The U.S. Preventing China and Other Countries from Access to U.S. Data

By Xun Yang | Louise He

The Justice Department of the U.S. issued and publicly posted the *Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons* ("PPPAD"), which is designed to address the "national-security risks posed by the continued efforts of countries of concern to access, exploit, and weaponize Americans' bulk sensitive personal and U.S. government-related data." Once the PPPAD becomes effective, it will further restrict the free flow of data, especially the data flow to China. This will, in turn, affect some of China's businesses.

I. Overview of the PPPAD

A. Background

With authority from Congress's International Emergency Economic Powers Act (IEEPA), President Biden issued Executive Order 14117 on February 28, 2024, to protect U.S. information and communications technology supply chains and sensitive data from foreign competitors. The Department of Justice (DOJ) released the PPPAD following the Executive Order's directions to protect information from technologically-driven exploitation by countries of concern.

The PPPAD was issued to address national security concerns about how six countries of concern may purchase and then use data on U.S. citizens in risky manners. Sensitive data, such as biometric, financial, and geolocation data, may reveal information that enables countries of concern to conduct activities harmful to the U.S., such as cyber-attacks, espionage, blackmail, and military enhancement. This rule aims to address the increased risk in countries of concern's data use in light of technological enhancements and the commercialization of useable data.

如果您需要本出版物的中文本，请联系:

Publication@llinkslaw. com

For more Llinks publications, please contact:

Publication@llinkslaw.com

B. Nature of the Rules

The PPPAD is regulated by the DOJ's National Security Division, a part of the U.S.'s executive branch, and implemented by its Foreign Investment Review Section (FIRS). Unlike congressional law, it will be implemented as an administrative law since it was issued due to directions from a Presidential Executive Order empowered by a Congressional Act.

C. Effectiveness

The PPPAD "will become effective 90 days after publication. Certain affirmative compliance obligations will be phased in with a larger effective date of 270 days after publication". This means the restrictions outlined within this rule will be effective 90 days after October 29, 2024, and the affirmative compliance obligations involving specific compliance responsibilities will be effective 270 days after October 29, 2024.

D. Application

PPPAD applies to all U.S. companies that engage in the specifically regulated activities. The DOJ estimates this rule would "directly financially impact approximately 3,000 companies engaged in data brokerage and an additional 1,500 firms that currently engage in restricted transactions involving government-related data and bulk U.S. sensitive personal data with covered persons." The regulated activities do not constitute a large portion of data transactions in the U.S. in general because this rule regulates specific types of data transactions relating to data access to the six specific countries of concern.

II. Obligations under the PPPAD

A. Data Covered

The PPPAD regulates or prohibits transactions involving "United States Government-related data or bulk U.S. sensitive personal data…[that] falls within a class of transactions that…may enable access by countries of concern or covered persons" to said data and "meets other criteria specified by the Order."

Two categories of U.S. Government-related data are regulated under the PPPAD despite the volume of the data and include "any precise geolocation data within geographic areas listed on the Department's public Government-Related Location Data List" and "any sensitive personal data marketed as linked to current or recent former U.S. Government employees or contractors."

The "bulk" threshold applies to data, regardless of processing through methods like anonymization, that exceeds certain thresholds during the 12 months prior to transactions. These thresholds are: (1) human genomic data on over 100 U.S. persons, and the three other covered categories of human 'omic data on over 1,000 U.S. persons, (2) biometric identifiers on over 1,000 U.S. persons, (3) precise geolocation data on over 1,000 U.S. devices, (4) personal health data and personal financial data on over 10,000 U.S. persons, (5) certain covered personal identifiers on over 100,000 U.S. persons, or (6) any combination of these data types that meets the lowest threshold for any category in the dataset.

Sensitive personal data, in this case, is defined as data that may link to U.S. individuals or groups of individuals and is categorized as “(1) certain covered personal identifiers; (2) precise geolocation data; (3) biometric identifiers; (4) human genomic data and three other types of human ‘omic data; (5) personal health data; and (6) personal financial data.” A few exclusions to sensitive personal data under those six categories of data exist, including publicly available information or data that does not identify specific individuals.

B. Concerned Countries and Cover Persons

The PPPAD prohibits or restricts data transferals to the following countries of concern and covered persons.

Countries of concern include China, Cuba, Iran, North Korea, Russia, and Venezuela.

Covered persons are defined as “(1) foreign entities that are 50 percent or more owned by a country of concern, organized under the laws of a country of concern, or have their principal place of business in a country of concern; (2) foreign entities that are 50 percent or more owned by a covered person; (3) foreign employees or contractors of countries of concern or entities that are covered persons; and (4) foreign individuals primarily resident in countries of concern.”

C. Prohibited Transactions

Two types of transactions are prohibited under the PPPAD. They are data brokerage and covered data transactions of “bulk human ‘omic data or human biospecimens” that allow countries of concern or covered persons to access bulk sensitive or government-related data.

