

Online Videogame Cos. Must Prepare For China Data Law

SEPTEMBER 3, 2021

This article was originally published in [Law360](#). Any opinions in this article are not those of Winston & Strawn or its clients. The opinions in this article are the author's opinions only.

The People's Republic of China is a critical market for the online videogame industry, and China strictly regulates that industry for content, addiction avoidance, protection of minors, and other factors.

Data is an important asset for online videogame companies, and China has developed a powerful regulatory regime for data protection. In its most recent data protection move, the PRC National People's Congress passed the Personal Information Protection Law, or PIPL, which will come into effect on Nov. 1.

The PIPL creates unique challenges that will particularly affect the online videogame industry because of the industry's nature, the PIPL's extraterritorial application,^[1] and the magnitude of China-based users. These challenges include the need for Mandarin-language terms of use and consents^[2] as well as the necessity for companies that process China-based personal information outside China to appoint a responsible party inside China.^[3]

Additional challenges exist for companies in conducting cross-border transfers of personal information from China.^[4] However, one of the most significant challenges for online videogame companies will be fulfilling the required procedures and instituting adequate protections for China-based gamers under the age of 14, or minors.

Make no mistake, China takes the protection of its children seriously. In the last six months, China has revised its Law on the Protection of Minors,^[5] taken regulatory steps against the tutoring industry,^[6] and made negative statements through state owned media on the effect of online videogames on children.

The PIPL takes the protection of minors a step further and extends those requirements to companies outside China.

The operations of online videogame companies outside China may inadvertently become subject to the PIPL's requirements by allowing China-based users to access its games operated outside China.

While it is typical for online videogame companies to have specialized versions of games in China to comply with local content-based regulations, it is also common for China-based users to play online videogames on servers

outside China to access more titles and less restrictive games and gameplay.

Many of those China-based users are minors. Thus, online videogame companies are more likely to become subject to the rigid requirements of the PIPL for processing the personal information of minors.

The personal information of minors is not treated as regular personal information in the PIPL. Under Article 53, the personal information of minors under the age of 14 is classified as sensitive personal information.

As opposed to regular personal information, the distinction for personal information of minors and its classification as sensitive personal information has the following significant ramifications:

- It is necessary to obtain advanced and informed parental consent to process minors' personal information.
- Personal information processors must formulate special personal information processing rules for minors' personal information.
- Sensitive personal information can be processed only when there is a specific purpose and sufficient necessity, and strict protective measures must be employed.
- Personal information processors must conduct a personal information protection impact assessment before processing sensitive personal information.

For online videogame companies with operations in China, games published in China or online videogame companies considering entering the China market, compliance with the PIPL is not optional.

The Cyberspace Administration of China, or CAC, will have oversight of compliance with the PIPL, and in recent weeks it has gone on an enforcement push, mandating cybersecurity reviews and ordering China-based mobile-application stores to remove numerous mobile apps for data and personal information protection issues.

In addition, the CAC shares leadership with the Propaganda Department, which sits over the National Press and Publication Administration. The National Press and Publication Administration controls the publications of games.

Thus, beyond the penalties authorized in the PIPL, which can be substantial—up to 50 million yuan or 5% of the previous year's turnover—access to the China market is at risk. At the same time, China's regulators will hold a more favorable view of companies that attempt to comply with the PIPL in their operations outside China as a demonstration of respect.

Compliance with the PIPL's provisions from overseas, particularly those related to minors' personal information, will be challenging, and both technical and legal solutions are required.

Technically, the first challenge will be to identify the origin of users when those users are probably accessing overseas servers via a virtual private network. While utilizing a VPN may not be permitted in China, the PIPL does not include a safe-harbor provision when users utilize a VPN.

The next challenge will be to identify the age of the users to determine whether parental consent is required, followed by confirming that it is the parent who provided that consent.

This requirement is less burdensome inside China because it has long requirements for online companies to verify identification. Tencent Holdings Ltd. provides an example of how companies inside China are attempting to comply. It has stated that it will use facial recognition technology to help protect minors.

Outside China, this will be both a legal and a business consideration, and a blanket practice for all users and all regions may not be suitable. Furthermore, using facial recognition, biometrics, etc. outside China may trigger additional issues under the PIPL.

From a legal perspective, companies need to consider how to draft consents and terms of use. Online videogame

companies always encounter the question whether to create separate terms of use for different jurisdictions according to local laws.

In this situation, the answer is clear: The best practice for online videogame companies will be to draft terms of use and consents in accordance with China law.

The personal information impact assessment will also require the integration of technical and legal teams, and the final document may end up being reviewed by China regulators. Thus, it should be conducted in a way that will satisfy China's regulators.

However, because this is a new procedure and guidance has yet to be issued, it is advisable to start early and communicate with regulators to make sure the impact assessment is properly completed before the PIPL comes into effect.

For online videogame companies' operations outside China, compliance with the PIPL will be particularly challenging. Companies will want to utilize local counsel with experience in helping foreign companies with data compliance in China to help complete the process before the November deadline, because the CAC is already taking enforcement actions.

Most of the compliance challenges will be front loaded, and quality compliance policies and procedures will make future maintenance less costly and burdensome. The cost of not taking steps to comply could be losing access to the China market.

[1] Under article 3, the PIPL will have extraterritorial application and apply to the processing of personal information of people within the PRC outside the borders of the PRC (1) where the purpose is to provide products or services to people in the PRC, (2) where the purpose is to analyze or assess activities of people in the PRC, or (3) for other unspecified circumstances.

[2] PIPL article 13 provides for consent as a basis for processing personal information. PIPL article 14 requires that consent be fully informed consent.

[3] PIPL article 53 requires offshore personal information processors subject to the PIPL under article 3 to appoint a representative inside of China.

[4] PIPL chapter III provides the rules for cross-border transfer of personal information.

[5] The revisions to the Law on Protection of Minors came into effect on June 1, 2021.

[6] On July 24, 2021, the General Office of the Communist Party of China Central Committee and the General Office of the State Council issued rules limiting online tutoring and homework.

5 Min Read

Related Topics

Law360

Privacy and Data Security

Videogames

China

Related Capabilities

Privacy & Data Security

Compliance Programs

Technology, Media & Telecommunications

Related Regions

North America

Asia

Related Professionals



Jacob Harding