FACT SHEET: Justice Department Will Issue Advance Notice of Proposed Rulemaking Following Forthcoming Groundbreaking Executive Order Addressing Access to Americans' Bulk Sensitive Personal Data by Countries of Concern

Background

Americans today generate a significant digital footprint that can, in the absence of protective measures, be exploited by countries of concern to the detriment of our national security. Countries of concern are buying Americans' sensitive personal data, and they are also accessing it through vendor, employment, investment, and other commercial relationships of companies subject to their jurisdiction. For example, countries of concern may use biometric, financial, genomic, geolocation, or health data, as well as personal identifiers, to understand Americans' patterns of life, spending and purchase habits, financial troubles, desires, likes and dislikes, visits to potentially sensitive locations like places of worship, government facilities, gambling venues, and health clinics, and information about locations and details of other sensitive locations and activities. Countries of concern can then use this data to engage in malicious cyber-enabled activities, espionage, coercion, influence, and blackmail; build profiles on and target activists, academics, journalists, dissidents, government personnel, political figures, and members of non-governmental organizations and marginalized communities for surveillance, influence, and intimidation; to curb dissent and for other nefarious purposes. Countries of concern are already applying advanced technologies, like big-data analytics, artificial intelligence, and high-performance computing, to more effectively manipulate, use, and act on sensitive data to enable their nefarious activities.

Even as the Department and the rest of the U.S. Government work to prosecute and block illicit means of obtaining this data, like computer hacking, our current laws leave open lawful access to vast amounts of Americans' sensitive personal data. Buying personal data and accessing it through other commercial relationships is currently legal in the United States. Our existing national-security authorities, like Committee on Foreign Investment in the United States (CFIUS) and Team Telecom, allow us to review and address these data-security risks on a case-by-case basis for discrete kinds of activities. However, no existing laws comprehensively and prospectively address the national security risks posed by access by countries of concern or covered persons subject to their jurisdiction or control to sensitive personal data through commercial transactions. This targeted new program will be designed to address this gap in our national security authorities.

Executive Order and ANPRM

President Biden will issue this groundbreaking E.O. under the International Emergency Economic Powers Act (IEEPA), which vests the President with authority to deal with extraordinary threats to national security that have their source in whole or in part outside the United States. In tandem with the issuance of the E.O., the Department will issue an Advance Notice of Proposed Rulemaking (ANPRM) to provide additional details on the proposed rules and to provide notice and solicit comment from the public.

The E.O. will direct the Department, in consultation with other relevant federal agencies, to issue regulations addressing transactions that involve U.S. persons' bulk sensitive personal data or U.S. Government-related data, that pose an unacceptable risk of access by countries of concern or covered persons subject to their jurisdiction, and that meet other criteria. As the lead implementing agency, the Department will work closely with other agencies in a whole-of-government effort to ensure that the program is carefully calibrated to address the most serious national security risks. In particular, the E.O. will give important roles to the Departments of State, Commerce, the Treasury, Homeland Security, and other agencies through robust interagency consultation requirements, including on rulemakings, licensing decisions, identifying countries of concern, and designating covered persons. The program will not be administered through a case-by-case review of data transactions. Instead, the Department's regulations will establish generally applicable and transparent rules for engaging in specific categories of data transactions with certain countries of concern or covered persons subject to their jurisdiction.

Countries of concern: The ANPRM will contemplate identifying six countries of concern: China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba, and Venezuela.

Covered persons: The program will regulate U.S. persons' data transactions with "covered persons" which will be defined categorically to include certain classes of entities and individuals subject to the jurisdiction, direction, ownership, or control of countries of concern because, as a legal and practical matter, providing data to these persons will place that data within the reach of the countries of concern. The E.O. will define four categories of covered persons: (1) "an entity owned by, controlled by, or subject to the jurisdiction or direction of a country of concern"; (2) "a foreign person who is an employee or contractor of such an entity"; (3) "a foreign person who is an employee or contractor of a country of concern"; and (4) "a foreign person who is primarily resident in the territorial jurisdiction of a country of concern." As described in the forthcoming E.O. and ANPRM, anyone who is a U.S. citizen, national, or lawful permanent resident; anyone admitted to the United States as a refugee or granted asylum; any entity organized solely under U.S. laws or jurisdiction; and any person located in the United States would not fall into these categories of covered persons. The E.O. will also authorize the Department to supplement these categories of covered persons by designating specific entities or individuals as covered persons if they meet certain criteria, such as being owned or controlled by or subject to the jurisdiction or direction of a country of concern or acting on behalf of a country of concern or another covered person. The Department intends to publish and regularly update this non-exhaustive list of designated covered persons to assist with compliance and provide greater clarity about particular individuals and entities.

