SULLIVAN & CROMWELL LLP

S&C memo

November 14, 2024

U.S. Department of Justice Proposes Rules to Regulate the Transfer of Sensitive U.S. Data to Countries of National Security Concern

Covered Large-Scale International Data Transfers Would Be Prohibited or Restricted; Comments Due by November 29, 2024

SUMMARY

On October 21, 2024, the U.S. Department of Justice ("DOJ") published a Notice of Proposed Rulemaking ("NPRM") setting forth proposed regulations that would prohibit or restrict the large-scale transfer of specified classes of sensitive U.S. personal data (including biometric, genomic, health, geolocation, financial, and other identifying information), as well as certain data relating to government sites and employees, to six countries of perceived national security concern: China, Russia, Iran, North Korea, Cuba, and Venezuela.[1] The NPRM follows an Advance Notice of Proposed Rulemaking ("ANPRM") that the DOJ issued on February 28, 2024.

The proposed rules would establish an extensive regulatory framework designed to protect sensitive bulk U.S. data from exploitation by countries perceived as posing national security threats. In essence, if a covered transaction involves covered data and implicates a country of concern, it is either prohibited or restricted unless subject to an exemption or covered by a general or specific license. The regime is intended to complement existing statutory and regulatory frameworks such as the Committee on Foreign Investment in the United States ("CFIUS"), which has the authority to review covered investments in U.S. business by foreign persons for threats to U.S. national security. The NPRM was published in the Federal Register on October 29, 2024, and the DOJ is soliciting public comments until November 29, 2024.

EXECUTIVE ORDER

The proposed rules are designed to implement Executive Order 14117, "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern" (the "Executive Order").[2] The Executive Order stated that countries of concern use such sensitive U.S. data "to track and build profiles on United States individuals, including federal employees and contractors, for illicit purposes, including blackmail and espionage," and that their access to such data "through data brokerages, third-party vendor agreements, employment agreements, investment agreements, or other such arrangements poses particular and unacceptable risks to our national security." It further noted that the restrictions should be "specific, carefully calibrated actions" that will "not broadly prohibit United States persons from conducting commercial transactions, including exchanging financial and other data as part of the sale of commercial goods and services."

The Executive Order directed the Attorney General to issue rules to prohibit or restrict U.S. persons from engaging in certain data-related activities and data transactions and granted the DOJ both civil and criminal enforcement authority.

DEPARTMENT OF JUSTICE RULEMAKING

In its press release announcing the NPRM, the DOJ stated that "[t]he proposed rule is tailored to address the specific national security risks stemming from access by countries of concern and covered persons to Americans' bulk sensitive personal data and certain sensitive U.S. government-related data," echoing the national security concerns identified in Executive Order 14117. The press release further noted that these measures complement the United States' commitment to: "(i) promoting an open, global, interoperable, reliable, and secure internet;" (ii) "protecting human rights online and offline;" (iii) "supporting a vibrant, global economy by promoting cross-border data flows that are required to enable international commerce and trade;" and (iv) "facilitating open investment."[3]

The NPRM would establish a two-prong structure:

- "Prohibited transactions" would be forbidden in their entirety.
- "Restricted transactions," by contrast, would be prohibited only if they do not comply with specified security requirements that are being developed by the Cybersecurity and Infrastructure Agency ("CISA"), a component of the Department of Homeland Security.

For both prohibited and restricted transactions, an exemption or license may be available to allow the transaction.

Transactions

The NPRM defines a "transaction" as "any acquisition, holding, use, transfer, transportation, exportation of, or dealing in any property in which a foreign country or national thereof has an interest." The parameters and restrictions of the NPRM—which are subject to public comment—include the following:

Countries of Concern

The NPRM identifies six countries of concern—the People's Republic of China, including the Special Administrative Region of Hong Kong and the Special Administrative Region of Macau; the Russian Federation; the Islamic Republic of Iran; the Democratic People's Republic of Korea; the Republic of Cuba; and the Bolivarian Republic of Venezuela—because these countries "have engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or the security and safety of U.S. persons," and pose a significant risk of exploiting covered data to "the detriment of the national security of the United States or the security and safety of U.S. persons."

