SULLIVAN & CROMWELL LLP

S&C memo

March 1, 2024

President Biden Issues Executive Order Granting Authorities to Regulate the Transfer of Sensitive U.S. Data to Countries of National Security Concern

Accompanying Advance Notice of Proposed Rulemaking by the U.S. Department of Justice Signals Forthcoming Regulatory Framework

SUMMARY

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" (the "Executive Order"), delegating new authorities to the U.S. Department of Justice ("DOJ") and other agencies to regulate the transfer of sensitive U.S. data to countries of national security concern. The Executive Order focuses primarily on personal and other sensitive information, such as U.S. persons' financial information, biometric data, personal health data, geolocation data, and information relating to government personnel and facilities.[1]

The Executive Order directs the DOJ to take the lead in issuing regulations that will prevent the large-scale transfer of sensitive data to "countries of concern," and to establish greater protections for sensitive government-related data, including geolocation information pertaining to federal personnel and sensitive government sites.[2] Additionally, it directs the DOJ to work with the Department of Homeland Security to develop security standards to prevent access by countries of concern to Americans' data through commercial means.[3] It further instructs the DOJ to coordinate its implementation with other federal agencies, and directs those agencies to take additional steps related to the protection of sensitive U.S. data.

Simultaneous with the issuance of the Executive Order, the DOJ issued an Advance Notice of Proposed Rulemaking ("ANPRM"). The ANPRM provides public notice of the DOJ's implementation plan, describes the potential contours of the forthcoming regulatory regime, and solicits public comments.[4] The ANPRM identifies the six countries of concern that it anticipates will be a focus of new DOJ regulations: China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba, and Venezuela.[5] The publication of the ANPRM commences a 45-day public comment period.[6] The Executive Order directs that within 180 days of the order's issuance (August 26, 2024), the DOJ must issue a Notice of Proposed Rulemaking containing the DOJ's proposed regulations.[7]

EXECUTIVE ORDER

President Biden issued the Executive Order pursuant, in part, to the International Emergency Economic Powers Act (IEEPA), which grants the President the power to address extraordinary national security threats that originate in whole or in part outside the United States, and is also a key authorizing statute for existing U.S. sanctions regulations administered by the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC").[8]

The Executive Order seeks to address threats associated with the transfer of bulk sensitive personal data and government-related data to countries of concern.[9] In recent years, national security and data privacy experts have expressed concerns about foreign actors' ability to purchase or otherwise obtain sensitive personal data about U.S. persons, including government and military personnel, due to significant regulatory gaps in U.S. laws governing financial and consumer data. The order notes that countries of concern use such 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[.]"[10] It further notes that the restrictions will be "specific, carefully calibrated actions," and 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[.]"[11]

The Executive Order, among other things, directs the Attorney General to issue regulations that prohibit or restrict U.S. persons from engaging in certain activities and data transactions.[12] The order grants the DOJ both regulatory and criminal authority to enforce the proposed rules.[13]

DEPARTMENT OF JUSTICE RULEMAKING

In announcing the DOJ's ANPRM, Attorney General Merrick Garland noted that "[o]ur adversaries are exploiting Americans' sensitive personal data to threaten our national security," including by "purchasing this data to use blackmail and surveil individuals, target those they view as dissidents here in the United

States, and engage in other malicious activities."[14] Assistant Attorney General for the National Security Division Matthew G. Olsen similarly stated, "[t]oday's announcement fills a key gap in our national security authorities, affording the Justice Department a new and powerful enforcement tool to protect Americans and their most sensitive information from being exploited by our adversaries."[15]

The DOJ's ANPRM sets forth the currently contemplated regulatory framework, which would establish "generally applicable and transparent rules for [U.S. persons] engaging in specific categories of data transactions" with the relevant countries of concern and with so-called "covered persons" who are subject to the jurisdiction or control of those countries.[16] As detailed below, this program would significantly mirror the existing 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.

The ANPRM proposes defining 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."[17] The DOJ anticipates that its regulations will classify certain transactions as either "prohibited" or "restricted" depending on the sensitivity of the transaction.[18] "Prohibited transactions" would be forbidden in their entirety.[19] "Restricted transactions," by contrast, would be prohibited only if they do not comply with specified security requirements developed by the Secretary of Homeland Security.[20]

The parameters and restrictions that the DOJ is currently contemplating—which are subject to public comment and specific questions raised in the ANPRM—include the following:

Covered Persons:

- The regulations would govern certain data transactions that U.S. persons conduct with so-called "covered persons" who fall under the jurisdiction, direction, ownership, or control of "countries of concern," and whose receipt of the data would therefore place it within reach of a country of concern.[21]
- Covered persons would be defined as entities or individuals subject to the jurisdiction, direction, ownership, or control of the six countries of concern (China, Russia, Iran, North Korea, Cuba, and Venezuela) and would include:
  - entities owned by, controlled by, or subject to the jurisdiction or direction of a country of concern;
  - foreign persons who are employees or contractors of such entities;
  - foreign persons who are employees or contractors of a country of concern;
  - foreign persons who are primarily residents in the territorial jurisdiction of a country of concern; and
  - foreign persons identified in a public list of persons determined to be covered persons by the DOJ.[22]

