FACT SHEET: Justice Department Moving Forward with Publishing a Proposed Rule to Protect Americans' Sensitive Personal Data from Countries of Concern

On October 21, the Department issued a Notice of Proposed Rulemaking (NPRM) to address the national-security risks posed by the continued efforts of countries of concern to access, exploit, and weaponize Americans' sensitive personal data. As previewed in the Department's Advance Notice of Proposed Rulemaking (ANPRM) published in March, the proposed rule would establish a new national-security program to prohibit or restrict U.S. persons from engaging in certain categories of data transactions with countries of concern and covered persons that pose unacceptable national-security risks of giving those countries or persons access to government-related data or bulk sensitive personal data. The Department welcomes public comment on the NPRM within 30 days of its publication in the Federal Register.

This fact sheet offers a concise summary of the rule. For specific details about the proposed rule, please refer to the NPRM.

Background

Americans generate a vast digital footprint that, without protective measures, countries of concern can weaponize to threaten our national security. These countries of concern can purchase or access Americans' sensitive personal data and U.S. Government-related data (government-related data) through various commercial transactions and relationships. They utilize biometric, genomic, financial, geolocation, and health data, along with certain personal identifiers, to analyze Americans' lifestyles, spending habits, financial issues, preferences, and personal visits to sensitive locations like places of worship, government facilities, and health clinics. This data is then used for cyber-attacks, blackmail, espionage, and intimidating activists, academics, political figures, and journalists, as well as other malicious activities. Countries of concern employ advanced technologies like big-data analytics, artificial intelligence (AI), and high-performance computing to manipulate and exploit this data more effectively. Despite efforts to restrict unlawful access to data, current laws permit countries of concern to access Americans' sensitive personal data and government-related data through commercial means, and existing national security authorities only address these risks on a case-by-case basis. To address this risk, on February 28, 2024, President Biden issued Executive Order 14117, "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern" (E.O.).

Executive Order and NPRM

Acting under the International Emergency Economic Powers Act, which vests the President with authority to deal with extraordinary threats to national security and foreign policy that have their source in whole or in part outside the United States, the E.O. directed the Department to establish and implement new regulations to address the threat from certain countries of concern attempting to access and exploit Americans' sensitive personal data. In parallel, the Department of Justice released a nearly 90-page Advance Notice of Proposed Rulemaking (ANPRM), previewing the proposed rule to implement the E.O. and soliciting public comment. During the 45-day period for public comment on the ANPRM, the Department received 67 comments and separately engaged with over 100 companies, industry groups, and other stakeholders to seek their feedback.

As previewed in the ANPRM, the NPRM would limit or prohibit U.S. persons from engaging in certain classes of transactions that pose an unacceptable risk of giving countries of concern or covered persons access to Americans' government-related data or bulk sensitive personal data. Among other things, the NPRM would identify certain classes of prohibited, restricted, and exempt transactions; identify countries of concern and covered persons to which the prohibitions and restrictions apply; establish processes for licensing and advisory opinions; define terms and set bulk thresholds for triggering the proposed rule's prohibitions and restrictions on covered data transactions involving bulk sensitive personal data; address recordkeeping, auditing reporting, and other compliance requirements; and establish enforcement mechanisms including civil penalties.

Countries of Concern: As previewed in the ANPRM, the proposed rule would designate six countries — China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia, and Venezuela — as countries of concern because they 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 because they pose a significant risk of exploiting bulk sensitive personal data or government-related data.

Covered Persons: The proposed rule would generally regulate U.S. persons' data transactions with "covered persons" through which there is an unacceptable risk that countries of concern, as a legal and practical matter, can access sensitive personal data. As previewed in the ANPRM, the proposed rule primarily defines four classes of covered persons: (1) foreign entities that are 50 percent or more owned by a country of concern, organized under the laws of a country of concern, or has its principal place of business in a country of concern; (2) foreign entities that are 50 percent or more owned by a covered person; (3) foreign employees or contractors of countries of concern or entities that are covered persons; and (4) foreign individuals primarily resident in countries of concern.

As also previewed in the ANPRM, these four classes would be supplemented by a public list of individuals and entities designated by the Department as covered persons. Under the proposed rule, the Department could designate any person, regardless of location, that it determines to be, or to have been, controlled by or under the jurisdiction of a country of concern or a covered person, or who acts, has acted, or is likely to act on behalf of such entities, or who knowingly causes or is likely to cause a violation of this part, as a covered person.