This list is identical to the list of "foreign adversaries" established by the Department of Commerce for purposes of the "ICTS rule," which allows the Department of Commerce to review information and communications technology and services "transactions" and restrict or prohibit those that pose an "undue or unacceptable risk" to U.S. national security or the safety of U.S. persons where those transactions involve "foreign adversaries."[4]

Covered Persons

The regulations would apply only to certain data transactions that U.S. persons conduct with so-called "covered persons," defined as those "meaningfully subject to the ownership, direction, jurisdiction of a country of concern, or control of a country of concern or covered person."[5]

Covered persons would be defined as entities or individuals under the jurisdiction, direction, ownership, or control of the above-referenced six countries of concern.

This definition specifically includes an entity that is a foreign person and that:

- is 50 percent or more owned, directly or indirectly, by a country of concern;
- is organized or chartered under the laws of a country of concern; or
- has its principal place of business in a country of concern.

In addition, "covered person" would include (1) any foreign individual who is an employee or contractor of such an entity or of a country of concern itself and (2) any foreign individual who is primarily a resident in the territorial jurisdiction of a country of concern.

Any foreign entity that is 50 percent or more owned, directly or indirectly, by an entity or individual described above would also be covered.

Citizens of countries of concern residing in third countries would not categorically be covered, but could be included if they are working for the government of a country of concern or for an entity that is a covered person.

The NPRM excludes U.S. persons from being categorically treated as covered persons. Under the NPRM, the term "U.S. person" is defined as a "United States citizen, national, or lawful permanent resident; or 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; or 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." For example, any U.S.-based subsidiary of a covered person is considered a U.S. person for these regulations, as are citizens of countries of concern located in the United States. This definition is similar to, but broader than, the Office of Foreign Assets Control's definition of "U.S. person."[6]

Significantly, the proposed rule allows for the Attorney General to designate an individual or entity as a covered person and then publish that designation in the Federal Register. This includes those not already captured by other elements of the definition.[7] However, the Attorney General's authority to do so only arises following a determination that an individual:

- is subject to the control, jurisdiction, or direction of a country of concern;
- is acting on behalf of or purporting to act on behalf of a country of concern or covered person; or
- has knowingly caused or directed a violation of the rule.

Under the proposed rule, designation by the Attorney General as a covered person is effective upon announcement by the DOJ, at which point "a U.S. person with actual knowledge of the designated person's status would be prohibited from knowingly engaging in a covered data transaction with that person."

Covered Data

The proposed rules would apply only to "covered data." As currently contemplated, this would include two categories: (i) bulk U.S. sensitive personal data and (ii) U.S. Government-related data that poses an unacceptable risk of access by countries of concern or covered persons.

Bulk Sensitive Personal Data

The prohibitions and restrictions on transactions involving sensitive personal data only apply to transactions that contain a "bulk" data set, meaning those that include a collection or set of sensitive personal data relating to U.S. persons, where the number of U.S. persons in the data set is greater than the specified bulk threshold—which varies depending on the type of data, as discussed below—at any point in the preceding 12 months. The regulations would apply regardless of whether that threshold is exceeded through a single covered data transaction or aggregated across multiple transactions and regardless of whether the data is anonymized, pseudonymized, de-identified, or encrypted.