Data brokerage stands for any commercial transaction involving the transferal of data that the data recipient did not collect directly, as defined “as the sale of data, licensing of access to data, or similar commercial transactions involving the transfer of data from any person (“the provider”) to any other person (“the recipient”), where the recipient did not collect or process the data directly from the individuals linked or linkable to the collected or processed data.” This definition of data brokerage defines the activity by its transactional nature and the result of the transaction instead of by the identity of the parties. In its responses to public comments, the DOJ confirms its intentions behind defining data brokerage as such and does not further restrict activities considered data brokerage by, for example, adding requirements involving monetary transactions, knowledge of sales, or the specific identity of the data provider.

D. Restricted Transactions

The PPPAD also restricts certain transactions involving vendors, employment, and non-passive investment agreements with countries of concern or covered persons. These transactions are required to meet security requirements developed by the Department of Homeland Security's Cybersecurity and Infrastructure Agency (CISA), such as cybersecurity measures.

Vendor agreements are defined under the PPPAD as the following: "any agreement or arrangement, other than an employment agreement, in which any person provides goods or services to another person, including cloud-computing services, in exchange for payment or other consideration." The DOJ is "tentatively considering" applying a strict standard and not granting exemptions to either of the discussed cases where vendor agreements involve parties related to countries of concerns where such involvement is unnecessary. The DOJ reasons that it does not consider such practices "reasonable and typical": "it does not believe that an employment agreement or a vendor agreement that gives a covered person access to U.S. persons' bulk sensitive personal data is a reasonable and typical practice in providing the underlying financial services that do not otherwise involve covered persons or a country of concern."

E. Exempted Transactions

The PPPAD also lists transactions that are exempt from prohibitions and regulations, including:

a) Personal communications that do not transfer anything of value; the import or export of informational materials involving expressive materials; and travel information, including data about personal baggage, living expenses, and travel arrangements;
b) Official U.S. Government activities;
c) Financial services if they involve transactions ordinarily incident to and part of providing financial services;
d) Corporate group transactions between a U.S. person and its foreign subsidiary or affiliate, if they are ordinarily incident to and part of routine administrative or business operations;
e) Transactions required or authorized by Federal law or international agreements;
f) Investment agreements after they have become subject to certain mitigation or other action taken by the Committee on Foreign Investment in the United States (CFIUS), if CFIUS explicitly designates them as exempt;
g) Transactions that are ordinarily incident to and part of the provision of telecommunications services;
h) Data transactions with countries of concern or covered persons involving drug, biological product, device, or combination product approvals or authorizations if the data transactions involve "regulatory approval data" necessary to obtain or maintain regulatory approval;
i) Other clinical investigations and post-marketing surveillance data if the transactions are part of clinical investigations regulated by the FDA.

III. Impact on Chinese businesses

While it is still too early to assess how the PPPAD will affect Chinese businesses with operations in the U.S. or those that operate on data generated from the U.S., it is clear that the PPPAD will impact Chinese companies' ability to acquire or access data generated in the U.S.

The normal course of financial business may remain unaffected, as the PPPAD exempts the transfer of financial data that is ordinarily incident to and part of providing financial services. However, the study of the financial behavior of U.S. residents will be impacted.

Data transfers necessary for completing e-commerce transactions will not be affected, as transactional data is processed as needed to complete online transactions. However, the collection of data for studying the expenditure behaviors of U.S. citizens will be impacted.

The "big data" business is likely to be heavily impacted, as it often involves the transfer of large volumes of data without ordinary transactions. This means that industries such as those involving the development of artificial intelligence and research on autonomous driving will need to closely monitor the impact of the PPPAD.

If you would like to know more information about the subjects covered in this publication, please contact:

Xun Yang
+86 21 3135 8799
xun.yang@llinkslaw.com

SHANGHAI

19F, ONE LUJIAZUI
68 Yin Cheng Road Middle
Shanghai 200120 P.R.China
T: +86 21 3135 8666
F: +86 21 3135 8600

BEIJING

30F, Central Tower, China Overseas Plaza, 8 Guanghuadongli,
Chaoyang District
Beijing 100020 P.R.China
T: +86 10 5081 3888
F: +86 10 5081 3866

SHENZHEN

18F, China Resources Tower
2666 Keyuan South Road,
Nanshan District
Shenzhen 518063 P.R.China
T: +86 755 3391 7666
F: +86 755 3391 7668

HONG KONG

Room 3201, 32/F, Alexandra House
18 Chater Road
Central, Hong Kong
T: +852 2592 1978
F: +852 2868 0883

LONDON

1/F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

www.llinkslaw.com

Wechat: LlinksLaw

WE LINK LOCAL LEGAL INTELLIGENCE WITH THE WORLD