Simpson Thacher

Report from Washington

New Regulatory Regime to Strictly Restrict Access to U.S. Sensitive Personal Data from China and Other Countries of Concern

December 16, 2024

Overview

The Department of Justice ("DOJ") has issued a Notice of Proposed Rulemaking ("NPRM") to implement Executive Order 14117 on *Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern*. The proposed rules, if adopted, would create the most comprehensive regulatory regime yet to restrict transfer of U.S. sensitive personal data not only through brokerage transactions but also in many other types of transactions relating to China or other countries of concern.

At a high level, the proposed rules would prohibit or restrict U.S. persons from knowingly directing or engaging in defined classes of transactions that allow persons in countries of concern or those otherwise deemed a "covered person" access to enumerated categories of sensitive data–specifically, bulk U.S. sensitive personal data and U.S. government-related data.

We expect the regulations, once finalized, will have significant implications for many companies or businesses that have access to bulk U.S. sensitive personal data or U.S. government-related data. The regulations will regulate not just data brokerage agreements, but also vendor, employment, and investment agreements. As a result, virtually all companies with sensitive U.S. data, even those who never buy or sell data, will be required to review their employment, vendor, and investor relationships to ensure compliance with applicable prohibitions and restrictions, including those governing employees, service providers and shareholders organized, based or resident in China and other countries of concern. The new regulations will also apply to service providers with access to data that they host or process for third parties. Thus, a wide range of companies with access to sensitive data—such as datacenter operators and cloud-service providers—should carefully evaluate the NPRM and take steps to ensure they are prepared to be fully compliant when the regulations are finalized.

We highlight below a few observations about the expansive scope of this regulatory regime before providing a summary of the key elements of the NPRM.

Key Observations Regarding the Scope of Proposed Rules

1. **The proposed rules apply whenever a U.S. person has "access" to covered sensitive data, and "access" is defined broadly**. Subject to limited exceptions, the rules would prohibit or restrict any U.S. person with access to covered sensitive data, which includes both bulk U.S. sensitive personal data and also government-related data regardless of volume, from sharing, transferring or providing access to that sensitive data to any covered person, generally including any person from a country of concern, like a Chinese or Russian resident or company (more detailed definition in our summary below). Notably, "access" is defined to include not only the ability to obtain but also to "divert, release, affect" in any way the covered data whether they are "anonymized, pseudonymized, de-identified, or encrypted." The DOJ explicitly declined to remove "divert" from the definition despite public comments about the facially expansive scope. Defined as such, companies with access to data that they host, store, or transfer—even if that data is encrypted or secured by their customers and inaccessible to them—are arguably within the scope of the NPRM. Additionally, commentary accompanying the NPRM explicitly contemplates that data centers and cloud-service providers would need to comply with the proposed rules when certain conditions exist, such as when the knowledge standard is met, which we will discuss below in #5.

2. **The proposed rules restrict a wide range of transactions commonly present in daily corporate operations—including engaging vendors, hiring foreign nationals, and seeking non-passive investors—when there is a nexus to China or other countries of concern**. The proposed new rules would impose restrictions on a wide range of other more common transactions including (i) vendor agreements, (ii) employment agreements, and (iii) non-passive investment agreements. Each of those would be restricted if they involve any type of covered sensitive data. Specifically, U.S. persons are permitted to engage in those types of transactions (to the extent they involve access to sensitive data) only when certain security requirements adopted by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) are satisfied, which will be discussed below in #4.

   In practice, any U.S. person who has access to covered sensitive data should conduct due diligence with respect to all its vendor relationships, employee and contractor relations, and capital structures to assess its compliance obligations before the new rules take effect.

3. **The proposed rules restrict investments by covered persons into U.S. entities or U.S. real estate that involve covered sensitive data, with an exception for "passive investment."** As noted above in #2, the new rules impose restrictions on sensitive data transactions that involve an investment agreement, that is any "agreement or arrangement in which any person, in exchange for payment or other consideration, obtains direct or indirect ownership interests in or rights in relation to (1) real estate located in the United States or (2) a U.S. legal entity."

   However, "passive investments" are explicitly excluded from the scope. Excluded passive investments include not only investments into publicly traded securities or SEC-registered index or mutual funds, but

also certain limited partner (LP) investments in pooled investment funds, provided that the covered person holds less than 10% in total voting and equity interest and is not afforded any rights "beyond those reasonably considered to be standard minority shareholder protections." Specifically, to qualify for passive investments, the LP contribution must be "solely capital and the [LP] cannot make managerial decisions" or be "responsible for any debts beyond its investment, and does not have the formal or informal ability to influence or participate in the fund's or a U.S. person's decision-making or operations."