The proposed rules would establish six categories of "sensitive personal data." These categories, listed in descending order based on the DOJ's determination of sensitivity, are defined as follows:

- **Human genomic data** is data representing the nucleic acid sequences that constitute the entire set or a subset of the genetic instructions found in a human cell, including the result or results of an individual's "genetic test" and any related human genetic sequencing data. The DOJ is considering whether to include other data, such as epigenetic data (data involving changes in DNA that do not alter the underlying DNA sequence), in the final rule and is actively soliciting comments on the subject. The proposed "bulk threshold" for human genomic data is more than 100 U.S. persons. This clarifies the potential thresholds proposed in the ANPRM, which ranged from a low of 100 to a high of 1,000.[8]
- **Biometric identifiers** are measurable physical characteristics or behaviors used to recognize or verify the identity of an individual, such as facial images, voiceprints and patterns, retina and iris scans, palm prints, fingerprints, gait, and keyboard usage patterns.[9] The proposed "bulk threshold" for this type of data is more than 1,000 U.S. persons (compared to the range of possible thresholds proposed in the ANPRM: 100–10,000).
- **Geolocation and related sensor data** is data such as GPS coordinates or Internet Protocol (IP) address geolocation that identifies the real-time or historical physical location of an individual or a device with a precision of 1,000 meters or less. The proposed bulk threshold for this type of data is more than 1,000 U.S. devices. The ANPRM contemplated setting the threshold somewhere between 100 and 10,000 devices.[10]
- **Personal health data** is information describing bodily functions, height and weight, vital signs, symptoms, and allergies; social, psychological, behavioral, and medical diagnostic, intervention, and treatment history that relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual.[11] The proposed bulk threshold for personal health data is more than 10,000 U.S. persons. The possible thresholds considered in the ANPRM ranged from a low end of 1,000 to a high end of 1,000,000.[12]
- **Personal financial data** is information about an individual's bank account or credit, charge, or debit card, including purchases and payment history.[13] The proposed bulk threshold for this personal financial data is more than 10,000 U.S. persons. The ANPRM anticipated a threshold between 1,000 and 1,000,000.[14]
- **Covered personal identifiers** include three categories of covered personal identifiers: (1) any listed identifier—such as government identification numbers, financial account numbers, SIM or MAC addresses, demographic or contact data, advertising identifiers, login information, network-based identifiers, or call-detail data—used in combination with another listed identifier; (2) listed identifiers used in combination with other bulk sensitive personal data; and (3) listed identifiers usable to identify an individual from a data set when linked or linkable to other listed identifiers or to other sensitive personal data.[15] The proposed bulk threshold for this type of data is more than 100,000 U.S. persons. This clarifies the range proposed in the ANPRM, which ranged from a low end of 10,000 to a high end of 1,000,000.[16] Two exceptions to this category are proposed:
    - (1) demographic/contact data linked only to other demographic/contact data, for example, "a first and last name linked to a residential street address, an email address linked to a first and last name, or a customer loyalty membership record linking a first and last name to a phone number—would not constitute covered personal identifiers"; and
    - (2) network-based identifiers, login information, or call center data when linked to the same type of identifier and only as necessary for the provision of telecommunications and similar services.

Government-Related Data

The NPRM bifurcates "government-related data" into subcategories related to specific locations and personnel.

- Location: "Any precise geolocation data, regardless of volume, for any location within any area enumerated on the Government-Related Location Data List [a currently non-comprehensive list of eight sets of latitude/longitude coordinates] which the Attorney General has determined poses a heightened risk of being exploited by a country of concern to reveal insights about locations controlled by the Federal Government, including insights about facilities, activities, or populations in those locations, to the detriment of national security, because of the nature of those locations or the personnel who work there." The DOJ anticipates that it will add to this list, and that the final rule may include the worksites of Federal government national security employees; military installations; embassies or consulates; or other national security support facilities.
- Personnel: Sensitive personal data, regardless of volume, that a transacting party markets as "linked or linkable to current or recent former employees or contractors, or former senior officials, of the United States Government, including the military and Intelligence Community."

The ANPRM also contemplates further defining government-related data to include precise geolocation data connected to such individuals or sensitive locations.

