COVINGTON

China Enacts Encryption Law

October 31, 2019

Privacy

On October 26, 2019, China enacted a landmark Encryption Law, which will take effect on January 1, 2020. The Encryption Law significantly reshapes the regulatory landscape for commercial encryption, including foreign-made commercial encryption products, but leaves many questions to be answered in future implementing regulations.

Prior to the adoption of the final version of the Encryption Law, (an unofficial translation is available here) two previous drafts were released for public comments in April 2017 and July 2019 (see Covington's alert summarizing the previous versions here and here). The final version of the Encryption Law replaces almost two decades of regulations and largely tracks the regulatory framework proposed in the 2019 draft. The Encryption Law also introduces a few new changes, including calling for non-discriminatory treatment of multinationals engaging in the "research, manufacturing, distribution, services, and import/export" of commercial encryption products and prohibiting forced transfer of encryption technologies. Highlights of the final version of the Encryption Law as enacted are explained below.

1. Definition and Classification of Encryption

Consistent with prior drafts, the Encryption Law defines "encryption" as "technologies, products, or services applying specific transformations to information to effect encryption protection or security authentication" (Article 2).

The Encryption Law classifies encryption into three categories: core encryption, ordinary encryption, and commercial encryption (Article 6). "Core" encryption and "ordinary" encryption are used for the protection of information constituting "state secrets,"[1] while commercial encryption is used to protect information that is not considered state secrets. Furthermore, core encryption and ordinary encryption, but not commercial encryption, are themselves considered state secrets, and will be subject to strict regulation by the State Cryptography Administration (SCA) (Article 7). The Encryption Law does not define "core" or "ordinary" encryption.

[1] Under Chinese law, state secrets are classified into three levels: top secret, secret, and confidential. The difference between "core" and "ordinary" encryption is that "core" encryption can be used to protect all three levels of state secrets, but "ordinary" encryption can be used only to protect state secrets at the secret and confidential levels.

2. Commercial Encryption

Use of Commercial Encryption

The Encryption Law states that commercial encryption is not a state secret and that entities and individuals can use commercial encryption to protect network and information security in accordance with laws in China (Article 8). However, the Law is silent on a more precise definition of commercial encryption, so companies are still left without significant guidance regarding when a particular technology is deemed to be "commercial encryption" and thus subject to the Encryption Law.

The Encryption Law also provides that entities engaging in commercial encryption must comply with mandatory national standards in this area and their own published technical standards, in addition to complying with laws and regulations (Article 24).

Note that this approach of deregulating commercial encryption departs significantly from the approach taken by the previous encryption regulations,[2] which were first adopted in 1999. Under the previous regulations, the import, export, sale, use of, and scientific research upon encryption products and technologies in China were heavily regulated through a series of permits for production, sale, and use. In particular, entities and individuals were previously required to use only approved encryption products manufactured in China, and no entity or individual was allowed to distribute or use foreign-produced commercial encryption products. An exception was offered to foreign entities (including foreign-invested entities) and individuals: such entities and individuals can apply to the SCA to import foreign-produced commercial encryption products for their own use.

The language in the new Encryption Law seems to remove most of the prior restrictions on the use of foreign-produced commercial encryption products, but foreign-produced commercial encryption products and services may still be subject to import and export control requirements, testing and certification requirements (under limited circumstances) and national security review requirements, as discussed below. The head of SCA also indicated in an article that the regulators will soon update the previous regulations so the Encryption Law can be fully implemented.[3]

Import and Export Control Requirements

The Encryption Law establishes an import licensing and export control framework that governs (i) the import of commercial encryption that "may impact national security or the public interest" and "provide an encryption protection function," and (ii) the export of commercial encryption that "may impact national security or the public interest" or is required by China's international obligations. The list of commercial encryption in scope of this framework will be published by the Ministry of Commerce in conjunction with the SCA and the General Administration of Customs at an unspecified later date (Article 28).

The same provision also makes clear that these import licensing and export control requirements do not apply to commercial encryption used in "products for consumption by the general

[2] Regulations on Administration of Commercial Encryption (1999); Administrative Rules on the Use of Commercial Encryption Products (2007).

[3] 新时代密码工作的坚强法律保障 ("Strengthening Legal Protections in a New Era of Cryptography Work")

population." The Encryption Law does not define this term, leaving unclear how this important exemption would work in practice.

Testing and Certification of Commercial Encryption Products and Services

Similar to the Cybersecurity Law, the Encryption Law encourages organizations and enterprises to voluntarily apply to qualified testing and certification agencies for the testing and certification of their commercial encryption products (Article 25). The final version of the Encryption Law also adds a provision to impose strict confidentiality obligations on testing and certification agencies, preventing them from disclosing state secrets and trade secrets obtained during the certification process (Article 25).

