Fortifying US Data: Proposed Rule Would Establish a New Regime To Restrict or Prohibit Certain Data Transactions With Countries of Concern

Skadden

December 17, 2024

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

Brian J. Egan
Partner / Washington, D.C.
202.371.7270
brian.egan@skadden.com

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

Tatiana O. Sullivan
Counsel / Washington, D.C.
202.371.7063
tatiana.sullivan@skadden.com

Alyssa R. Domino
Associate / Washington, D.C.
202.371.7139
alyssa.domino@skadden.com

One Manhattan West
New York, NY 10001
212.735.3000

1440 New York Ave., NW
Washington, DC 20005
202.371.7000

On October 29, 2024, the U.S. Department of Justice (DOJ) published a proposed rule (Proposed Rule) that would restrict or prohibit certain transactions with China, Russia and other countries of concern involving U.S. sensitive personal data or U.S. government-related data (Data Risk Regime). DOJ has not announced its planned timing for finalizing the Proposed Rule, but the final rule will likely not come into effect before the end of the Biden administration. While we believe it is likely that the Trump administration will support some version of the policies in the Proposed Rule, it is not clear whether the incoming administration will seek to make significant changes to the Proposed Rule before it is finalized.

The Proposed Rule, which was issued pursuant to Executive Order (EO) 14117, follows DOJ's March 2024 advanced notice of proposed rulemaking (ANPRM) on the same subject, which is covered in our prior alert ("Commerce Department Seeks Comment on Restrictions on 'Connected Vehicle' Components From 'Foreign Adversaries,'" March 4, 2024). The Proposed Rule is designed to restrict the passage of certain types of bulk data and government-related data from U.S. persons to China and Russia, among other countries, to address U.S. government concerns related to counterintelligence and the development of AI capabilities. While the Proposed Rule does not cover all the personal data typically captured under data privacy regulations, it nonetheless covers a broad range. The Data Risk Regime created in the Proposed Rule is expected to impact numerous market sectors, such as data brokers, health care providers, financial service providers, insurance companies, internet service providers, online and brick-and-mortar retail chains, schools, "smart product" sellers, rental agencies, ancestry agencies, software vendors, geolocation firms, gaming firms, bulk biospecimen providers and third-party vendors, such as cloud-service providers.

The Proposed Rule

The Data Risk Regime will either restrict or prohibit "covered data transactions," which are transactions between U.S. persons and "covered persons" involving access to "bulk U.S. sensitive personal data" or "government-related data" through any of four arrangements: data brokerage, employment agreements, investment agreements or vendor agreements.

Bulk US Sensitive Personal Data

The Proposed Rule keeps the same six categories of "sensitive personal data" outlined in the ANPRM, with some key clarifications for "covered personal identifiers."

<table>
<tr><th colspan="3">Categories of Sensitive Personal Data</th></tr>
<tr><td>Covered Personal Identifiers</td><td>Precise geolocation data</td><td rowspan="5">Categories of Covered Personal Identifiers:
– Full or truncated government identification or account number
– Full financial account numbers or personal identification numbers associated with a financial institution or financial-services company
– Device-based or hardware based identifier
– Demographic or contact data
– Advertising identifier
– Account authentication data
– Network-based identifier
– Call-detail data</td></tr>
<tr><td>Biometric identifiers</td><td>Human genomic data</td></tr>
<tr><td>Personal health data</td><td>Personal financial data</td></tr>
<tr><td colspan="2">Any combination thereof</td></tr>
</table>

Fortifying US Data: Proposed Rule Would Establish a New Regime To Restrict or Prohibit Certain Data Transactions With Countries of Concern

For example, the Proposed Rule confirms that a single listed personal identifier is not sensitive personal data nor is a combination of two pieces of demographic or contact data (*e.g.*, a first name and an address). Further, the Proposed Rule also adds an exemption for network-based identifiers, account-authentication data or call-detail data (*e.g.*, an IP address) that is not linked to other sensitive personal data and is necessary to telecommunications networking or networking services (*e.g.*, a mobile network).

The Proposed Rule formally establishes "bulk" data thresholds from 100 to 100,000, depending on the category of sensitive personal data. Bulk thresholds are met both through a single covered data transaction or aggregated across covered data transactions within the preceding 12 months. The Proposed Rule defines "access" to bulk U.S. sensitive personal data broadly, to include access to anonymized, pseudonymized, de-identified or encrypted data. The Proposed Rule does not impose a legal requirements to decrypt data to comply but expects that existing business analytics regarding volume and type of data would enable businesses to evaluate whether bulk thresholds are met.

Government-Related Data

Similar to the ANPRM, "government-related data" includes (1) precise geolocation data (*i.e.*, within 1,000 feet) for individuals within defined sensitive geographic areas (the Government-Related Location Data List) and (2) sensitive personal data, regardless of volume, that is marketed as linked or linkable to current and former government personnel. The Proposed Rule clarifies that data sets that may include sensitive personal data relating to U.S. government personnel would be treated as bulk U.S. sensitive personal data — and thus subject to bulk thresholds — unless a U.S. person "markets" such data as linked or linkable to current and former government personnel. Conversely, data sets that include precise geolocation data within the Government Related Location Data List would appear to be treated as government-related data regardless of whether it is mixed with other data sets. The Proposed Rule initially identified eight geographic locations that appear to coincide with various headquarters facilities for national level collection and cybersecurity missions within the intelligence community. The Proposed Rule notes that the finalized rule will include additional national security sensitive locations.