Covered Data Transactions

The proposed regulations would only apply to "covered data transactions," a term defined to include any transaction that involves access to "covered data" and is classified as a data brokerage transaction, vendor agreement, employment agreement, or investment agreement.[17]

- A transaction "involves" covered data when it provides for any access to such data by the counterparty to a transaction.
- "Access" is defined as "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."
- "Data-brokerage transactions" are 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."
- Employment agreement "means 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." To illustrate the risk posed by such a transaction, the NPRM provides examples, including: "a U.S. company that employs a team of individuals who are citizens of and primarily reside in a country of concern and have access to back-end IT services and company systems that contain bulk human genomic data."
- Vendor agreement "means 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." To illustrate the risk provided by such a transaction, the NPRM provides examples, including: "A U.S. company, which is owned by an entity headquartered in a country of concern and has been designated a covered person, establishes a new data center in the United States to offer managed services. The U.S.

company's data center serves as a vendor to various U.S. companies to store bulk U.S. sensitive personal data collected by those companies."

Exempt Transactions

- The proposed rule specifically exempts several classes of data transactions. These include three categories of data transactions—namely, "personal communications, information or informational materials, and data that is ordinarily incident to travel to or from another country," to the extent that such transactions are statutorily exempt under IEEPA.
  - "Personal communications" are defined as "any postal, telegraphic, telephonic, or other personal communication that does not involve the transfer of anything of value."
  - The DOJ is proposing to limit "information or informational materials" to *expressive* material, specifically, "publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and news wire feeds." Additionally, and consistent with OFAC regulations and IEEPA itself, the DOJ would exclude "information or informational materials that are not fully created and in existence at the date of the data transaction, or the substantive or artistic alteration or enhancement of information or informational materials, or the provision of marketing and business consulting services, including to market, produce or co-produce, or assist in the creation of information or informational materials."
  - Data ordinarily incident to travel includes information related to the "importation of accompanied baggage for personal use; maintenance within any country, including payment of living expenses and acquisition of goods or services for personal use; and arrangement or facilitation of such travel, including nonscheduled air, sea, or land voyages."
- The proposed rule's exemptions also include:
  - data transactions that are for the official business of the United States government;
  - data transactions "ordinarily incident to and part of the provision of financial services," including banking, capital markets, and financial insurance services and transactions required for compliance with any Federal statutory or regulatory requirements;
  - corporate group transactions, defined as data transactions (i) between a U.S. person and its subsidiary or affiliate located in or otherwise subject to the jurisdiction, control, ownership, or direction of a country of concern and (ii) "ordinarily incident to and part of administrative or ancillary business operations" such as transactions related to payroll, human resources, or compliance purposes;
  - transactions required or authorized by federal law or by international agreements to which the United States is a party;
  - investment agreements subject to a CFIUS action;[18]
  - data transactions ordinarily incident to and part of telecommunications services, including international calling, mobile voice, and data roaming (but excluding data brokerage transactions involving countries of concern and covered persons);
  - data transactions "necessary to obtain and maintain regulatory approval to market a drug, biological product, medical device, or combination product in a country of concern" but only to the extent that this is data that is de-identified, required for authorization or approval, and reasonably necessary to evaluate the safety and effectiveness of the covered product; and
  - data transactions "[o]rdinarily incident to and part of the collection or processing of clinical care data . . . and necessary to support or maintain authorization by the FDA."

Prohibited or Restricted Transactions

- A transaction is either "prohibited" or "restricted" depending on the particular category of transaction involved.