Sensitive Personal Data: As previewed in the ANPRM, the proposed rule would regulate transactions involving six categories of sensitive personal data that a country of concern or covered person could exploit to harm U.S. national security if that data is linked or linkable to any identifiable U.S. individual or to a discrete and identifiable group of U.S. persons. These six categories are: (1) certain covered personal identifiers (e.g., names linked to device identifiers,

social security numbers, driver's license, or other government identification numbers); (2) precise geolocation data (e.g., GPS coordinates; (3) biometric identifiers (e.g., facial images, voice prints and patterns, and retina scans); (4) human genomic data (e.g., DNA within each of the 24 distinct chromosomes in the cell nucleus, including results from genetic testing); (5) personal health data (e.g., height, weight, vital signs, symptoms, test results, diagnosis, and psychological diagnostics); and (6) personal financial data (e.g., information related to an individual's credit, debit cards, bank accounts, and financial liabilities, including payment history).

As also previewed in the ANPRM, the Department proposes to categorically exclude certain categories of data from the definition of the term "sensitive personal data," such as public or nonpublic data that do not relate to an individual (e.g., trade secrets and proprietary information), data that is already lawfully publicly available from government records or widely distributed media, and personal communications and certain informational materials.

Bulk Sensitive Personal Data Thresholds and U.S. Government-Related Data: As previewed by the ANPRM, the proposed rule's prohibitions and restrictions would generally apply only to covered data transactions involving sensitive personal data that exceeds certain bulk volume thresholds. "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." The proposed rule 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, 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, or any combination of these data types that meets the lowest threshold for any category in the dataset. As the proposed rule details, the Department based these proposed thresholds on an extensive risk-based analysis, taking into account the threats, vulnerabilities, and consequences associated with the human-centric and machine-centric characteristics of each type of data.

As the ANPRM previewed, these bulk thresholds would not apply to transactions involving certain government-related data, which would be regulated regardless of the volume. The proposed rule defines two categories of government-related data. With respect to data on the locations of government activities, the proposed rule would treat any precise geolocation data within geographic areas listed on the Department's public Government-Related Location Data List as government-related data. In determining whether to add a geographic area to a list, the Department would work with agency partners to determine whether the area poses a heightened risk of being exploited by a country of concern to reveal insights about federal government-controlled locations, which could harm national security. With respect to data on U.S. Government personnel, the proposed rule would treat any sensitive personal data marketed as linked to current or recent former U.S. Government employees or contractors (including the military and intelligence community) as government-related data.

Prohibitions and Restrictions: As previewed in the NPRM, the proposed rule identifies categories of covered data transactions involving access to government-related data or bulk sensitive personal data that U.S. persons are prohibited or restricted from engaging in with countries of concern or covered persons.

- The two categories of **prohibited transactions** are data brokerage and covered data transactions involving access to bulk human genomic data or biospecimens from which such data can be derived.
- The three categories of **restricted transactions** are vendor, employment, and non-passive investment agreements. These restricted transactions are permitted if they meet certain security requirements developed by the Department of Homeland Security's Cybersecurity and Infrastructure Agency (CISA) that seek to mitigate the risk of access by countries of concern or covered persons. As announced in a Federal Register notice and posted online, CISA is concurrently publishing its proposed security requirements for public comment. As laid out in that proposal, these security requirements would include 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.
- The proposed rule would also address the risk of data being **resold or transferred through third parties** to countries of concern or covered persons by requiring U.S. persons engaged in data brokerage with any foreign person that is not a covered person to satisfy certain conditions, including contractually requiring that the foreign person refrain from reselling or providing access to that data to a country of concern or covered person through a subsequent covered data transaction.
- To address potential **circumvention** of the regulations, the proposed rule would prohibit U.S. persons from knowingly directing any covered data transaction that would be a prohibited if conducted by a U.S. person. The proposed rule would also prohibit transactions designed to evade the regulations, those that cause or attempt to cause a violation of the regulations, and conspiracies to violate the regulations.

Exempt Transactions: As previewed in the ANPRM, the proposed rule would exempt certain classes of data transactions. Building on the specific exemptions previewed in the ANPRM and based on helpful feedback from commenters and the Department's engagements, the proposed rule would add further exemptions related to clinical-trial data and telecommunications. The proposed rule's exemptions include:

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, such as banking, capital markets, or financial insurance services; financial activities authorized for national banks; activities defined as financial in nature or complementary to a financial activity under the Bank Holding Company Act; transfer of personal financial data incidental to e-commerce; and the provision of investment management services that provide advice on portfolios or assets for compensation, including related ancillary 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, such as human resources, payroll, taxes, permits, compliance, risk management, travel, and customer support.

