Simpson Thacher

# Report from Washington

## New Regulations Restrict Access to U.S. Sensitive Personal Data by China and Other Countries of Concern

April 8, 2025

### Overview

Today, the Department of Justice's ("DOJ") final rule implementing Executive Order 14117 on *Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern* (the "Final Rule") took effect, creating the most comprehensive regulatory regime yet to restrict the transfer of, and access to, U.S. sensitive personal data. The Final Rule was issued in December of last year and regulates transfers of U.S. sensitive personal data through data brokerage transactions and many other types of transactions relating to China (including Hong Kong and Macau) or other countries of concern (Russia, Iran, North Korea, Cuba, and Venezuela). The Final Rule will have significant implications for U.S. persons engaging in international data transfers and will be particularly relevant to data-driven businesses, from life sciences and health data companies to data center operators and cloud-service providers.

At a high level, the Final Rule prohibits 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.

The Final Rule will have significant implications for many companies that have access to bulk U.S. sensitive personal data or U.S. government-related data. The Final Rule regulates not just data brokerage, 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 Final Rule 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 U.S. data should carefully evaluate the Final Rule and prepare to comply with the relevant requirements.

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

## Key Observations Regarding the Scope of the Final Rule

1. **The Final Rule applies whenever a U.S. person has "access" to covered sensitive data, and "access" is defined broadly**. Subject to limited exceptions, the rules 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). "Access" is defined to include logical or physical access, including the ability to read or view, in any form, including through IT systems. 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 Final Rule. Additionally, commentary accompanying the Final Rule explicitly contemplates that data centers and cloud-service providers would need to comply with the Final Rule when certain conditions exist, such as when the knowledge standard is met, which we will discuss below in #5.

2. **The Final Rule restricts 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 Final Rule not only prohibits data brokerage but also imposes 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. Note, however, that it is ambiguous under some circumstances whether a particular relationship should be categorized as restricted vendor agreement or prohibited data brokerage.

   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 ensure compliance with the Final Rule.

3. **The Final Rule restricts 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 Final Rule imposes 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 or private entity, 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. As a result, the Final Rule will 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 Final Rule contemplates certain overlaps with CFIUS. If an investment agreement is already subject to a CFIUS action, the restrictions under the Final Rule 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. In tandem with the publication of the Final Rule, CISA published the security requirements on January 8, 2025, which includes both organizational and system-level requirements as well as data-level requirements:

   a. 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.

   b. 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, by October 6, 2025, 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. These additional obligations, to be clear, are separate and independent from the CISA requirements. Effective on April 8, 2025, no restricted transaction may be taken unless the U.S. company complies with the CISA security requirements. Detailed compliance and reporting obligations are included in our summary of key terms at the end.

5. **The Final Rule adopts a knowledge standard for imposing liability, protecting U.S. persons who conduct reasonable due diligence.** The Final Rule does not adopt a strict liability regime and instead prohibits or restricts 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 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. U.S. persons who transact in or give access to covered sensitive data to counterparties will be well-served to consider including contractual representations and warranties in their agreements with counterparties.

   The Final Rule commentary addresses under what circumstances an intermediary service provider, such as a cloud-service provider, could be found liable under the Final Rule. 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 Final Rule. 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 Final Rule 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 Final Rule does 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 Final Rule imposes no restriction on transactions solely between U.S.-incorporated entities or entirely within the U.S., unless any party is separately designated. A U.S. company, for example, can hire a Chinese national residing in the U.S. 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 #9 below.

However, the Final Rule makes clear that any attempt to evade or avoid the rule would be a violation. For instance, as illustrated in an example to the Final Rule, a data broker cannot invite a Chinese national to travel to the U.S. and transfer the covered sensitive data to him while he is in the U.S., 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 U.S., 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 and have significant implications for companies that transfer and access health data**. 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. U.S. sensitive personal data is broadly defined to include personal identifiers, precise geolocation data, biometric identifiers, human 'omic data, personal health data, and personal financial data, as well as any combination thereof. Many of the data categories are broad, ambiguous and complex to navigate. For instance, "precise geolocation data" is defined to include both real-time and historical data that identifies the location of an individual or a device 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 health data.

