How Will the New Bulk Data Transfer Rule Impact China's Game Companies?

U.S. TECH LAW UPDATE[1]

March 14, 2025
By: Chao Yu | Ziwei Zhu

On December 27, 2024, the Department of Justice ("DOJ") issued a final rule implementing the Executive Order 14117 aimed at preventing access to Americans' bulk sensitive personal data and U.S. government-related data by certain countries or persons (the "Final Rule"). The Final Rule is set to take effect on April 8, 2025, 90 days after its publication in the Federal Register, while certain due diligence requirements for restricted transactions will become effective on October 6, 2025, 270 days after publication.

The Final Rule establishes a new national security framework that prohibits or restricts U.S. persons from engaging in certain transactions that may result in the transfer of bulk U.S. sensitive personal data and/or government related data to a person in a country of concern. The Final Rule could have wide-ranging implications for both U.S. and China companies across various industries, including the video game industry.

To facilitate the implementation of the Final Rule, the U.S. Cybersecurity and Infrastructure Security Agency ("CISA") released the final Security Requirements for Restricted Transactions (the "Security Requirements") on January 3, 2025.[2] The Security Requirements set forth the standards and measures that U.S. persons must satisfy in order to engage in restricted transactions, and are incorporated by reference into the Final Rule.

This U.S. Tech Law Update provides an overview and summary of the key provisions of the Final Rule. It then explores the data collection practices of China game companies expanding into the U.S. market. Finally, this article assesses the potential implications of the Final Rule for the U.S. operations of China game companies and outlines strategic recommendations to effectively navigate these developments.

1. Overview of the Final Rule

The prohibitions and restrictions under the Final Rule apply only to covered data transactions between a U.S. person and a country of concern or a covered person. The Final Rule defines covered data transactions as "any transaction that involves access by a country of concern or covered person

[1] This U.S. Tech Law Update is provided by Pillar Legal, P.C. (the "Firm") as a service to clients and other readers. The information contained in this publication should not be construed as legal advice, and use of this memorandum does not create an attorney - client relationship between the reader and the Firm. In addition, the information has not been updated since the date first set forth above and may be required to be updated or customized for particular facts and circumstances. This U.S. Tech Law Update may be considered "Attorney Advertising" under applicable law. Questions regarding the matters discussed in this publication may be directed to the Firm at the following contact details: +1-415-463-4997 (San Francisco office and San Diego office), +86-21-5876-0206 (Shanghai office), email: info@pillarlegalpc.com. Firm website: www.pillarlegalpc.com.

[2] See CISA website here.

to government-related data or bulk U.S. sensitive personal data and that involves: (1) data brokerage; (2) a vendor agreement; (3) an employment agreement; or (4) an investment agreement."

A. U.S. Person

The Final Rule defines the term "U.S. person" broadly, including U.S. citizens, lawful permanent residents, entities organized under U.S. laws (including foreign branches), and any person located within the United States. Under this definition, a U.S. entity organized solely under the laws of the United States, even if ultimately owned or controlled by a China company, will be considered a U.S. person unless otherwise designated by the Attorney General.[3] Additionally, a Chinese national residing in the U.S. is also considered as a U.S. person unless designated otherwise.[4]

B. Countries of Concern and Covered Person

The list of countries of concern in the Final Rule currently includes China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia, and Venezuela.

The Final Rule's definition of "covered person" is:

(a) A foreign person that is an entity that is 50 percent or more owned, directly or indirectly, individually or in the aggregate, by one or more countries of concern or persons described in paragraph (b) below; or that is organized or chartered under the laws of, or has its principal place of business in, a country of concern;

(b) A foreign person that is an entity that is 50 percent or more owned, directly or indirectly, individually or in the aggregate, by one or more persons described in paragraph (a) above or (c), (d), or (e) below;

(c) A foreign person that is an individual who is an employee or contractor of a country of concern or of an entity described in paragraph (a) or (b) above, or (e) below;

(d) A foreign person that is an individual who is primarily a resident within the territorial jurisdiction of a country of concern; or

(e) Any person, wherever located, determined by the Attorney General: (i) to be, to have been, or to be likely to become owned, controlled by, or subject to the jurisdiction or direction of a country of concern or a covered person; (ii) to act, to have acted or purported to act, or to be likely to act for or on behalf of a country of concern or covered person; or (iii) to have knowingly caused or directed, or to be likely to knowingly cause or direct a violation of the Final Rule.

[3] See Example 8 of Section 202.256(b) of the Final Rule.
[4] See Example 1 of Section 202.256(b) of the Final Rule.