Sensitive personal data: The E.O. will define "sensitive personal data" to mean "covered personal identifiers, geolocation and related sensor data, biometric identifiers, human 'omic data, personal health data, personal financial data, or any combination thereof, as further defined in regulations issued by the Attorney General pursuant to section 2 of th[e] order, and that could be exploited by a country of concern to harm United States national security if that data is linked or linkable to any identifiable United States individual or to a discrete and identifiable group of United States individuals." As the ANPRM will describe in more detail, the contemplated program would further refine the scope of these sensitive personal data categories to regulate: (1) specifically listed categories and combinations of covered personal identifiers (not all personally identifiable information); (2) precise geolocation data; (3) biometric identifiers; (4) human genomic data; (5) personal health data; and (6) personal financial data. "Sensitive personal data" will not include data that is a matter of public record, such as court records or other government records, that is lawfully and generally available to the public; personal communications under 50 U.S.C. § 1702(b)(1); or expressive information under 50 U.S.C. 1702(b)(3) such as videos, artwork, or publications. In addition, before the Department can regulate data transactions involving types of human 'omic data other than human genomic data, the E.O. will require a report and recommendation assessing the risks and benefits of potentially doing so.

Bulk thresholds and U.S. Government-related data: The program will generally regulate the specified categories of data transactions in the six categories of sensitive personal data only if the transactions exceed prescribed bulk volumes (i.e., a threshold number of U.S. persons or U.S. devices). However, those bulk volumes would not apply to transactions involving certain U.S. Government-related data: the program will regulate data transactions involving sensitive personal data on U.S. Government personnel or locations regardless of the volume of such data. For U.S. Government-related data on personnel, the ANPRM will contemplate focusing on sensitive personal data that a transacting party (like a data broker) markets as linked or linkable to current or recent former employees or contractors, or former senior officials, of the federal government, including the Intelligence Community and military. For U.S. Government-related data on locations, the ANPRM will contemplate focusing on geolocation data that is linked or linkable to certain sensitive locations within geofenced areas that the Department would specify on a public list.

Covered data transactions*:* Under the forthcoming E.O., the Department will identify categories of highly sensitive data transactions that will be prohibited as well as categories of restricted transactions that may proceed on the condition that they comply with predefined security requirements to mitigate access to the data by countries of concern. The forthcoming ANPRM contemplates identifying two categories of prohibited data transactions between U.S. persons and countries of concern or covered persons: (1) data-brokerage transactions, and (2) genomic-data transactions involving the transfer of bulk human genomic data or biospecimens from which such data can be derived. The ANPRM will contemplate identifying three categories of restricted data transactions: (1) vendor agreements involving the provision of goods and services (including cloud-service agreements); (2) employment agreements; and (3) investment agreements. The security requirements applicable to these restricted transactions will be established by the Department of Homeland Security's Cybersecurity and Infrastructure Agency. These security requirements will be designed to mitigate the risk of access by countries of concern or covered persons and may include cybersecurity measures such as basic

organizational cybersecurity posture requirements, physical and logical access controls, data masking and minimization, and the use of privacy-preserving technologies.

Exempt data transactions: Under the forthcoming E.O. and ANPRM, the program will contain several across-the-board exemptions for data transactions that would be excluded from regulation to the extent that they are:

(1) ordinarily incident to and part of financial services, payment processing, and regulatory compliance (such as banking, capital-markets, or financial-insurance activities; financial activities under the purview of other regulators; the provision or processing of payments involving the transfer of personal financial data or covered personal identifiers for the purchase and sale of goods and services; and legal and regulatory compliance);

(2) ordinarily incident to and part of ancillary business operations (such as payroll or human resources) within multinational U.S. companies;

(3) activities of the U.S. Government and its contractors, employees, and grantees (such as federally funded health and research activities, which the funding agencies will regulate themselves); or

(4) transactions required or authorized by federal law or international agreements (such as the exchange of passenger-manifest information, INTERPOL requests, and public-health surveillance).

The forthcoming ANPRM also contemplates exempting certain investments that do not convey the rights or influence that ordinarily pose an unacceptable national-security risk of giving countries of concern or covered persons access to sensitive personal data.

Licensing and advisory opinions: As directed by the forthcoming E.O., the ANPRM will contemplate establishing processes for the Department to issue general and specific licenses and advisory opinions. General licenses will give the Department flexibility to exempt, alter the conditions for, or allow wind-down periods for certain categories of otherwise-regulated transactions. Specific licenses would give companies and individuals an opportunity to apply for an exception to the rules to engage in a specific data transaction, and the Department would make licensing decisions with the concurrence of the Departments of State, Commerce, and Homeland Security. Companies and individuals would also be able to request advisory opinions about the application of the regulations to specific transactions.

In addition to directing the establishment of this targeted new program, the E.O. will take three additional steps to enhance existing authorities to address data-security risks:

- For U.S. telecommunications infrastructure, the E.O. will direct the Committee for the Assessment of Foreign Participation in the U.S. Telecommunications Services Sector (Team Telecom), which is chaired by the Attorney General, to prioritize reviewing existing licenses for submarine cable systems owned or operated by country-of-concern entities or landing in a country of concern; to publicly issue policy guidance regarding

reviews of license applications, including the assessment of third-party data-security risks; and to take further steps to address data-security risks on an ongoing basis.

