COVINGTON

China Releases Draft Encryption Law for Public Comment

May 9, 2017

Data Privacy and Cybersecurity

On April 13, 2017, China's State Cryptography Administration ("SCA") published a draft Encryption Law ("the draft Law") for public comment.

After several years of drafting, the draft Law, if enacted as drafted, would be the first Chinese statute to systematically address encryption, covering "the research, production, management, import and export, testing, authentication, use, and regulation of encryption." China has long regulated the import, export, sale, use, and scientific research of "commercial" encryption. The draft Law, however, provides rules for three categories of encryption—"ordinary" encryption, "core" encryption, and "commercial" encryption—with a view to establishing a uniform regulatory framework that would govern all types of encryption and providing SCA with greater enforcement authority.

In addition to expanding the scope of the current "commercial" encryption regulations, the draft Law could have significant implications for a range of companies that use or provide encrypted products and encryption-related services in China:

- The draft Law is unclear whether users are obliged to use only pre-approved domestic commercial encryption products, or whether foreign-invested entities and individuals located in China are still entitled to apply to SCA to use foreign-produced commercial encryption products or technologies, an exception provided by the current regulations.
- The draft Law signals potential overlap with the Cybersecurity Law, which will take effect in June 2017, by requiring a national security review for the use of encryption products or encryption-related services by operators of Critical Information Infrastructure, if such use has the potential to impact China's national security.
- For national security reasons or for criminal investigations, the draft Law provides that various government entities can require telecommunications companies and Internet service providers to provide "decryption technology support."
- The draft Law provides for civil and criminal penalties for non-compliance for both entities and individuals.

This alert highlights key features of the draft Law and reviews potential implications.

Highlights of the Draft Law

In releasing the draft Law, the SCA highlighted several guiding principles:

Objectives and Definition of Encryption

The draft Law broadly applies to the research, production, management, import, export, testing, authentication, use, and regulation of encryption (Article 2).

"Encryption" is defined as "items or technologies using specific transformations to data and other information to effect encryption protection or security authentication" (Article 3).

The draft Law emphasizes the centralized and unified regulation of encryption, led directly by the Chinese Community Party (Articles 4, 5).

Encryption Classification

The draft Law provides for three encryption classifications: core encryption, ordinary encryption, and commercial encryption (Article 7). Core and ordinary encryption can be used for the protection of data constituting "state secrets," while commercial encryption is used to protect data that are not state secrets (Article 10).

Management of Encryption Products and Services

The draft Law provides for the licensing and cataloging by SCA of commercial encryption products and services (Articles 11) and the management of e-government and electronic authentication services (Articles 13, 14). The draft Law's treatment of commercial encryption is generally consistent with existing regulations governing such encryption but are less detailed. As noted above, the draft Law stops short of requiring entities and individuals to use only preapproved commercial encryption products and does not provide a penalty for users using unapproved commercial encryption products. It is uncertain whether the current commercial encryption regulations will be revised later to align with this Law.

Encryption Security

Security concerns are foundational to the draft Law's proposed regulatory framework. The draft Law establishes an import and export regime governing encryption (Article 16); a testing and authentication system (Article 17); a security rating and inspection system (Article 18); a security collaboration mechanism employing early warning systems, notifications, and emergency consultations (Article 19); decryption obligations of telecommunications companies and Internet service providers (Article 20); and prohibitions on breaching encrypted data or systems and misuse of encryption (Article 21).

Encryption Enforcement Structure

The draft Law authorizes SCA and its local counterparts to supervise, inspect, and enforce the laws governing encryption applications and encryption security, and to investigate encryption breach incidents (Article 27). To this end, the draft Law provides for enforcement mechanisms (Article 28) and enforcement authority, including conducting on-site inspections and investigations, accessing relevant data, and seizing illegal equipment and facilities (Article 29).

Potential Implications

Several features of the draft Law raise questions about implementation and enforcement. First, although "commercial encryption" is relatively clearly defined as encryption protecting data other than "state secrets" (consistent with the existing commercial encryption regulations), the key classifications of "core encryption" and "ordinary encryption" are not defined with any degree of clarity. Both "core" and "ordinary" encryption can implicate the protection of state secrets, and further clarification of their scope and the distinction between the two may fall to future implementing regulations.

The draft Law also signals potential overlap with the Cybersecurity Law, which will take effect in June 2017 (see Covington's previous alert here). The draft Law, like the Cybersecurity Law, draws attention to the special status of Critical Information Infrastructure, providing that such infrastructure must use encryption to protect data in accordance with applicable laws, regulations, and standards (Article 12) and calls on national security reviews for encrypted products and services used for the protection of such infrastructure, if China's national security might be impacted (Article 18).

Compulsory decryption support could also be a future flashpoint. Article 20 provides that for national security reasons or for criminal investigations, various government entities can legally require telecommunications companies and Internet service providers to provide "decryption technology support." Moreover, telecommunications companies and Internet service providers are required to keep such cooperation confidential. When balancing between data security and privacy, on the one hand, and national security, on the other, the draft Law tips decisively in favor of national security.

Several provisions provide for penalties in cases of non-compliance, though the scope and magnitude of many penalties are not defined. Article 37 provides that any failure to provide decryption support or to maintain confidentiality in violation of Article 20 can result in monetary penalties imposed on the organization and individual employees, with serious violations resulting in detention of five to 15 days. Monetary penalties are not specified. Article 33 authorizes monetary penalties for the illegal operation of commercial encryption products or provision of commercial encryption services or e-government or electronic authentication services. In addition to questions about the magnitude of such penalties, it is unclear whether they would extend to the numerous consumers who use commercial encryption, as opposed to the product manufacturers and service providers alone. Article 35 provides for unspecified penalties for violations of Article 16, which prohibits the export of "core" and "ordinary" encryption and subjects the import and export of commercial encryption to a licensing regime.

Lastly, and more generally, SCA's expansive investigatory and enforcement authorities under Article 29 creates the potential for tensions with regulated parties. Businesses that seek to comply in good faith may be concerned about the SCA's ability to conduct on-site inspections and investigations, access data, and seize equipment and facilities.

Those interested in learning more about the draft Encryption Law may contact the following Covington lawyers:

Eric Carlson	+86 21 6036 2503	ecarlson@cov.com
Tim Stratford	+86 10 5910 0580	tstratford@cov.com
Yan Luo	+86 10 5910 0516	yluo@cov.com
Victor Ban	+1 202 662 5553	vban@cov.com

This information is not intended as legal advice. Readers should seek specific legal advice before acting with regard to the subjects mentioned herein.

Covington & Burling LLP, an international law firm, provides corporate, litigation and regulatory expertise to enable clients to achieve their goals. This communication is intended to bring relevant developments to our clients and other interested colleagues. Please send an email to unsubscribe@cov.com if you do not wish to receive future emails or electronic alerts.