Effectively, this means that if a fund has any China-based LP investor, the fund must make sure its LP interest falls below 10% and is entirely passive in terms of the LP rights afforded to such investor, were the fund to make investments into U.S. companies or real estate that have access to covered sensitive data. If adopted, the proposed rules will thus place an additional compliance burden on U.S. private equity firms, to the extent they have LP investors from countries of concern. The private equity firms should undertake due diligence to assess whether the target business has access to covered sensitive data, and if so, evaluate whether the LP exemption is satisfied. The proposed rules contemplate potential overlaps with CFIUS. If an investment agreement is already subject to a CFIUS action, the restrictions under the proposed rules would not apply.

4. **U.S. persons must implement robust compliance measures when engaging in restricted transactions.** As noted, a U.S. person cannot engage in the above-described restricted transactions, including those involving vendor, employee or investment agreements, unless it meets the CISA security requirements. The CISA has proposed both organizational and system-level requirements as well as data-level requirements:

    - Organizational and system-level requirements cover documentation and policy requirements, access controls, and data risk assessments. Specific measures include, among others, (i) implementing organizational cybersecurity policies, practices, and requirements, (ii) designating an individual responsible for cybersecurity, (iii) patching vulnerabilities quickly and routinely, (iv) implementing logical and physical access controls to restrict access to covered sensitive data, and (v) conducting data risk assessments to evaluate the sufficiency of data-level requirements.
    - Data-level requirements focus on minimizing exposure to covered sensitive data through measures including, among others, (i) adopting data minimization and data masking strategies, such as implementing a data retention and deletion policy, (ii) applying encryption during the restricted transactions, and (iii) leveraging privacy-enhancing technologies to process covered data.

    In addition, a U.S. company engaging in any restricted transaction must also adopt a written data compliance program, conduct annual third-party audits, and maintain relevant records for at least 10 years. Detailed compliance and reporting obligations are included in our summary of key terms at the end.

5. **The proposed rules adopt a knowledge standard for imposing liability, protecting U.S. persons who conduct reasonable due diligence.** The proposed rules would not adopt a strict liability regime and instead prohibit or restrict transactions only when the U.S. person had actual or

constructive knowledge that the transaction was prohibited or restricted. Conducting due diligence, therefore, can help shield U.S. persons from liability. This construct is similar to other new rules involving transactions involving China, like the outbound investment program recently promulgated by the U.S. Treasury Department (please see our previous client alert for more details). The DOJ indicated that it will take into account all relevant facts and circumstances when determining if a U.S. person has actual or constructive knowledge. Commentary to the NPRM clarifies that U.S. persons are not required to conduct diligence on the employment practice of counterparties (that is, whether the counterparty will hire covered persons who may in turn have access to covered sensitive data). Nevertheless, U.S. persons who transact in or give access to covered sensitive data to counterparties will still be well-served to consider including contractual representations and warranties in their agreements with counterparties.

The NPRM commentary addresses under what circumstances an intermediary service provider, such as a cloud-service provider, could be found liable under the proposed rules. If a U.S. entity merely stores encrypted data on behalf of a U.S. customer and does not have access to the encryption key (or has access only to an emergency backup encryption key usable only at the customer's explicit request), and if the U.S. entity is reasonably unaware of the kind or volume of data involved, the U.S. entity generally would not meet the knowledge standard of the proposed rules. By contrast, if a cloud-service provider specializes in storing and processing healthcare data and reasonably should have known that its customers' encrypted healthcare data are covered sensitive data, the cloud-service provider would have knowledge if engaging in any prohibited or restricted transaction. These examples show that mere service providers are at risk of running afoul of the proposed rules even absent actual knowledge of the specific nature of the data.

6. **Covered persons generally exclude individuals physically in the U.S. and entities incorporated in the U.S., which means transactions solely between U.S. persons or entirely within the U.S. are generally not covered.** We include a more detailed definition of "covered person" in our summary of key terms below, but it is worth noting that the proposed rules do not categorically define all Chinese nationals or all Chinese-owned companies as covered persons. Individuals physically in the U.S. or entities incorporated in the U.S. are not covered persons, unless they are separately designated by the DOJ. In other words, the proposed rules impose no restriction on transactions solely between U.S.-incorporated entities or entirely within the United States, unless any party is separately designated. A U.S. company, for example, can hire a Chinese national residing in the United States to work on covered sensitive data.

   A U.S.-based company can also transfer covered sensitive data to its foreign branch office in China without violating the rule (assuming no covered person within or outside the company is gaining access to the sensitive data). By contrast, a U.S. company can transfer covered sensitive data to its subsidiary or affiliate in China only when certain conditions for intra-corporate transfers are met. See #6 below.

