Updates
September 03, 2019

China’s New Draft Encryption Law

The Standing Committee of the National People's Congress released the *Encryption Law of the People's Republic of China (Draft)* for public comment on July 5, 2019 (the "2019 Draft"). The Encryption Law is being enacted to do the following:

- regulate encryption application and management,
- promote encryption development,
- safeguard network and information security,
- protect the data security rights of companies and people, and
- safeguard China's national security and public interests (art. 1).

The 2019 Draft supersedes a prior draft issued by China's State Cryptography Administration and includes important changes with respect to the definition of encryption and the management of commercial encryption. Most importantly, the 2019 Draft deletes a controversial provision in the prior draft that would have required telecommunications operators and internet service providers to decrypt and thus provide the People's Republic of China (PRC) access to information whenever necessary for national security or the prosecution of criminal cases.

Highlights of the 2019 Draft

Definition of Encryption

The word "encryption" is defined extremely broadly such that it refers to all products, technologies and services using encryption protection or security authentication to protect information. (art. 2).

Three Categories of Encryption

The 2019 Draft defines three categories of encryption. Core and common encryptions are used to protect PRC state secrets, with the former category protecting "top secret" information and the latter category protecting common "secrets." (arts. 6 and 7). Commercial encryption refers to encryption used to protect information that does not rise to the level of a state secret, often used by people and companies to protect network and information security (arts. 7 and 8).

Commercial Encryption Requirements

The 2019 Draft codifies the general rule that people and companies may not steal the encrypted information of others (art. 12) and instructs all people and companies to immediately report to the appropriate PRC authorities any breach or compromise of a core or common encryption (art. 17). In addition, and most importantly for people and companies that do not have or transmit any state secrets, the 2019 Draft provides detailed requirements regarding the security management of commercial encryption, such as the following:

1. Commercial encryption products involving national security, national economy, livelihood of PRC citizens will be listed as "network-critical equipment and network security-specific products" and may be sold only after they pass a safety authentication or inspection (art. 26);

2. Critical information infrastructure (CII) must be protected by commercial encryption as required by relevant laws and regulations. The operators of the CII also must protect it using commercial encryption and conduct security assessments accordingly (art. 27); and
3. Every CII operator must pass a national security review before purchasing and using any network products or services involving commercial encryption that might in any way have an impact on national security (art. 27).

Supervision of Commercial Encryption

Policy of Import and Export: The PRC will implement a policy of import licensing and export control for all commercial encryption involving national security and social public interests (art. 28).

Supervision and Management Information Platform: A unified supervision and management information platform for commercial encryption will be established by a number of different government departments. The supervision of commercial encryption will be carried out on a day-to-day basis as well as through random spot-checks, although all companies using commercial encryption should establish self-disciplinary protocols to monitor and supervise the people within each organization (art. 31).

Legal Liabilities

Any person who steals another's encrypted information, invades another's system or jeopardizes national security and the lawful and social rights and interests of others will be subject to an investigation and/or criminal penalties (arts. 32 and 41). For all other violations of the 2019 Draft, the relevant departments will issue warnings, order corrections, confiscate any inappropriate gains, and/or impose a fine of no more than three times of the amount of those gains, etc. (arts. 33-40).

Impact of the Encryption Law

Once implemented, what is now the 2019 Draft will become the formal Encryption Law and the first law in the PRC to address encryption-related issues under a unified legal framework. The 2019 Draft is still vague on details, however, and leaves much room for further interpretation on how to implement and comply with the relevant provisions. This is a law that is already two years in the making, and we expect it will take several more years before the 2019 Draft becomes final.

Authors

Geoffrey A. Vance

Partner
GVance@perkinscoie.com 312.324.8477

Explore more in

Corporate Law Privacy & Security Communications

Related insights

Update

CFPB Finalizes Proposed Open Banking Rule on Personal Financial Data Rights

Update

FDA Food Import and Export Updates for Industry