Prohibited Transactions

- The proposed rule would prohibit U.S. persons (unless authorized by an exemption or license) from knowingly:
  - engaging in a covered data transaction involving data brokerage with a country of concern or covered person;
  - engaging in a covered data transaction involving data brokerage with any foreign person unless the U.S. person "[c]ontractually requires that the foreign person refrain from engaging in a subsequent covered data transaction involving that data with a country of concern or covered person." Notably, this is the sole circumstance where the proposed rule could impact transactions not directly involving a country of concern or a covered person;
  - engaging in a covered data transaction involving access to bulk human genomic data (or biospecimens from which such data can be derived); or
  - directing any covered data transaction that would be prohibited if conducted by a U.S. person.
- Under the terms of the NPRM, the term "knowingly" includes actual or constructive knowledge of the conduct, the circumstances, or the result of the transaction.
- The proposed rule would also prohibit (1) any transactions that have the purpose of evading or avoiding, or that cause a violation of or attempt to violate, the proposed rule's prohibitions and (2) conspiracies formed to violate the proposed rule's prohibitions.

Restricted Transactions

- The proposed rule would restrict—and thereby require extra security measures for—data transactions that involve covered data and are (i) vendor agreements involving the provision of goods and services (including cloud service agreements), (ii) employment agreements, or (iii) investment agreements.
- These transactions would be allowed if they meet security requirements proposed by CISA. CISA is concurrently publishing its proposed security requirements for public comment. In brief, CISA's proposal would involve "cybersecurity measures such as basic organizational cybersecurity policies and practices, physical and logical access controls, data masking and minimization, encryption, and the use of privacy-enhancing techniques" in connection with such transactions.[19]

Auditing and Recordkeeping Obligations for Restricted Transactions

- For U.S. persons engaging in restricted transactions, the NPRM mandates that they conduct an audit that adheres to certain standards:
  - The auditor must be qualified and competent, independent and external, and not be a covered person or a country of concern;
  - The audit must occur once a calendar year in which the U.S. person engages in a restricted transaction and must cover the preceding 12 months; and
  - The audit must examine the U.S. person's data transactions and data compliance program as required by the proposed rule.
- Further, a U.S. person engaging in restricted transactions must keep "a full and accurate record of each such transaction engaged in, and such record shall be available for examination for at least 10

years after the date of such transaction." The rule specifically mandates that the following records be maintained:

- A written policy describing the data compliance program, certified annually;
- A written policy describing the implementation of applicable security requirements;
- The results of any annual audits that verify compliance with the security requirements;
- Documentation of the due diligence conducted to verify the data flow involved in any restricted transaction;
- Documentation of the method of data transfer;
- Documentation of the dates the transaction began and ended;
- Copies of any agreements associated with the transaction;
- Copies of any relevant licenses or advisory opinions;
- The document reference number for any original document issued by the Attorney General, such as a license or advisory opinion;
- A copy of any relevant documentation received or created in connection with the transaction; and
- An annual certification by the employee responsible for compliance of the completeness and accuracy of the records documenting due diligence.

Licensing and Advisory Opinions

- The Executive Order authorized the Attorney General to issue licenses authorizing otherwise prohibited or restricted transactions. The NPRM outlines a process by which regulated parties may seek and be issued licenses. The conditions and requirements for licensing are still undetermined, but the NPRM suggests that licensing may be conditioned upon "additional disclosure requirements, ongoing reporting obligations, recordkeeping obligations, due diligence requirements, certification requirements, cybersecurity requirements, or inclusion of certain contractual terms."
  - General licenses would be published in the Federal Register and could be relied on by all affected parties.
  - Specific licenses would cover only parties who apply for and are issued such a license and would only apply to the specific transactions for which the license was sought.
- The proposed rule also creates a process by which the Attorney General can offer interpretations of the terms of the rule through official guidance or written advisory opinions. Under the terms provided in the NPRM, the DOJ may publish general guidance through FAQs posted online, and U.S. persons engaging in a potentially regulated transaction may request a specific interpretation of the rules as applied to the contemplated transaction.

Finding of a Violation and Penalties

- The NPRM establishes that the civil and criminal penalties provided for in Section 206 of IEEPA are applicable to violations of the proposed rule. Penalties may be based on noncompliance, material misstatements or omissions, false certifications or submissions, or "other actions and factors." Specifically, the program addresses:
  - **Penalty Structure**: Potential penalties for violations of the Final Rule include civil and criminal penalties up to the maximum amount set forth in section 206 of IEEPA (for civil violations, the greater of $250,000 (currently $368,136, as adjusted pursuant to the Federal Civil Penalties Inflation Adjustment Act of 1990, as amended) or twice the amount of the transaction, and for criminal violations, $1,000,000, 20 years in prison (if a natural person), or both).