- The above definition would include any entity that is 50 percent or more owned, directly or indirectly, by a country of concern, or that is organized or chartered under the laws of, or has its principal place of business in, a country of concern, even if the company is private.[23]
- The regulations would exclude from this definition U.S. citizens, nationals, or lawful permanent residents; any persons admitted to the United States as refugees or granted asylum; any entities organized solely under U.S. laws or jurisdiction; and any person located in the United States.[24]
- Significantly, the Executive Order authorizes the DOJ to "supplement these categories of covered persons by designating specific entities or individuals as covered persons" if they meet certain criteria—including, for example, if they are owned and controlled by a country of concern or are acting on its behalf.[25] The DOJ has expressed an intent to publish and regularly update a non-exhaustive list of designated covered persons.[26]

Covered Data

The proposed rules described in the ANPRM would apply only to "covered data." As currently contemplated, this would include two categories, namely (i) bulk 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 Executive Order delegates to the DOJ the authority to define the amount of sensitive personal data that qualifies as "bulk." The covered sensitive personal data would include:
  - **covered personal identifiers**, [27] such as government identification numbers, financial account numbers, IP or MAC addresses, advertising identifiers, and login information;[28]
  - **geolocation and related sensor data**, limited to precise geolocation data that identifies the physical location of an individual or device within a narrow precision to be specified in the final regulations;[29]
  - **biometric identifiers**, such as facial images, voice prints and patterns, retina and iris scans, palm prints, fingerprints, gait, and keyboard usage patterns;[30]
  - **human 'omic data**, limited initially to human genomic data but to potentially include other data, such as proteomic, epigenomic, and metabolomic data;[31]
  - **personal health data**, including but not limited to information relating to payment for the provision of health care to an individual;[32] and
  - **personal financial data**, including banking information, credit card data, and credit reports."[33]
- Data that is a matter of public record, personal communications, or expressive information would not be classified as covered data.[34]

Government-Related Data

- The Executive Order defines "United States Government-related data" as "sensitive personal data that, regardless of volume, the Attorney General determines poses a heightened risk of being exploited by a country of concern to harm United States national security" and that:
  - a transacting party identifies as being linked or linkable to categories of current or recent former employees or contractors, or former senior officials, of the federal government, including the military;

- is linked to categories of data that could be used to identify current or recent former employees or contractors, or former senior officials, of the federal government, including the military; or
- is linked or linkable to certain sensitive locations, the geographical areas of which will be specified publicly, that are controlled by the federal government, including the military.[35]

- The ANPRM also contemplates further defining government-related data to include precise geolocation data connected to such individuals or sensitive locations.[36]
- Unlike existing U.S. privacy laws, the ANPRM would not exempt data that has been anonymized, pseudonymized, de-identified, or encrypted.[37]

Covered Transactions

- The proposed regulations would only apply to "covered data transactions," currently anticipated to include only (1) data brokerage transactions, (2) vendor agreements, (3) employment agreements, and (4) investment agreements.[38] Notably, and as described below, the DOJ does not currently intend for covered transactions to encompass, among others, those ordinarily incident to financial services or transactions that are required or authorized by federal law or international agreements.[39]
- In addition, and as noted above, the program would regulate bulk transactions that exceed a prescribed volume, determined by the number of U.S. persons or devices.[40] The DOJ is considering, and has published in the ANPRM, specific volume thresholds for each category of data, based on the data's vulnerability to exploitation by a country of concern and the potential consequences of such exploitation.[41] The ANPRM contemplates that datasets exceeding any of the following thresholds would present a high risk of exploitation by a country of concern: covered personal identifiers, personal health data, or personal financial data of more than 1,000,000 U.S. persons; biometric identifiers or precise geolocation data of more than 10,000 U.S. persons or U.S. devices, respectively; and human genomic data of more than 1,000 U.S. persons.[42] If a U.S. person engages in multiple covered transactions involving the same foreign person or covered person, the DOJ would aggregate data across the preceding 12 months to determine whether a threshold has been exceeded.[43]
- The ANPRM also contemplates regulating certain transactions between U.S. persons and foreign parties that are *not* countries of concern or covered persons. Specifically, the DOJ is considering a provision which would provide that "no U.S. person . . . may knowingly engage in a covered data transaction involving data brokerage with any foreign person unless the U.S. person contractually requires that the foreign person refrain from engaging in a subsequent covered data transaction involving the same data with a country of concern or covered person."[44] The DOJ notes that this potential requirement would "address the risk that data is 're-exported' by foreign third parties to countries of concern."[45]

Exempt Transactions

- Similar to OFAC's approach in IEEPA-based sanctions, the DOJ would exempt certain transactions from these restrictions and prohibitions. The following categories, among others, may be excluded from the definition of covered transactions:
  - personal communications that do not involve the transfer of something of value[46] or information or informational materials;[47]
  - transactions ordinarily incident to financial services, payment processing, and regulatory compliance, such as banking, capital markets, or financial insurance activities;
  - intra-entity transactions incident to and part of ancillary business operations within multinational U.S. companies, such as payroll or human resources;

- activities of the U.S. Government, its contractors, employees, and grantees; and
- transactions required or authorized by federal law or international agreements.[48]

Scope of Prohibited vs. Restricted Transactions

- The status of U.S. persons' transactions as either "prohibited" or "restricted" would depend on the particular category of transaction involved.