   Notably, the definition of "personal health data" includes extensive information such as physical measurements; health attributes (*e.g.*, vital signs, symptoms, allergies); logs of exercise habits; diagnostic, intervention, and treatment history; immunization data; test results; data on reproductive and sexual health; and data on the use or purchase of prescribed medications. Health companies that transfer and access health data will need to assess what health data they transfer and access to determine if they are subject to this new regulatory regime, which does not track commonly-used definitions of health information in current U.S. health privacy laws and regulations, such as "individually identifiable health information" under the Health Insurance Portability and Accountability Act ("HIPAA") Privacy Rule or "personal health records" ("PHR") and "PHR identifiable health information" under the Federal Trade Commission Health Breach Notification Rule.

   In addition, a standalone "personal identifier" in isolation does not constitute sensitive data. A "personal identifier" must be linked to other listed identifiers 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. **The Final Rule contains two exemptions of vital importance for pharmaceutical, biotechnology, medical device, and life sciences companies.**

We term these exemptions the "Drug Approval Exemption" and the "Clinical Exemption."

The Drug Approval Exemption provides an exemption with respect to transactions involving "regulatory approval data" that are "necessary to obtain or maintain regulatory authorization or approval to research or market a drug, biological product, device, or a combination product" (hereinafter, "covered product"). Defined as such, there are two levels of conditions to be met before the Drug Approval Exemption can apply. Before the Drug Approval Exemption can apply, there are two levels of conditions that must be met: (1) data-level conditions; and (2) transaction-level conditions. First, with respect to data-level conditions, regulatory approval data must meet each prong of the definition of "regulatory approval data," below. The Final Rule's reliance on cross-references to U.S. Food and Drug Administration ("FDA") regulations for determinations of what has been de-identified or pseudonymized and discussion of the purposes for which the data is used with respect to approval and research make the analysis of which data are covered much different than a typical U.S. health privacy regulation. Second, with respect to transaction-level conditions, the Drug Approval Exemption requires that the transaction as a whole be "*necessary* to obtain or maintain regulatory authorization or approval to research or market a [covered product]." For example, if a U.S. company engages a vendor in a country of concern to store and organize regulatory approval data but such activities are not mandated by local law, the transaction with the vendor would *not* be considered "necessary" for obtaining regulatory approval and hence *not* qualify for the Drug Approval Exemption.

The Clinical Exemption applies to data transactions that are "ordinarily incident to and part of": (1) certain drug and device clinical investigations regulated *by the FDA*, or clinical investigations that support FDA applications for research or marketing permits for covered products or infant formula; or (2) the collection or processing of clinical care data indicating real-world performance or safety of products, or of postmarketing surveillance data, provided the collection and processing is necessary to support or maintain FDA authorization and provided the data is de-identified or pseudonymized consistent with FDA regulations. To fall within the scope of the Clinical Exemption, if the clinical investigation is not conducted pursuant to certain FDA statutory provisions regarding investigational new drugs and investigational new devices listed in the Final Rule, then the clinical investigation must support an application to FDA for research or marketing of a covered product or infant formula. While there is no definition for "ordinarily incident to and part of," the phrase indicates that this exemption covers only data transactions that are routine, inherent, and directly connected to the specified FDA-regulated clinical investigations, and not, for example, data transactions involving real-world performance data that are not necessary to maintain an FDA authorization, such as a "local-for-local" study or clinical trial conducted in a country of concern to support an application for approval by that country's regulators. Transactions falling outside these characterizations may fall outside of the Clinical Exemption.

9. **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 Final Rule 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 Final Rule 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, in particular in light of the undefined but vague scope of "ordinarily incident to."

10. **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 Final Rule places 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 Final Rule, 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 Final Rule 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. By way of an example, the DOJ specifically notes that a non-U.S. company has caused a U.S. company to violate the data brokerage prohibition by developing a mobile app for the U.S. company and knowingly incorporating tracking pixels or software development kits that transfer covered sensitive data to a country of concern or covered person.