  - **Investigative Powers**: The DOJ is authorized to investigate potential violations by conducting hearings, examining and deposing witnesses, and issuing subpoenas for documents and witnesses related to any alleged violations.
  - **Procedural Elements**: When the DOJ has reason to believe a civil regulatory violation has occurred, it will issue a pre-penalty notice informing the alleged violator of the intent to impose a monetary penalty. This notice includes the alleged violation, the proposed penalty, and relevant, non-privileged information that supports the DOJ's findings.
  - **Right to Respond**: Alleged violators are provided the right to respond to a pre-penalty notice within 30 days. They may submit a written presentation detailing why a penalty is unwarranted.
  - **Final Penalty Imposition**: In regards to civil enforcement, following review of any responses, if the DOJ finds a violation, it will issue a final penalty notice, constituting final agency action. The violator has the right to seek judicial review of the final agency action.
- The NPRM also provides a process by which the DOJ might issue a finding of a violation of the proposed rule where it has found that "a party has violated the regulations and that an administrative response short of a civil monetary penalty is warranted." Specifically, an alleged violator has the right to contest an initial finding of a violation and will be given "relevant information that is not privileged, classified, or otherwise protected, that forms the basis for the finding of violation, including a description of the alleged violation."
- Additionally, the NPRM states that the DOJ may for purposes of civil liability under the regulations "infer knowledge of the designated person's status on the part of any U.S. person engaging in a covered data transaction with that person."

OBSERVATIONS AND IMPLICATIONS

The NPRM reflects the DOJ's continued focus on perceived national security threats arising from the efforts of certain foreign actors to obtain and misappropriate sensitive data relating to U.S. persons, companies, and government agencies. The proposed rule would create a significant and potentially sweeping new regulatory framework that many companies will need to address and incorporate into their operations, privacy policies, and corporate compliance programs. This program would also significantly mirror aspects of the existing International Emergency Economic Powers Act ("IEEPA") based economic sanctions regime through features such as general and specific licenses, exempted transactions, evasion as a potential basis for liability, and provisions addressing re-exports. Several aspects of the rule suggest that its implementation could have wide-ranging implications across a range of industries and sectors. In this regard, several points are worth highlighting:

- *First*, the proposed definition of "prohibited" transactions suggests that U.S. data brokers and companies engaged in genomic testing, research, and/or other activities involving U.S. genomic data will face the most sweeping prohibitions on data transfers to countries of concern. For example, data brokers that transfer bulk U.S. financial data to parties in China (including Hong Kong or Macao) could face civil or criminal penalties in the event that they engage in transactions exceeding the applicable data volume threshold. Notably, the NPRM selected bulk thresholds at or closer to the lower end of the range of possible thresholds contemplated in the ANRPM for each of the six categories of "sensitive personal data," stating that these thresholds are "approximately the middle order of magnitude of the preliminary ranges identified in the ANPRM."
- *Second*, the proposed definition of "restricted" transactions means that companies across a range of sectors will likely have to monitor and implement government-mandated data security requirements

before providing access to sensitive bulk U.S. data to countries of concern. Because "restricted" transactions will include (i) vendor agreements involving the provision of goods and services (including cloud service agreements), (ii) employment agreements, and (iii) investment agreements, the rule will potentially affect companies in a number of different industries that allow for their clients or counterparties to access sensitive U.S. data. The affected industries are likely to include, for example, financial technology (Fintech); business intelligence and analytics; cloud software and computing; artificial intelligence; recruiting and personnel management; healthcare; finance and investment; online advertising and marketing; and international exports and trade. In addressing these new data security requirements, companies in these and other sectors will also need to comply with rules and guidance issued by agencies that might not otherwise regulate them—namely, the DOJ and CISA/the Department of Homeland Security.