Under the Final Rule's definition, the term "covered person" encompasses a broad range of individuals and entities with ties to China. For example, a wholly owned China subsidiary of a German company qualifies as a "covered person." Additionally, a Singapore based company that is 50% or more owned by a China based company is also considered a "covered person,"[5] and any individual, even a Singaporean national, working for that Singapore based company is considered a "covered person".[6]

C. Covered Data

Not all data is subject to the restrictions or prohibitions of the Final Rule; only the transfer of bulk U.S. sensitive personal data and government-related data is considered to pose potential national security risks.

The U.S. regulates sensitive personal data based on corresponding "bulk" thresholds. The term "bulk" is defined as any amount of sensitive personal data that meets or exceeds the following thresholds at any point in the preceding 12 months, whether through a single transaction or aggregated across multiple transactions "involving the same U.S. person and the same foreign person or covered person".

Data Category	**"Bulk" Threshold**
Human 'omic data[7]	More than 1,000 U.S. persons, or in case of human genomic data, more than 100 U.S. persons
Biometric identifiers	More than 1,000 U.S. persons
Precise geolocation data (within 1,000 meters)	More than 1,000 U.S. devices
Personal health data	More than 10,000 U.S. persons
Personal financial data	More than 10,000 U.S. persons
Covered personal identifiers	More than 100,000 U.S. persons

Unlike the data privacy laws in other countries, such as the European Union's General Data Protection Regulation (GDPR) and China's Personal Information Protection Law (PIPL), which allow the transfer of personal information if such information is anonymized, the Final Rule prohibits

[5] The foreign ownership threshold may be satisfied in the aggregate. See Example 7 of Section 202.211(b) of the Final Rule.
[6] See Example 5 of Section 202.211(b) of the Final Rule.
[7] According to Section 202.224 of the Final Rule, human 'omic data means (1) human genomic data, (2) human epigenomic data, (3) human proteomic data and (4) human transcriptomic data, but excludes pathogen-specific data embedded in human 'omic data sets.

or restricts transferring "bulk U.S. sensitive personal data" to countries of concern or a covered person, even if such data is anonymized, pseudonymized, de-identified, or encrypted.[8]

D. Covered Data Transactions

The covered data transaction means any transaction that involves access to any government-related data or bulk U.S. sensitive data and that involves (i) data brokerage, (ii) vendor agreement, (iii) employment agreement or (iv) investment agreement. The term "access" is defined broadly to cover logical or physical access, including the ability to obtain, read, copy, decrypt, edit, divert, release, affect, alter the state of, or otherwise view or receive, in any form, including through information systems, information technology systems, cloud-computing platforms, networks, security systems, equipment, or software. The covered data transactions can be further divided into prohibited transactions and restricted transactions as discussed below.

(1) Prohibited Transactions

Prohibited transactions are the following covered data transactions:

(a) Any covered data transaction involving data brokerage with a covered person or a country of concern. Notably, "data brokerage" is broadly defined as "sale of data, licensing of access to data, or similar commercial transactions involving the transfer of data from any person (the provider) to another (the recipient), where the recipient did not collect or process the data directly from the individuals linked or linkable to the collected or process data", which covers a range of transactions that many businesses may not consider "brokering" transactions in the traditional commercial sense.

One example given in the Final Rule states that a U.S. company owning or operating a mobile app for U.S. users with available advertising space qualifies as engaging in "data brokerage" if it provides bulk sensitive personal data (such as IP address and advertising IDs of more than 100,000 U.S. persons in a 12-month period) to an advertising exchange based in China.[9]

(b) Any covered data transaction involving data brokerage with any foreign person that is not a covered person, unless the U.S. person imposes contractual commitments on the foreign person not to engage in a subsequent transaction involving that data with a country of concern or covered person, and reports any known or suspected violation within 14 days to the DOJ.

(c) Any covered data transaction that involves access by a covered person to bulk U.S. human 'omic data or to human biospecimens from which bulk human 'omic data could be derived.

[8] See definition of "bulk U.S. sensitive personal data" in Section 202.206 of the Final Rule.
[9] See Example 4 of the Section 202.214(b) of the Final Rule.

(d) Any transaction structured for the purposes of evading or circumventing the regulations would also be prohibited. For example, if a U.S. subsidiary of a company headquartered in a country of concern grants a non-covered foreign company access to bulk U.S. sensitive personal data it collects from U.S. persons while knowing (or reasonably should know) that the foreign company is merely a shell entity that will transfer the data to the subsidiary's parent company, such a transaction would be deemed an attempt to circumvent the regulations and is prohibited.[10]

(e) Any transaction in which a U.S. person knowingly directs a covered data transaction that constitutes a prohibited transaction or restricted transaction that fails to comply with the requirements in the Final Rule.