US Persons and Covered Persons

The Proposed Rule applies to transactions between "U.S. persons" on the one hand and "covered persons" on the other. U.S. persons are defined as any person located in the U.S.; U.S. citizen, national or lawful permanent resident; person admitted as a refugee or granted asylum; or entity organized under the laws of the U.S. or any jurisdiction within the U.S. (including foreign branches). "Covered persons" include persons from covered countries of concern, which include China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba and Venezuela, and (i) companies owned by, controlled by or subject to the jurisdiction or direction of a country of concern; (ii) foreign employees of, or contractors with such entities or a country of concern; (iii) foreign persons who are primarily residents of a country of concern; and (iv) any person DOJ designates as a covered person for violating the proposed rule. The Proposed Rule clarifies that all U.S. persons — including U.S. subsidiaries of covered persons, and individuals located in the U.S., even temporarily — are not considered "covered persons" unless they are specifically designated by DOJ as "covered persons."

Prohibited and Restricted Covered Data Transactions

Under the Proposed Rule, "prohibited transactions" include all covered data transactions involving "data brokerage" regardless of the type of bulk U.S. sensitive personal data involved, and all covered data transactions resulting in access to bulk human genomic data. "Restricted transactions" include covered data transactions in the form of vendor, employment, and investment agreements that involve bulk U.S. sensitive personal data or government-related data and that are not otherwise "prohibited." The Proposed Rule establishes a baseline set of cybersecurity mitigation measures that would authorize restricted transactions with covered persons. The proposed requirements are set forth in a proposed rule issued by the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency ("CISA") simultaneously with the Proposed Rule.

The Proposed Rule also identifies a number of exemptions for transactions ordinarily incident to basic cross-border commercial activity or provision of key services such as banking and financing, e-commerce, and telecommunications. It will important to carefully consider these exemptions, as the prohibitions and restrictions are broad and exemptions are narrowly focused on specific sets of activities, rather than the type of entity performing them. Thus, the transfer of the same sets of data for different purposes can result in different outcomes when it comes to compliance and coverage under the regulations.

Additional Requirements for US Persons

Like many contemporaneous U.S. rules and regulations governing transactions with China, the Proposed Rule imposes additional diligence and other limitations on U.S. persons transacting with third parties or working for non-U.S. persons. For example, the Proposed Rule clarifies that U.S. persons who are participating in data brokerage of sensitive data with foreign

persons must limit their ability to resell, or allow access to, that data by countries of concern through contractual restrictions. The Proposed Rule also requires U.S. persons to report any known or suspected violations of contractual restrictions. The Proposed Rule also prohibits U.S. persons from "knowingly" directing any covered data transaction by a non-U.S. person that would be a prohibited transaction (including restricted transactions that do not comply with the security requirements) if engaged in by a U.S. person. This extends to instances where the U.S. person should have known the transaction was a prohibited transaction.

Compliance Requirements

DOJ recommends that U.S. companies establish risk-based compliance programs to track, and where necessary restrict or prohibit, data flows pursuant to the Proposed Rule. Key aspects of a compliance program include: senior management buy-in, risk assessments, internal controls, and the establishment of policies and procedures with respect to data transactions. The Proposed Rule also provides that the DOJ can require any U.S. person to furnish under oath information related to any covered data transaction.

The Proposed Rule imposes affirmative compliance requirements as a condition of engaging in a restricted transaction such as those restricted transactions completed pursuant to CISA established cybersecurity requirements. Compliance requirements include: (i) establishing and implementing data compliance programs with risk-based procedures for verifying data flows; (ii) annually auditing to verify and improve compliance with security requirements; (iii) preparing an annual report that would include information about any attempted prohibited transaction; (iv) and keeping records of all restricted transactions for at least 10 years.

Conclusion

This Proposed Rule comes on the heels of a number of new and proposed regulations targeting the development and deployment of key national security-related technologies (*e.g.*, artificial intelligence and cybersecurity capabilities) by China and other countries and persons of concern. For example, the Department of the Treasury recently issued a rule limiting U.S. outbound investment in Chinese companies active in developing certain artificial intelligence and other specified advanced technologies. The Department of Commerce issued proposed rules in 2024 that would require reporting on foreign use of U.S. cloud computing services to train large AI models and on activities related to the development or acquisition of "dual-use" artificial intelligence and computing clusters. Finally the Department of Commerce has ramped up their use of authorities to address supply chain risks associated with the use of information and communication technologies and services from China and other countries of concern that could, if exploited, provide access to sensitive data.

Similar to these other regulatory authorities, the Proposed Rule is designed to limit the national security impact of technological advancements supporting the military and intelligence ambitions of countries of concern. DOJ notes that the development of technologies such as artificial intelligence, high-performance computing and big-data analytics by countries of concern amplifies the threat posed by these countries' access to government-related data or Americans' bulk sensitive personal data.

DOJ stresses that the Proposed Rule is a national security rule rather than a data privacy rule. Like the Proposed Rule, existing data privacy protection regimes generally require companies to understand and maintain awareness of the types of data they collect and store. That said, the new Data Risk Regime will no doubt add additional compliance costs and risks to business dealings with countries of concern.