   However, the proposed rules make clear that any attempt to evade or avoid the proposed rule would be a violation. For example, the commentary notes that a data broker cannot invite a Chinese national to travel

to the United States and transfer the covered sensitive data to him while he is in the states, knowing that he will bring the data back to China. While the transfer itself is not covered by the rule because the individual is physically in the United States, the transaction as a whole has the purpose of evading the regulations and is thus prohibited.

7. **The definitions of categories of covered sensitive data are broad and complex**. Categories of covered sensitive data, including U.S. government-related data and bulk U.S. sensitive personal data, are listed below in our summary of key terms. Given the limited space of this alert memorandum, we have not provided the full definition for each data category, but we would note that many of these definitions are broad, ambiguous and complex to navigate.

   For instance, "precise geolocation data" is defined to include data identifying location within 1,000 meters, which could be easily met for many devices. A similarly broad scope is also present in the definition for personal financial and healthcare data. In addition, "personal identifiers" requires various listed identifiers to be linked to be covered, which makes assessment difficult in many cases. Companies having reason to believe that they may have access to any of the categories of sensitive data should consider engaging advisors, as needed, to undertake an appropriate review.

8. **Intra-corporate group transactions may fall within defined exemptions, but case-by-case assessment is required to determine applicability**. Corporate group transactions between a U.S. person and its foreign subsidiary or affiliate are exempted if "they are ordinarily incident to and part of routine administrative or business operations." The NPRM commentary notes that this intra-corporate group exemption applies to routine administrative conduct such as sharing employees' covered personal identifiers for HR purposes, payroll transactions like salary payment to overseas employees or contractors, or sharing data for regulatory compliance and risk management. By contrast, examples in the NPRM indicate that this exemption would not apply to sharing data with foreign subsidiaries in China or another country of concern for the purpose of conducting research and developing software. Many intra-corporate group transactions may not be neatly categorized as within or outside the enumerated exemption.

9. **U.S. persons are not allowed to "direct" a prohibited transaction by a non-U.S. person, and non-U.S. persons may also be liable**. The proposed rules place primary liability on U.S. persons to comply with the restrictions on various data transactions we discussed above. U.S. persons are also prohibited from "directing" a non-U.S. person to engage in a data transaction that would be prohibited if engaged in by a U.S. person. Thus, U.S. parent companies, executives, principals or shareholders that have control over non-U.S. entities should be aware of these obligations.

   Non-U.S. persons may face liability under the proposed rules, too. Similar to the U.S. sanctions regulatory regime administered by the Office of Foreign Assets Control ("OFAC"), non-U.S. persons are prohibited from causing or conspiring to cause U.S. persons to violate the proposed rules and are prohibited from engaging in conduct that evades the rules. If enforcement precedents by OFAC provide any guidance, DOJ

may bring enforcement actions against foreign persons where there is a U.S. nexus to the transaction, such as the involvement of a U.S. counterparty or intermediary.

Key Elements of the NPRM

U.S. person	Defined as "any United States citizen, national, or lawful permanent resident; any individual admitted to the United States as a refugee under 8 U.S.C. 1157 or granted asylum under 8 U.S.C. 1158; any entity organized solely under the laws of the United States or any jurisdiction within the United States (including foreign branches); or any person in the United States."
Countries of concern	China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia, and Venezuela
Covered persons	(1) 50 percent or more owned by a country of concern, organized or chartered under the laws of a country of concern, or has its principal place of business in a country of concern; (2) 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. Or anyone the DOJ designates.
Prohibited transactions	Two classes of prohibited transactions (only if involving access to government data or bulk U.S. sensitive data): 1. ***data brokerage***—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. 2. any covered transactions (*i.e.*, brokerage or any of the three restricted transactions described below) involving access to ***bulk human genomic data or biospecimens*** from which such data can be derived.
Restricted transactions	The following three categories of restricted transactions are permitted ***only if*** they meet security requirements developed by the Department of Homeland Security's Cybersecurity and Infrastructure Agency (CISA). 1. *Covered data transaction (*i.e.*, only if involving access to government data or bulk U.S. sensitive data) involving* ***vendor agreement***—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. 2. *Covered data transaction involving* ***employment agreement***—any agreement or arrangement in which an individual, other than as an independent contractor, performs work or performs job functions directly for a person in exchange for payment or other consideration, including employment on a board or committee, executive-level arrangements or services, and employment services at an operational level. 3. *Covered data transaction involving* ***non-passive investment agreement***—any agreement or arrangement in which any person, in exchange for payment or other consideration, obtains direct or indirect ownership interests in or rights in relation to (1) real estate located in the United States or (2) a U.S. legal entity. But certain passive investments are excluded, including investment into a publicly traded security, or security offered by an SEC-registered investment company, certain LP investments, provided that the investment gives the covered person less than 10% voting and equity interest.

