Evolving trade war challenges: new Encryption Law and the related supply chain and data security considerations

April 1, 2020

In brief

One important aspect of the "technology decoupling" between US and China is in the area of cyber and information security, where China is overhauling its legal regime that governs encryption used in China to protect network and data confidentiality.

As China enacted the Encryption Law of the People's Republic of China ("**Encryption Law**") in October 2019, multinational corporations ("**MNCs**") became concerned with the prospect of this new law compromising their data security in China. The implications of this new law also go beyond data security and could substantially impact the supply chains of MNCs in China involving controlled encryption items.

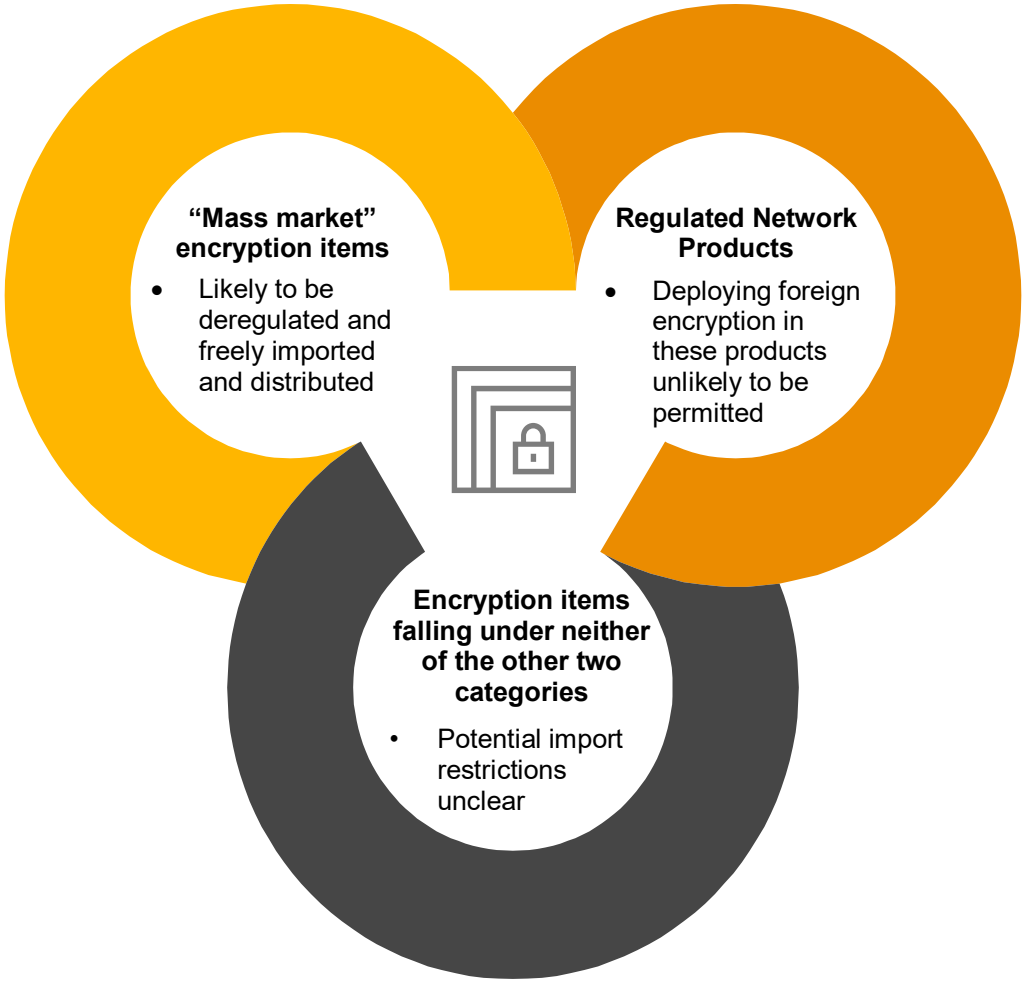
While this new legal regime will not be fully established until the State Council and the Statement Encryption Management Bureau ("**SEMB**") roll out all the implementation regulations, we highlight below some key issues that MNCs should take into account when evaluating their data and network security strategies in China, as well as the impacts of the new regime on the viability of the current supply chain structures.

