlawful manufacturing, selling, importing and exporting, examining, certifying and utilizing of cryptography products or services.

In short, OSCCA can do basically whatever it deems necessary for the purposes of enforcing its rights as the regulatory authority in charge of cryptography (including investigating FIEs who have already obtained an import permit and OSCCA approval to use), again pointing to how China sees cryptography as essentially an extension of state secrecy and national security administration. The only concession to abuse of powers and so forth by OSCCA officials is set out in Article 39 where it suggests that they will be subject to administrative disciplinary measures in accordance with law.

Conclusion

The Draft Cryptography Law is the first comprehensive law in the cryptography field. It is heavily politicized, with over half of the forty three articles relating to government supervision and liability for breach; many of the provisions are high-level 'government speak' or administrative and inward-looking in nature. Perhaps the most worrying, albeit unsurprising aspect of the Draft Cryptography Law is the way it overtly leaves telecom operators and Internet content providers (and arguably anyone else in China) with little choice when government authorities demand decryption support. Effectively this allows government to drive a coach and horses through the regime for protecting data privacy in the name of investigating national security concerns or alleged crimes. The potential for abuse is obvious: if someone wants to say chase down a certain individual, all they have to do is convince someone in the MPS or MNS to use their powers to find that person's data trail and the relevant telecoms or internet service providers have to decrypt the traffic on request (or possibly supply the decryption key to the Chinese authorities to allow them to decrypt future traffic). This means that the Chinese state security organs essentially have access to decrypted private correspondence on demand.

For foreign cryptography technology providers, it basically means they are still shut out of Chinese cryptography products market for the simple reason that they cannot sell into China except to FIEs and other limited foreign organs with an import permit and OSCCA approval to use, and even if they were to get a permit to manufacture or sell locally,[3] they may find the concept of having to allow their customers to provide the Chinese government with decryption keys on demand difficult to swallow.

Contacts

Jun Wei
Partner, Beijing
+86 10 6582 9501
jun.wei@hoganlovells.com

Roy Zou
Partner, Beijing
+86 10 6582 9596
roy.zou@hoganlovells.com

Liang Xu
Partner, Beijing
+86 10 6582 9577
liang.xu@hoganlovells.com

Philip Cheng
Partner, Shanghai
+86 21 6122 3816
philip.cheng@hoganlovells.com

Andrew McGinty
Partner, Shanghai
+86 21 6122 3866
andrew.mcginty@hoganlovells.com

Mark Parsons
Partner, Hong Kong
+852 2840 5033
mark.parsons@hoganlovells.com

3 Research suggests that there are significant trade barriers to setting up FIE in China selling Commercial Cryptography products, even those produced locally.

Alicante
Amsterdam
Baltimore
Beijing
Brussels
Budapest
Caracas
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
Rio de Janeiro
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar
Warsaw
Washington, D.C.
Zagreb

Our offices
Associated offices

www.hoganlovells.com

"Hogan Lovells" or the "firm" is an international legal practice that includes Hogan Lovells International LLP, Hogan Lovells US LLP and their affiliated businesses.

The word "partner" is used to describe a partner or member of Hogan Lovells International LLP, Hogan Lovells US LLP or any of their affiliated entities or any employee or consultant with equivalent standing. Certain individuals, who are designated as partners, but who are not members of Hogan Lovells International LLP, do not hold qualifications equivalent to members.

For more information about Hogan Lovells, the partners and their qualifications, see www.hoganlovells.com.

Where case studies are included, results achieved do not guarantee similar outcomes for other clients. Attorney advertising. Images of people may feature current or former lawyers and employees at Hogan Lovells or models not connected with the firm.

©Hogan Lovells 2017. All rights reserved.