Government-related data	**No bulk threshold** for the following two categories of government-related data: 1. any precise geolocation data (precision within 1 km) within geographic areas listed on the DOJ's public Government-Related Location Data List; 2. any sensitive personal data marketed as linked to current or recent former U.S. Government employees or contractors (including the military and intelligence community).
Bulk U.S. sensitive personal data	The proposed rules would establish the following bulk thresholds: • human genomic data on over 100 U.S. persons, • biometric identifiers on over 1,000 U.S. persons, • precise geolocation data on over 1,000 U.S. devices (precision within 1 km), • personal health data on over 10,000 U.S. persons, • personal financial data on over 10,000 U.S. persons, • certain covered personal identifiers on over 100,000 U.S. persons (examples include demographic or contact data (*e.g.*, first and last name, birthplace, ZIP code, address, phone number, email address and similar public account identifiers) that are linked to government ID numbers, financial account numbers, device/hardware-based identifier, advertising identifiers, account-authentication data (*e.g.*, username, password), network-based identifier/IP address, or call-detail data), • or any combination of these data types that meets the lowest threshold for any category in the dataset. "Bulk" refers to any amount of sensitive personal data, whether the data is anonymized, pseudonymized, de-identified, or encrypted, that exceeds certain thresholds in the aggregate over the preceding 12 months before a covered data transaction.
Exempted transactions	Data transactions involving the following are exempted: 1. **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; 2. Official U.S. Government activities; 3. **Financial services** if they involve transactions ordinarily incident to and part of providing financial services; 4. **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; 5. Transactions required or authorized by Federal law or international agreements; 6. Investment agreements after they have become subject to certain mitigation or other action taken by the CFIUS if CFIUS explicitly designates them as exempt; 7. Transactions that are ordinarily incident to and part of the provision of **telecommunications services**, including international calling, mobile voice, and data roaming; 8. Drug, biological product, and medical device authorizations if the data transactions involve "regulatory approval data" necessary to obtain or maintain regulatory approval in a country of concern; 9. Other **clinical investigations and post-marketing surveillance data** if regulated by FDA.
Licensing	DOJ authorized to issue ***general*** licenses and ***specific*** licenses.
Compliance & reporting requirements	Affirmative compliance obligations as conditions for U.S. persons that engage in a restricted transaction: • implement a comprehensive compliance program, which would include implementing risk-

based procedures to verify and log data flows, sensitive personal and government-related data types and volume, transaction parties' identities, data end-use and transfer methods, and vendor identities;

- establishing written policies on data security and compliance that are certified annually by a responsible officer or employee, conducting and retaining the results of an annual audit by an independent auditor to verify compliance with the security requirements established by CISA, and maintaining and certifying the accuracy of records of relevant documentation for 10 years.

Reporting requirements for certain persons:

- annual reports filed by U.S. persons engaged in restricted transactions involving cloud computing services, if they are 25% or more owned, directly or indirectly, by a country of concern or covered person;
- reports by any U.S. person that has received and affirmatively rejected an offer from another person to engage in a prohibited transaction involving data brokerage;
- reports by U.S. persons engaged in a covered data transaction involving data brokerage with a foreign non-covered person if the U.S. person knows or suspects that the foreign counterparty is violating the restrictions on resale and onward transfer to countries of concern or covered persons; and
- reports by U.S. persons invoking the exemption for certain data transactions that are necessary to obtain or maintain regulatory approval to market a drug, biological product, device, or a combination product in a country of concern.

Penalty

Violations can result in civil and criminal penalties.

- up to $368,136 or twice the amount of the transaction involved, whichever amount is greater.
- willful violations can lead to criminal fines up to one million dollars ($1,000,000) and up to 20 years imprisonment.

For further information regarding this memorandum, please contact one of the following authors:

WASHINGTON, D.C.

Abram J. Ellis
+1-202-636-5579
aellis@stblaw.com

Malcolm J. (Mick) Tuesley
+1-202-636-5561
mick.tuesley@stblaw.com

Mark B. Skerry
+1-202-636-5523
mark.skerry@stblaw.com

Ryan D. Stalnaker
+1-202-636-5992
ryan.stalnaker@stblaw.com

NEW YORK CITY

George S. Wang
+1-212-455-2228
gwang@stblaw.com

David H. Caldwell
+212-455-2612
dcaldwell@stblaw.com

Daniel S. Levien
+1-212-455-7092
daniel.levien@stblaw.com

BEIJING

Shuhao Fan
+86-10-5965-2987
shuhao.fan@stblaw.com

Xue Feng
+86-10-5965-2999
xue.feng@stblaw.com