- *Third*, the fact that "covered persons" broadly include foreign entities that (i) are 50 percent or more owned, directly or indirectly, by a country of concern, (ii) are organized or chartered under the laws of a country of concern, (iii) have their principal place of business in a country of concern, or (iv) are 50 percent or more owned, directly or indirectly, by a covered person, means that companies engaging in numerous types of business transactions will need to conduct potentially extensive due diligence on their counterparties to determine whether provision of access to U.S. data to the counterparty would implicate the regulations.
- *Fourth*, despite its potentially wide-reaching impact, the proposed rule contains certain features that limit its applicability and would ensure that it does not function as a comprehensive data privacy protection framework akin to the European General Data Protection Regulation or similar regimes. Most notably, the various exemptions outlined in the proposed rule—including for personal communications, informational materials, data transfers between and among corporate affiliates, transactions incident to financial services, and transactions incident to telecommunications services—suggest that the DOJ intends to exclude the majority of everyday commercial and business transactions from the rule's ambit. In addition, the fact that the proposed rule expressly applies only to transactions involving six specified countries will limit its regulatory and economic impact.
- *Finally*, companies and financial institutions may wish to take advantage of the 30-day comment period in order to shape or object to particular aspects of the proposed rule in advance of the DOJ's publication of a final version. For example, the DOJ has solicited comments on specific topics such as the risks and benefits of regulating genetic and other 'omic data (*i.e.,* data generated from humans that characterizes or quantifies human biological molecule(s), such as human genomic data, epigenomic data, proteomic data, transcriptomic data, microbiomic data, or metabolomic data) and the costs of complying with the framework created by the proposed rule. Additionally, CISA is soliciting comments on the proposed data security requirements. Parties that could be adversely affected by the proposed rule should therefore consider raising concerns with the DOJ before a final rule is issued.

* * *

ENDNOTES

[1] Department of Justice, *NPRM: Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons* (Oct. 21, 2024), *available at* https://www.justice.gov/d9/2024-10/nsd_104_-_data_security_-_1124-aa01_-_notice_of_proposed_rulemaking_0.pdf. Accompanying the NPRM, DOJ also issued a fact sheet containing additional explanations. *See* Department of Justice, *FACT SHEET: Justice Department Moving Forward with Publishing a Proposed Rule to Protect Americans' Sensitive Personal Data from Countries of Concern* (Oct. 21, 2024) (the "DOJ Fact Sheet"), *available at* https://www.justice.gov/opa/media/1374016/dl.

[2] Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern (Feb. 28, 2024).

[3] Department of Justice, *Justice Department Issues Comprehensive Proposed Rule Addressing National Security Risks Posed to U.S. Sensitive Data* (Oct. 21, 2024) https://www.justice.gov/opa/pr/justice-department-issues-comprehensive-proposed-rule-addressing-national-security-risks.

[4] 15 C.F.R. § 791 (2024).

[5] NPRM at *131.

[6] *See, e.g.*, 31 CFR § 560.314; 31 CFR § 598.318 (not including those admitted as refugees or asylum seekers as "U.S. persons").

[7] NPRM at *134-35.

[8] ANPRM at *25.

[9] NPRM at *35.

[10] ANPRM at *25.

[11] NPRM at *41.

[12] ANPRM at *25.

[13] NPRM at *40.

[14] ANPRM at *25

[15] NPRM at *29-31.

[16] ANPRM at *25.

[17] NPRM at *22-23.

[18] This occurs when CFIUS has suspended a proposed or pending transaction or entered into or imposed mitigation measures to address a national security risk involving access to sensitive personal data by countries of concern or covered persons.

[19] DOJ Fact Sheet at *4.

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 900 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers or to any Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.