(2) Restricted Transactions

Any covered data transaction involving a vendor agreement, employment agreement or investment agreement with a country of concern or covered person would be regarded as a restricted transaction. To engage in a restricted transaction, the U.S. person must comply with the requirements specified in the Final Rule, including (i) adhering to the CISA Security Requirements, (ii) implementing a data compliance program (mandatory by October 6, 2025); (iii) conducting annual independent audits to assess compliance with security requirements (effective October 6, 2025); (iv) maintaining complete and accurate transaction records for a period of at least ten years; and (v) fulfilling reporting obligations upon request.[11]

The restricted transactions cover a broad range of business activities or services provided by individuals or entities from China.

(a) Under the vendor agreement scenario, a U.S. company engaging a covered person to provide services, such as IT, software development, data management, customer support, cloud computing services, will be regarded as a restricted transaction if the covered person will have access to bulk U.S. sensitive personal data while performing those services. However, as noted in an example provided in the Final Rule, the reverse scenario – where a covered-person company engages a U.S. company under a vendor agreement to perform services involving access to bulk U.S. sensitive personal data by the U.S. company – would not be considered a covered data transaction, as it does not grant the covered person access to the data.[12]

[10] See Example 3 of Section 202.304(b) of the Final Rule.
[11] According to Subpart K of the Final Rule, reporting obligations are mandatory in following cases: (i) any U.S. person who has received and rejected (including through automatic means such as software or digital tools) an offer to engage in a prohibited data brokerage transaction must submit a report within 14 days of rejecting the transaction; and (ii) any U.S. person with 25% or more of their equity interests owned, directly or indirectly, by a country of concern or covered person, who engages in a restricted transaction involving cloud-computing services on or after October 6, 2025, must file an annual report.
[12] See Example 3 of Section 202.210(b) of the Final Rule.

The distinction between the vendor agreement and data brokerage scenarios can be confusing, as both may involve granting a covered person access to bulk U.S. sensitive personal data. While the Final Rule does not explicitly state this, the key difference lies in who has the authority to independently determine the purpose and method of data processing, or, in other words, who is the "data controller." In the vendor agreement scenario, the covered person is always the service provider, with the U.S. person paying for services to achieve its operational goals. In contrast, in the data brokerage scenario, the covered person pays for access to or a license for the bulk U.S. sensitive personal data to fulfill its own operational objectives.

(b) Under the employment agreement scenario, hiring a covered person, such as (i) an employee or board director, regardless of nationality (except U.S. nationals) who resides in China, and (ii) an executive officer who is a China nationality but not live in the U.S., will be regarded as a restricted transaction if the covered person would have the responsibility and authority to access bulk U.S. sensitive personal data collected by the U.S. company.

(c) Under the investment agreement scenario, a covered person investing in a U.S. business will be regarded as a restricted transaction if the covered person may have access to bulk U.S. sensitive personal data, except for any of the following investment that:

- is made (i) into a publicly traded security, (ii) into a security offered by an investment company or company regulated as a business development company; or (iii) as a limited partner in a venture capital fund, private equity fund, fund of funds, or other pooled investment fund, if the limited partner's contribution is solely capital;
- gives the covered person less than 10% in total voting and equity interest; and
- does not give a covered person rights beyond those reasonably considered to be standard minority shareholder protections.

(3) Exempt Transactions

The Final Rule further provides exemptions for certain transactions to which the prohibitions and restrictions do not apply, including, among others: data transactions related to personal communication,[13] information or informational materials, travel, official business of the United States government, financial services,[14] corporate group transactions,[15] investment agreements

[13] Data transactions that involve any postal, telegraphic, telephonic, or other personal communication that does not involve the transfer of anything of value.

[14] Data transactions for providing provision of financial services including the transfer of personal financial data or covered personal identifiers incidental to the purchase and sale of goods and services (such as the purchase, sale, or transfer of consumer products and services through online shopping or e-commerce marketplaces).

[15] Data transactions between a U.S. person and its subsidiary or affiliate located in (or otherwise subject to the ownership, direction, jurisdiction, or control of) a country of concern, that are ordinarily incident to and part of administrative or ancillary business operations, including (i) human resources; (ii) payroll, expense monitoring and reimbursement, and other corporate financial activities; (iii) paying business taxes or fees; (iv) obtaining business permits or licenses; (v) sharing data with auditors and law firms for regulatory compliance; (vi) risk management; (vii) business-related travel; (viii) customer support; (ix) employee benefits; and (x) employees' internal and external communications.

subject to a CFIUS action, telecommunications services, drug, biological product, and medical device authorization, and other clinical investigations and post-marketing surveillance data.