## Key Elements of the Final Rule

| | |
|---|---|
| **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, individually or in the aggregate, by one or more countries 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;<br>(2) 50 percent or more owned, individually or in the aggregate, by one or more covered persons;<br>(3) foreign employees or contractors of countries of concern or entities that are covered persons; and<br>(4) foreign individuals primarily resident in countries of concern.<br>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):<br>1. ***data brokerage***—defined as the sale of data, licensing of access to data, or similar commercial transactions, excluding an employment agreement, investment agreement, or a vendor agreement, 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.<br>2. Any covered transactions (*i.e.*, brokerage or any of the three restricted transactions described below) involving access to ***bulk human 'omic 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).<br>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.<br>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.<br>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 U.S. 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:<br>1. any precise geolocation data (precision within 1 km) within geographic areas listed on the DOJ's public Government-Related Location Data List;<br>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 Final Rule would establish the following bulk thresholds:<br>• human genomic data on over 100 U.S. persons,<br>• human 'omic data on over 1,000 U.S. persons<br>• biometric identifiers on over 1,000 U.S. persons,<br>• precise geolocation data on over 1,000 U.S. devices (precision within 1 km),<br>• personal health data on over 10,000 U.S. persons,<br>• personal financial data on over 10,000 U.S. persons,<br>• 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),<br>• 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 the abovementioned thresholds in the aggregate over the preceding 12 months before a covered data transaction. |
| **Exempted Transactions** | Data transactions involving the following are exempted:<br>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;<br>2. Official U.S. Government activities;<br>3. **Financial services** if they involve transactions ordinarily incident to and part of providing financial services;<br>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;<br>5. Transactions required or authorized by Federal law or international agreements;<br>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;<br>7. Transactions that are ordinarily incident to and part of the provision of **telecommunications services**, including international calling, mobile voice, and data roaming;<br>8. Drug, biologic, medical device, and combination product regulatory authorizations if the data transactions involve "**regulatory approval data**" necessary to obtain or maintain regulatory authorization or approval to research or market such covered products (the "Drug Approval Exemption");<br>9. Data ordinarily incident to and part of certain **clinical investigations** or ordinarily incident to and part of the collection or processing of certain **clinical care data** or **post-marketing surveillance data** if necessary to support or maintain FDA authorization (the "Clinical Exemption"). |
| **Regulatory Approval Data** | Sensitive personal data that:<br>1. Has been de-identified or pseudonymized consistent with FDA regulations;<br>2. Is required by a regulatory entity (whether in a third country or in a country of concern) to be submitted to obtain or maintain authorization or approval to research or market a covered product; and<br>3. That is reasonably necessary for the relevant regulator (whether in a third country or in the country of concern) to assess the safety and effectiveness of the covered product. |
| **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:<br>• implementing a comprehensive compliance program, which would include 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, and establishing written policies on data security and compliance that are certified annually by a responsible officer or employee;<br>• 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.<br>Reporting requirements for certain persons:<br>• 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;<br>• 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;<br>• reports by U.S. persons invoking the exemption for certain data transactions that involve sensitive personal data that is "**regulatory approval data**" and that are necessary to obtain or maintain regulatory approval or authorization to market a drug, biologic, medical device, or a combination product or to research a drug, biologic, device or combination product; and<br>• reports by U.S. persons invoking the exemption for certain data transactions that are ordinarily incident to and part of (1) **clinical investigations** regulated by the FDA or clinical investigations that support applications to the FDA for research or marketing permits for drugs, biologics, devices, combination products, or infant formula, or (2) the collection or processing of **clinical care data** indicating real-world performance or safety of products, or the collection or processing of **post-marketing surveillance data** (including pharmacovigilance and post-marketing safety monitoring), and necessary to support or maintain authorization by the FDA. |
| **Penalty** | Violations can result in civil and criminal penalties.<br>• up to $368,136 or twice the amount of the transaction involved, whichever amount is greater.<br>• willful violations can lead to criminal fines up to one million dollars ($1,000,000) and up to 20 years imprisonment. |
| **Effective Date** | While the bulk of the Final Rule takes effect April 8, 2025, certain compliance & reporting requirements noted above will take effect on October 6, 2025, including:<br>• Implementing a data compliance program that sets forth relevant due diligence procedures;<br>• Conducting an annual audit that examines the U.S. persons' restricted transactions, data compliance program, record-keeping practices, and security requirements implemented;<br>• Filing of annual reports 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; and<br>• Filing of reports by any U.S. person that has received and affirmatively rejected an offer to engage in a prohibited transaction involving data brokerage. |

For further information regarding this report, 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

**Vanessa K. Burrows**
+1-202-636-5891
vanessa.burrows@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

**Jacob Madden**
+1-212-455-3283
jacob.madden@stblaw.com

BEIJING

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

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