5. **Transactions required or authorized by Federal law or international agreements**, which include agreements such as the Convention on International Civil Aviation (2022); the WHO constitution (1946); various U.S.-China agreements on customs, legal assistance, and taxation; the U.S.-Cuba Extradition Treaty (1905), U.S.-Russia agreements on customs (1994) and legal assistance (1999), the U.S.-Venezuela Legal Assistance Treaty (1997), and the International Health Regulations (2005). Additionally, transactions are exempt to the extent they are ordinarily incident to and part of compliance with federal law and regulations.
6. **Investment agreements** after they have become subject to certain mitigation or other action taken by the Committee on Foreign Investment in the United States (CFIUS), if CFIUS explicitly designates them as exempt.
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. "Regulatory approval data" would mean de-identified sensitive personal data required by a regulatory entity to research or market a drug, biological product, device, or combination product, including post-marketing studies and surveillance. It excludes data not necessary for assessing safety and effectiveness. The terms "drug," "biological product," "device," and "combination product" have the meanings set forth in 21 U.S.C. § 321(g)(1), 42 U.S.C. § 262(i)(1), 21 U.S.C. § 321(h)(1), and 21 CFR § 3.2(e).
9. **Other clinical investigations and post-marketing surveillance data** if the transactions are part of clinical investigations regulated by the Food and Drug Administration (FDA) under sections 505(i) and 520(g) of the Federal Food, Drug, and Cosmetic Act, or support FDA applications for research or marketing permits for drugs, biological products, devices, combination products, or infant formula. They are also exempt if they are part of the collection or processing of clinical care data indicating real-world performance or safety of products, or post-marketing surveillance data necessary to support or maintain FDA authorization, provided the data are de-identified.

Licensing: As previewed in the ANPRM, the proposed rule authorizes the Department to issue general licenses to authorize certain categories of otherwise prohibited or restricted transactions under specified conditions. Transactions meeting these conditions would not require further authorization and could, for example, ease sector-specific by authorizing orderly wind-down conditions for covered data transactions. As also previewed in the ANPRM, the proposed rule authorizes the Department to issue specific licenses for specific transactions by parties who apply for and disclose details of their intended transactions in a license application to the Department. The proposed rule sets out the requirements and procedures for the issuance of general and specific licenses, including the process to apply for a specific license or seek reconsideration of a denied license based on new information.

Guidance and Advisory Opinions: As previewed in the ANPRM, the proposed rule permits the Department to issue general public guidance to address frequently asked questions and common issues, as well as advisory opinions to address the applicability of the regulations to specific

transactions. The proposed rule permits regulated parties to request advisory opinions about the interpretation and application of the regulations to actual specific transactions, not hypothetical situations.

Compliance Obligations: As previewed in the ANPRM, the proposed rule would not prescribe general due-diligence, recordkeeping, reporting, or other compliance requirements across the U.S. economy or across all data transactions. Instead, like compliance under economic-sanctions programs administered by the Department of the Treasury's Office of Foreign Assets Control, U.S. companies and individuals would be expected to develop and implement compliance programs based on their individualized risk profiles. These risk-based compliance programs may vary depending on a range of factors such as the company's size and sophistication, products and services, customers and counterparties, and geographic locations. If a violation occurs, the Department would consider the adequacy of the compliance program in any enforcement action.

As also previewed in the ANPRM, the proposed rule would establish affirmative compliance obligations as conditions for U.S. persons that engage in a restricted transaction. These affirmative compliance obligations would include implementing 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. These conditions would also include 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 for 10 years documenting data transfer methods, transaction dates, agreements, licenses, advisory opinions, and any relevant documentation received or created in connection with the transactions.

Reporting Requirements: As previewed in the ANPRM, the proposed rule would establish certain reporting requirements to ensure compliance with these rules and safeguard national security, including:

- 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.

Enforcement: Similar to other IEEPA-based programs, the proposed rule permits the Department to conduct investigations, hold hearings, examine and depose witnesses, and issue subpoenas for witnesses and documents related to any matter under investigation. Violations can result in civil

and criminal penalties. Civil penalties, which are subject to the Federal Civil Penalties Inflation Act, can be up to $368,136 or twice the amount of the transaction involved, whichever amount is greater. The proposed rule establishes the processes for the Department to issue findings of violations and civil penalties, including an opportunity for parties to respond before the Department issues a penalty. Willful violations, on the other hand, can lead to criminal fines up to one million dollars ($1,000,000) and up to 20 years imprisonment.

The Department welcomes public comment on the proposed rule. You may send comments, identified by Docket No. NSD 104, through the Federal eRulemaking Portal at https://www.regulations.gov. Follow the instructions in the NPRM for sending comments.

For press inquiries, please contact DOJ's Office of Public Affairs. For all other inquiries about the rule, please contact NSD.FIRS.datasecurity@usdoj.gov.