2. Potential Challenges that China Game Companies May Face

A. Game Data and Covered Data

The data collected in connection with the operation of a game is unlikely to involve any government-related data, but it may, to some extent, involve sensitive personal data, particularly covered personal identifiers, precise geolocation data, and personal financial data.

(1) Covered Personal Identifiers

A covered personal identifier means any listed identifier, which is any piece of data in the following data fields, in combination with (a) any other listed identifier from the following data fields,[16] or (b) other data disclosed by a transacting party pursuant to the transaction such that the listed identifier is linked or linkable to other listed identifiers or to other sensitive personal data.[17]

Data Field	Description
Government Identification Data	Full or truncated government identification or account number, such as a Social Security number, driver's license or State identification number, or passport number
Financial Account Data	Full financial account numbers or personal identification numbers associated with a financial institution or financial services company
Device Identifier Data	Device-based or hardware-based identifier, such as International Mobile Equipment Identity (IMEI), Media Access Control (MAC) address, or Subscriber Identity Module (SIM) card number
Demographic & Contact Data	Demographic or contact data, such as first and last name, birth date, birthplace, ZIP code, residential street or postal address, phone number, email address, or similar public account identifiers
Advertising Identifier Data	Advertising identifier, such as Google Advertising ID, Apple ID for Advertisers, or other mobile advertising IDs
Account Authentication Data	Account-authentication data, such as account username, account password, or an answer to a security question
Network Identifier Data	Network-based identifier, such as Internet Protocol ("IP") address or cookie data
Call Detail & Communications Data	Call-detail data, such as Customer Proprietary Network Information

[16] See Section 202.234 of the Final Rule.

[17] Covered persona identifier excludes (i) demographic or contact data that is linked only to other demographic or contact data, and (ii) network-based identifier, account-authentication data, or call-detail data that is linked only to other network-based identifier, account-authentication data, or call-detail data as necessary for the provision of telecommunications, networking, or similar service.

A significant portion of data collected by games falls under this category, such as device IDs, advertising IDs, account usernames and passwords, verification codes, phone numbers, email addresses, birthdates, IP addresses, or cookie data. These data are often collected, processed, and transferred in combination with one another, making it easy for them to be identified as covered personal identifiers.

(2) Precise Geolocation Data

Precise geolocation data refers to data, whether real-time or historical, that identifies the physical location of an individual or a device with a precision of within 1,000 meters. While most games may not collect precise geolocation data, certain augmented reality (AR) games, such as Pokémon Go, do collect this data. Additionally, some game operators collect precise geolocation data for advertising purposes, and certain social games that rank players within specific geolocations may also collect this data.

(3) Personal Financial Data

Personal financial data refers to data about an individual's credit, charge, or debit card, or bank account, including purchases and payment history. Game companies usually collect players' purchase history and payment card details, either directly or indirectly, to confirm payments, record purchase history, or resolve payment disputes and inquiries. Although game companies generally do not provide payment services or process payments directly for players, they may receive and store personal financial data from distribution platforms or third-party payment service providers.

B. Relevant Data Transactions

China game companies expanding into the U.S. market often establish Singapore-based publishing entities to distribute their games overseas. These entities act as data controllers, collecting game data directly from U.S. players. Such companies may engage U.S. or global service providers to assist with publishing and marketing efforts in the U.S. These efforts can include renting U.S.-based servers, working with distribution platforms to distribute the game, and engaging local marketing service providers for user acquisition campaigns or advertising activities.

(1) Data Collection

While the definition of data brokerage is broad, it explicitly excludes situations where the recipient collects or processes data directly from individuals to whom the collected or processed data is linked or linkable. Therefore, data transactions between a U.S. individual and the Singapore publishing entity in accordance with the game's terms of service and privacy policy, are not considered covered data transactions under the Final Rule and are not subject to relevant obligations. Additionally, any transactions between the Singapore publishing entity and its Chinese parent company are not subject to the Final Rule, as the U.S. person element is absent.

(2) Server Services

The Singapore publishing entity's engagement with a U.S.-based cloud server provider to host the game and store U.S. players' bulk sensitive personal data may appear to be a restricted transaction involving a vendor agreement. However, in this case, the Singapore entity is the data provider, and the U.S. server provider is merely the recipient. As mentioned earlier, this transaction would not be considered a covered data transaction, as the covered person already possesses the data.