- For the U.S. health care market, the E.O. will direct the Departments of Defense, Health and Human Services, and Veterans Affairs, and the National Science Foundation, to consider taking steps to use their existing grantmaking and contracting authorities to prohibit federal funding that supports, or to otherwise mitigate, the transfer of sensitive health data and human genomic data to countries of concern and covered persons.

- For consumer protection, the E.O. will encourage the Consumer Financial Protection Bureau to consider taking steps to address the role that data brokers play in contributing to these national-security risks, including by continuing to pursue the rulemaking proposal under the Fair Credit Reporting Act identified at the September 2023 Small Business Advisory Panel for Consumer Reporting Rulemaking.

The proposed regulations will be targeted to address national security risks while minimizing the impact on economic and other activities, and will be designed to safeguard the continued cross-border data flows that are vital to our economy and communities. The U.S. Government's long-standing position on data flows have allowed for targeted restrictions on data flows that are necessary to meet national security needs. These actions not only align with the United States' longstanding support for the trusted free flow of data but also are consistent with U.S commitment to an open internet with strong and effective protections for individuals' privacy and measures to preserve governments' abilities to enforce laws and advance policies in the public interest. The Department will continue its engagements with stakeholders, including technology companies and advocates for privacy, safety, labor, and human rights, to move forward in a way that appropriately balances all these objectives.

Frequently Asked Questions

- ***What is the process for establishing the program?***

    - The E.O. and the ANPRM will not impose any immediate new legal obligations. Instead, the issuance of the E.O. and ANPRM will initiate two rounds of formal opportunities for the public to provide feedback on the contemplated program before any final rule is issued. On February 28, 2024, the Department will release an ANPRM, which is being published in the Federal Register with a 45-day period for public comment. The Department will carefully consider the comments on the ANPRM in subsequently preparing and issuing a notice of proposed rulemaking (NPRM), which will be published in the Federal Register for public comments. The Department will then carefully consider the comments on the NPRM in subsequently preparing and issuing the final rule. Companies and individuals will be required to comply with the regulations only after the final rule becomes effective.

- ***Does this E.O. give the Department new surveillance authorities or the ability to track Americans' data?***

    - No. This 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 forthcoming E.O. and ANPRM categorically exclude the regulation of transactions to the extent they involve personal communications under 50 U.S.C. § 1702(b)(1).

- ***Does this E.O. 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. Both the E.O. and ANPRM will categorically exclude 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 E.O. 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 acting on behalf of a country of concern.

- ***Would the program regulate data transactions between the United States and countries that are not countries of concern?***

    - The forthcoming ANRPM contemplates regulating only U.S. persons' data transactions in which a country of concern or covered person is a party, with only one limited exception (other than cases of evasion or circumvention): To address the risk that data is "re-exported" by foreign third parties to countries of concern, the program would allow a U.S. person to engage in a data-brokerage transaction with a foreign person that is not a covered person on the condition that the foreign person agree not to resell or give access to a country of concern or covered person.

- ***How does this new program align with existing authorities, such as CFIUS, Team Telecom, the Department of Commerce's ICTS program, and export controls?***

    - This program will complement and build upon existing authorities, offering additional protections for Americans' sensitive personal data and closing some gaps in our national-security authorities:

    - **CFIUS and Team Telecom** review only discrete kinds of transactions only on a transaction-by-transaction basis. Those authorities are not designed to provide prospective, categorical rules to address risks posed by commercial activities that involve the outright sale of data to countries of concern, or vendor or employment relationships that facilitate access to Americans' sensitive personal data by countries of concern.

    - The Department of Commerce's **ICTS program** regulates transactions and classes of transactions involving foreign-adversary-produced information and communications technologies and services used in the United States. By contrast, this data-security program will regulate transactions involving Americans' sensitive personal data that may be transferred to countries of concern.

    - **Export controls** are used to address the transfer of sensitive U.S. products and technologies and prevent countries of concern from acquiring and using them for malign purposes. But they do not address the flow of sensitive personal data itself or the counterintelligence and related risks posed by such data.

- ***How will U.S. companies and individuals be expected to comply with this program?***

    - As the forthcoming ANPRM describes in more detail, the contemplated program would not prescribe general due-diligence requirements, affirmative recordkeeping requirements, or affirmative reporting requirements across the U.S. economy. Instead, the contemplated program would use a familiar approach to compliance modeled on the IEEPA-based 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, which may vary depending on a range of factors such as their 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. The ANPRM contemplates establishing affirmative recordkeeping and reporting requirements only in discrete circumstances (as a condition of engaging in a restricted transaction or pursuant to a general or specific license).

- ***What are the penalties for violations of the program?***

    - The E.O. will authorize the Department of Justice to investigate violations of the regulations, including pursuing civil and criminal remedies available under IEEPA. As the forthcoming ANPRM describes, the Department is considering establishing

civil penalties for violations. The specific penalty for any particular violation would depend on the facts and circumstances of the violation, including the adequacy of any compliance program.