The changing import restriction landscape

The regulatory landscape in this regard may substantially change under the new regime.

Currently, encryption products or technologies that use foreign developed algorithms (referred to as "**foreign encryption items**") are, in theory, categorically prohibited from importation into China, unless they are used by China subsidiaries of foreign MNCs for the purpose of intra-group communications. In practice, however, companies may still be able to import some foreign encryption items, without triggering substantial compliance issues, through either: (1) online transmission of encryption software (on which current regulations do not impose any meaningful restrictive measures), or (2) incorporating the encryption into a larger instrument, of which the "core function" may be characterized as non-encryption-related.

In contrast, under the new Encryption Law, the level of restriction imposed on foreign encryption items may vary significantly (see the diagram below):



- At one extreme are the so-call "mass market" encryption items, which may be largely deregulated, and freely imported and distributed in China. While a clearer scope of the "mass market" items are still to be defined by the implementation regulations, the similar "mass market exclusion" regimes in other jurisdictions suggest that these may include primarily retail products.

- At the other extreme are the "critical network equipment" and "specialized network security products" (collectively "**Regulated Network Products**"), ranging from networking hardware, such as routers meeting certain capability standards, to software, such as intrusion detection systems ("**IDS**"), defined separately under the Cybersecurity Law. As encryption is widely deployed in these Regulated Network Products, they are at the intersection between the Cybersecurity Law and the Encryption Law. Under the new Encryption Law, this category of products will be subject to the tightest restrictions when it comes to market access. Deploying foreign encryption in these products is unlikely to be permitted.

- Between these two extremes are an array of encryption items that are neither retail products nor Regulated Network Products. These may include, for example, **elements (including hardware and software) to be incorporated into a product manufactured in China (e.g., an automotive part), components of chip manufacturing equipment (e.g., hardware security modules) that provide cryptographic keys to the chips, and technologies deployed to support an e-authentication system operated by a service provider in China**. Some of these products may be included in a new "dual-use encryption catalogue", which will be jointly published by SEMB, the General Administration of Customs ("**GAC**") and the Ministry of Commerce ("**MOFCOM**"), as part of China's new export control regulatory scheme to impose the import permit and export license requirements. As further discussed below, the nature and scope of controls over this category of encryption items may pose the greatest uncertainty to businesses.

Nature and scope of controls under the new scheme

With respect to this upcoming "dual-use encryption catalogue", the following aspects are worthy of note:

- **"Catch-all" language**. The three agencies will release a catalogue that provides a more definite scope of encryption items subject to import and export controls, compared to the current catalogue which contains only a non-exhaustive list and a rather vague "catch-all" provision. That said, it is still unclear whether the "catch-all" language will be entirely removed from the new catalogue, and if not, whether it will still draw a distinction between encryption and non-encryption items based upon their "core functionalities".

- **Scope of controlled foreign encryption expanding into software and technologies**. Because the new catalogue is to be published by MOFCOM, China's top export control authority, along with SEMB and GAC, it would very likely adopt the structure of a typical "dual-use catalogue", which includes not only tangible goods (to which tariff codes may be assigned in the catalogue), but intangibles that do not require import or export customs clearance. This will expand the scope of controlled encryption to encryption software and technologies, which are largely left as unregulated under current regulations.

- **End-use and end-user restrictions**. The current regulations only permit foreign encryption to be imported by subsidiaries of foreign MNCs for the purpose of intra-group communications. As a matter of fact, however, foreign encryption technologies and products are also widely used in other business activities, such as manufacturing, software engineering and customer or vehicle authentication, etc. One of the workarounds typically used to overcome such restrictions, as discussed above, involves characterising the foreign encryption as a "non-core function" of the product or system where it is deployed. It is worthwhile to note whether there will be any change to such end-use and end-user restrictions under the new implementation regulations.