Frequently Asked Questions

- **What has been the process for establishing the program?**
  - On Feb. 28, the President issued Executive Order (E.O.) 14117, Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern, to address the unusual and extraordinary threat to the national security and foreign policy of the United States posed by the continuing efforts of countries of concern to access Americans' bulk sensitive personal data and U.S. Government-related data. On March 5, 2024, the Department published an Advance Notice of Proposed Rulemaking (ANPRM) in the Federal Register with a 45-day period for public comment. The Department carefully considered the comments on the ANPRM in subsequently issuing the Notice of Proposed Rulemaking (NPRM). The Department will carefully consider the comments on the NPRM in preparing and issuing the final rule. Companies and individuals will be required to comply with the regulations only after the final rule becomes effective.

- **What part of the Department is responsible for implementing this authority?**
  - The Department of Justice's National Security Division will implement this authority, working closely with other Department components as appropriate and in coordination with the Department of Homeland Security and other agencies.

- **How long do I have to provide comments on the proposed rule?**
  - The comment period is 30 days from the date of publication in the Federal Register. Comments should be submitted via https://www.regulations.gov.

- **What will change for the private sector when the NPRM is issued?**
  - Nothing. Issuance of the NPRM will not impose any new legal obligations. The NPRM is not the final rule and does not take immediate effect.

- **Once in effect, who must comply with the final rule?**

- All U.S. persons must comply with the final rule, once in effect. Non-U.S. persons will also be subject to certain prohibitions of the final rule. For example, 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 final rule.

- **How will the proposed rule's restrictions on investment agreements interact with CFIUS?**
  - The proposed rule prescribes prospective and categorical rules to regulate a broad set of commercial transactions and relationships that afford countries of concern access to Americans' bulk sensitive personal data or government-related data, to include some investment agreements. The rule reflects a shift from relying solely on CFIUS's case-by-case approach to address transactions that parties voluntarily file to supplementing CFIUS's approach with more generally applicable, categorical data-security rules that govern a foreign investment from the outset. Where a transaction involves an investment agreement that is also a CFIUS covered transaction, the proposed rule's security requirements for a restricted transaction would apply until CFIUS takes certain actions. If CFIUS enters into a mitigation agreement that imposes data security-related mitigations that are more stringent than those required by the proposed rule or if CFIUS imposes an interim order or requires a transaction be abandoned or unwound, then the requirements of the proposed rule no longer apply. Additional details about how the proposed rule would interact with other authorities are discussed in part IV.K of the NPRM's preamble.

- **How will the proposed rule's restrictions on vendor agreements interact with the authorities exercised by the Department of Commerce's Office of Information and Communications Technology and Services (OICTS)?**
  - Generally, ICTS authorities focus on vendor transactions that involve information and communications technology or services designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries and that otherwise poses an unacceptable risk to U.S. national security. The proposed rule prescribes forward-looking, categorical rules and/or imposes security requirements across certain vendor agreements, some of which could also be subject to an action by the Department of Commerce pursuant to E.O. 13873. In these instances, the proposed rule would set a baseline of security requirements for such an agreement, while still allowing Commerce to take more stringent actions against a specific vendor, transaction, or class of ICTS beyond those requirements established by the proposed rule. Additional details about how the proposed rule would interact with other authorities are discussed in part IV.K of the NPRM's preamble.

- **Does this proposed rule ban apps or social-media platforms sourced from foreign adversaries?**
  - No. This program will not ban apps or social-media platforms, and it will not be about any single app or technology. This program will address only the most

serious data-security risks (not all national-security risks, such as application security or disinformation) posed by only a subset of the data collected and used by apps and social-media platforms (sensitive personal data, not all data), and only with respect to a limited number of identified countries of concern. And this program will address only the national security risks of giving those countries of concern access to this data—not the broader domestic privacy challenges posed by social media. The NPRM excludes the regulation of transactions to the extent they involve expressive information under 50 U.S.C. § 1702(b)(3), such as videos, artwork, and publications.

- **Does this proposed rule regulate the domestic collection, processing, and use of data in the United States?**
    - No. The program would not regulate purely domestic transactions between U.S. persons—such as the collection, maintenance, processing, or use of data by U.S. persons within the United States—except to the extent that such U.S. persons are affirmatively and publicly designated as covered persons.

- **Does this proposed rule give the Department new surveillance authorities or the ability to track Americans' data?**
    - No. The program has nothing to do with the U.S. Government's authorities to lawfully engage in law-enforcement and national-security activities to gather intelligence. Moreover, the proposed rule categorically excludes the regulation of transactions to the extent they involve personal communications under 50 U.S.C. § 1702(b)(1).