(3) Distribution Platforms

The situation with distribution platforms, however, is quite different. Platforms such as Steam or the Epic Games Store for PC games, PlayStation and Xbox for console games, or Google Play and Apple for mobile games may collect user account information, advertising IDs (which may be regarded as covered personal identifiers), and purchase information (which may be considered personal financial data) directly from players. This data is then shared with the game developer or game publisher for game operation purposes. Such data transactions between a U.S. distribution platform and the Singapore entity may be considered data brokerage if the distribution platform provides a covered person with access to bulk sensitive personal data. However, transactions for revenue settlement purposes may be excluded, as the Final Rule considers the transfer of personal financial data or covered personal identifiers incidental to the purchase and sale of goods and services (such as the purchase, sale, or transfer of consumer products and services through online shopping or e-commerce marketplaces) an exempted transaction.[18]

(4) Advertising and Marketing Services

As illustrated in the example shared in Section 1.D(1)(a) above, when a China game company places ads on a mobile app or website operated by a U.S. person targeting U.S. users and accesses bulk sensitive personal data (such as a user's IP address and advertising ID), it constitutes a prohibited transaction. Similarly, marketing services provided by a U.S. vendor that grant a covered person access to bulk sensitive personal data of U.S. players may also fall under the scope of prohibited transactions if the data is accessed for advertising analysis purposes.

C. Compliance or Data Localization

The enforcement strategy of the DOJ regarding the Final Rule remains uncertain. In general, the compliance burden appears to fall on U.S. distribution platforms or advertising/marketing service providers (the "Responsible U.S. Parties") that collect and share bulk U.S. sensitive personal data with foreign entities related to China. Before the effective date of April 8, 2025, these Responsible U.S. Parties should consider undertaking a comprehensive mapping of their data flows. This process involves identifying all types of data being transferred, the parties involved, and the jurisdictions in which these parties operate. Additionally, thorough due diligence must be conducted on all foreign clients to determine whether any data transactions could be classified as covered data transactions.

[18] See Section 202.505(4) of the Final Rule.

A significant challenge lies in determining whether a foreign entity qualifies as a covered person. For companies incorporated in jurisdictions with transparent corporate registries, such as Singapore, verifying client shareholders may be relatively straightforward. However, if a company or any of its shareholders is incorporated in jurisdictions like the Cayman Islands or the British Virgin Islands—where shareholder information is confidential—it may be difficult, if not impossible, for the Responsible U.S. Party to verify the beneficial owners of such foreign entities. This lack of transparency poses substantial compliance risks, as Responsible U.S. Parties may inadvertently engage with entities that do not comply with the Final Rule.

If a Responsible U.S. Party is aware that a game originates from China, it may choose to withhold detailed personal data that could be classified as bulk sensitive personal data. Alternatively, a Responsible U.S. Party might require entering a service agreement with the U.S. subsidiary of the China game company to avoid the complex compliance issues. In this scenario, the Responsible U.S. Party would transfer the data to such U.S. subsidiary, which qualifies as a U.S. person under the Final Rule. As such, this transfer is not subject to the Final Rule, and if the US subsidiary needs to transfer such bulk sensitive personal data to its China parent company, then it will be subject to Final Rules. Given these complexities, the implementation of the Final Rule may present various practical challenges; thus, China game companies should closely monitor the requirements set by their U.S. partners.

China game companies can consider avoiding access to any bulk sensitive personal data altogether if it is not essential to the game's operation. However, if accessing such data is necessary, the company may consider establishing a U.S. entity and employing U.S.-based personnel to process and review the data from distribution or advertising platforms. If a covered person needs access to this data, it is recommended that they enter into a vendor agreement, ensuring the U.S. entity maintains sole control over the sensitive personal data and complies with the Final Rule's requirements for restricted transactions.

However, if the China game company establishes a U.S. entity and processes U.S. player data that qualifies as bulk sensitive personal data, any transactions between this U.S. entity and its Chinese parent, service providers, or individuals should be carefully considered. The presence of the U.S. entity introduces the U.S.-person element, and any access by a covered person to bulk sensitive personal data collected by the U.S. entity, as well as any vendor, employment, or investment agreements involving a covered person may constitute a covered data transaction.

In our previous article, WOW vs. TikTok – The New Data Wars, we highlighted how China's PIPL and strict data localization rules often prevent foreign companies from accessing local data from outside China, while the U.S. has struggled to control access to its own data, even when concentrated in a single company like TikTok. However, with the introduction of the Final Rule, the U.S. now has a legal tool comparable to China's PIPL—its own version of data localization. While China's framework broadly restricts foreign access to critical data and personal information, the U.S. approach is more targeted, blocking only specific countries of concern from accessing bulk sensitive personal data and government-related information.