Also note, the "dual-use encryption catalogue" under the Encryption Law may not cover all the encryption items that are neither "mass market" items nor Regulated Network Products. For those that are not covered by the "dual-use encryption catalogue", the potential market access barriers may be more uncertain.

Use of foreign encryption for protecting data network in China

Under the Cybersecurity Law, the data networks in certain critical sectors (such as finance, telecommunication, energy, public transportation, public health, etc., known as "critical information infrastructure", or "**CIIs**") will be heavily regulated. As a result, the encryption of such networks, as well as the other aspects of the data security schemes adopted by the CIIs, will be subject to a highly discretionary review process, known as "national security review", administered by the top cybersecurity agencies.

While the details of this review process are still to be unveiled by the cybersecurity agencies, it is widely anticipated that government intervention in CII's encryption schemes, including the encryption algorithms and protocols, could be substantial. This may leave limited or no room for deploying foreign encryption in CII networks.

On the other hand, SEMB has also confirmed that non-CII networks are not subject to mandatory encryption requirements. This suggests that businesses may be free to choose the suitable encryption schemes for their non-CII networks. However, the availability of the encryption technologies and products to be deployed in their networks, in particular those classified as Regulated Network Products, will still be subject to the import and market access restrictions discussed above.

The risk of forced disclosure of encryption source codes to the Chinese authorities

The Encryption Law prohibits encryption regulators from forcing businesses or "third party institutes" to disclose encryption source codes. The reference to "third party institutes" in that provision suggests that those institutes, in addition to businesses themselves, may also gain access to encryption source codes.

Under the Encryption Law, those third party institutes are specifically designated as responsible for conducting a technical review process, known as "testing and accreditation", in order to determine the compliance of encryption items deployed in the products concerned with the applicable Chinese technical protocols and standards. If the encryption needs to undergo such "testing and accreditation" process, the risk of businesses disclosing source codes to the government-designated institutes may be relatively high.

The Encryption Law generally allows companies to engage third party institutes to conduct “testing and accreditation” on a voluntary basis, unless the encryption is deployed in Regulated Network Products, which will be subject to mandatory “testing and accreditation” requirements. Having said that, it is still likely that, in some projects (e.g., government procurement projects), the buyer requires passage of “testing and accreditation” as a precondition to signing a supply agreement, notwithstanding the non-mandatory nature of this process.

Another scenario in which the encryption source codes may need to be disclosed to third party institutes is that the encryption is deployed in a CII, as CIIs are subject to the “national security review”, which may involve a thorough examination of all aspects of the data security scheme, including encryption.

Conclusion

The implementation regulations for the Encryption Law are anticipated to be unveiled in the next few months, and will significantly change the current regulatory landscape. We encourage businesses to reassess the encryption deployed in their internal data networks and products, or otherwise utilized in their business operations in China, in order to evaluate the impacts of the new regulatory scheme on their data security and supply chains.

Let's talk

For a deeper discussion of how this impacts your business, please contact:

William Marshall
Partner
Tiang & Partners
Tel: +852 2833 4977
william.marshall@tiangandpartners.com

Frank Pan
Partner
Xin Bai Law Firm
Tel: +86 (21) 5368 4080
frank.ya.pan@xinbailaw.com

About us

Xin Bai Law Firm is an independent China law firm and a member of the PwC global network of firms, dedicated to providing clients with integrated solutions and high-quality legal advice in Mainland China, across Asia and globally. The lawyers are governed by Chinese regulatory standards and they provide legal opinions and advice to clients on matters under Chinese law. Principally based in Shanghai, our team operates across China and very often on global projects.

Tiang & Partners is an independent Hong Kong law firm. It is associated with PwC Legal International Pte. Ltd. (a licensed Foreign Law Practice) in Singapore. We also collaborate closely with Rui Bai Law Firm in Beijing and Xin Bai Law Firm in Shanghai to provide seamless legal services to our clients in China.

www.xinbailaw.com
www.tiangandpartners.com

pwc

Tiang & Partners
程偉賓律師事務所