However, testing and certification might be mandatory for certain commercial encryption products and services under Article 26, as described below. Note that the Encryption Law makes it clear that such testing and certification will follow the framework established by the Cybersecurity Law (Article 23) and there should be no duplicative or repetitive testing or certification requirements.

- "Commercial encryption products" that may affect "national security, national welfare and people's livelihood, and society's interest" shall be included in the *Catalogue of Critical Network Equipment and Network Security-specific Products* (Catalogue) (see Covington's previous blogpost describing this Catalogue here); as a result of the inclusion, such products will be required to go through mandatory testing and certification per the requirements under the Cybersecurity Law.
- If a "commercial encryption service" uses any equipment or products that are listed in the *Catalogue of Critical Network Equipment and Network Security-specific Products*, such commercial encryption service must be certified by qualified certification agencies.

Note that the Encryption Law does not provide a definition for "commercial encryption product." Nor does it define "commercial encryption service." According to a Q&A of the Encryption Law released by the Cyberspace Administration of China (CAC), the government plans to issue more catalogues to clarify the scope of commercial encryption products and services. It is unclear at this stage whether the "core function" test that has been introduced around since 2000 will be adopted to determine whether a product or service will be considered commercial encryption product or service. But the issuance of such catalogues will likely provide more clarity on what products or services may fall into the scope of "commercial encryption" product or service.

Security Assessment and National Security Review

The Encryption Law also imposes the following specific obligations on the operators of Critical Information Infrastructure (CII).

- Security Assessment. CII operators that are required to adopt commercial encryption for security purposes (in order to comply with other laws and regulations) are required to carry out a security assessment on their use of commercial encryption. Such security assessment can be conducted either by the CII operator themselves or by external testing agencies (Article 27).
- National Security Review. If the procurement and use of commercial encryption products and services may impact national security, CII operators must apply for a national security review led by the CAC and SCA (Article 27). Again, such a review should follow the process established by the Cybersecurity Law (see Covington's previous blogpost describing this process here).

Note that the above security assessment and national security review requirements apply to CII operators (i.e., users of commercial encryption) rather than manufacturers or providers of commercial products or services, which are different from the testing and certification requirements.

Enforcement and Penalties

The Encryption Law requires the SCA and other government agencies to enforce the rules through day-to-day supervision and random inspections. In addition, the government plans to link this enforcement mechanism with China's social credit system (Article 31), although the Encryption Law does not clarify how the two systems will interact.

Furthermore, Article 31 of the Encryption Law strictly prohibits the SCA and other government agencies from forcing (i) entities engaging in research, production, sale, service, and import/export of commercial encryption; and (ii) commercial encryption testing and certification agencies, to disclose the source code or other relevant proprietary information. SCA and other government agencies are also required to keep confidential the trade secrets and privacy information obtained when performing their duties.

The final section of the Encryption Law includes a number of provisions specifying penalties for non-compliance. For example, if an entity distributes or sells commercial encryption products or services that do not obtain certification or fail testing where such is required under Article 26, then the Administration for Market Regulation may issue a warning and confiscate illegal gains (Article 36). If a CII operator fails to use commercial encryption for security protection or fails to carry out security assessment in accordance with Article 27 of the Encryption Law, the SCA may issue a warning and order such CII operator to confiscate its violation; if such CII operator refuses to make rectification or the cybersecurity is harmed due to such violation, such CII operator may be subject to a fine in an amount of RMB 100,000 to 1,000,000 (about USD 14,500 to 145,000) and the person directly in charge may also be subject to a fine in an amount of RMB 10,000 to 100,000 (about USD 1,450 to 14,500).

Unanswered Questions

The Encryption Law outlines a new regulatory framework but leaves unanswered numerous questions that we typically receive from clients on encryption issues in China:

- How will a company know with some confidence whether a particular technology is "commercial encryption" and therefore subject to the Encryption Law?
- Aside from the guarantees in the Encryption Law, are there other ways to protect a company's technology during the testing and certification process?
- Subject to further interpretation on the scope of "products for consumption by the general population," can a company bring into China the same encryption-related products that the company uses worldwide, such as VPNs and encrypted hard drives?
- Can a foreign company do research on encryption issues in China, and if so, can such company export that research outside of China?

We anticipate that some of these questions may be answered in future implementing regulations.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our firm:

Yan Luo	+86 10 5910 0516	yluo@cov.com
Eric Carlson	+86 21 6036 2503	ecarlson@cov.com
Tim Stratford	+86 10 5910 0508	tstratford@cov.com
Kurt Wimmer	+1 202 662 5278	kwimmer@cov.com