Prohibited Transactions

- The ANPRM would completely prohibit U.S. persons from knowingly engaging in a transaction with a country of concern or covered person that involves covered data and that is either a (i) data brokerage transaction or (ii) genomic data transaction involving the transfer of bulk human genomic data (or biospecimens from which such data can be derived).[49]
- The DOJ intends for "knowledge" to encompass those who knew *or should have known* of the circumstances of the transaction.[50] The DOJ is also considering rules to prohibit evasion of the regulations, causing violations by others, attempts, and conspiracies.[51]

Restricted Transactions

- The ANPRM 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.[52]

Licensing and Advisory Opinions

- The DOJ would issue general and specific licenses as appropriate.[53] General licenses would allow exemptions, alterations, or wind-down periods for particular categories of regulated transactions, while specific licenses would permit exceptions for specific transactions.[54] The DOJ is considering certain requirements for specific licenses, such as ongoing reporting obligations and providing assurances that any data transferred in the transaction can be recovered, irretrievably deleted, or otherwise rendered non-functional.[55] The DOJ intends to make licensing decisions in consultation with relevant federal departments, such as the Departments of State, Commerce, and Homeland Security.[56] The DOJ is also considering a program to provide guidance through written advisory opinions, similar to the processes used by OFAC.[57]

Penalties

- The DOJ is also considering establishing a process for imposing civil monetary penalties similar to those followed by OFAC and the Committee on Foreign Investment in the United States (CFIUS).[58] Of particular relevance for business organizations, the DOJ has stated that the specific penalty for any violation would depend on the facts and circumstances of the violation, including the adequacy of an organization's compliance program.[59] In addition, while the DOJ is not currently planning broad implementation of due diligence, recordkeeping, or affirmative reporting requirements, it is considering imposing due diligence and recordkeeping requirements in certain circumstances, including as a condition of engaging in a restricted covered data transaction or as a condition of a general or specific license.[60] These requirements would include "know your vendor and "know your customer" requirements.[61]

IMPLEMENTATION BY OTHER AGENCIES

The Executive Order and the accompanying ANPRM take a "whole-of-government" approach, and several agencies beyond the DOJ will be involved in implementing policy under the Executive Order.

- For the telecom industry, the Executive Order directs 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, among other things, prioritize review of existing licenses for submarine cable systems owned or operated by country-of-concern entities or landing in a country of concern.[62]
- For the health care sector, the Executive Order directs the Departments of Defense, Health and Human Services, and Veterans Affairs, and the National Science Foundation, to consider taking steps to use their existing 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.[63]
- For consumer protection, the Executive Order encourages 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 a rulemaking proposal that would classify certain data brokers as consumer reporting agencies with attendant regulatory obligations.[64]

OBSERVATIONS AND IMPLICATIONS

The proposed framework represents a potentially expansive new regulatory regime that could have far-reaching consequences for the data privacy obligations of organizations operating in the United States and their employees. Once the regulations are implemented, the DOJ will have the power to investigate violations of these rules and to pursue civil and potential criminal penalties against individuals and entities pursuant to IEEPA.

Because the DOJ has modeled the proposed framework after the IEEPA-based economic sanctions regime and will evaluate business organizations' violations in light of the adequacy of their compliance programs, the regulations will likely require careful rethinking of legal and compliance risks.[65] Sanctions expertise will be helpful in navigating the new terrain. As with the existing IEEPA-based sanctions regime, companies and financial institutions will need to develop and implement compliance programs commensurate with their individualized risk profiles, looking to factors such as the size and sophistication of their data collection and products and services, customers and counterparties, and the location and nature of services provided by vendors. Accordingly, multinational organizations that handle or interact with the data of U.S. persons should begin to consider how to build these considerations into their business operations and their legal and compliance programs. Moreover, given the broad definition of "covered persons," organizations will need to consider conducting diligence on the ownership and control of counterparties to determine whether they fall within that definition. Further, organizations that may be substantially affected by these regulations should consider participating in the public comment process for

the ANPRM. This initial comment period could present an early opportunity for these organizations to help shape this new regulatory regime.

The ANPRM will be subject to a 45-day comment period following publication in the Federal Register. The DOJ will then consider the comments and issue a notice of proposed rulemaking (NPRM), which will be published in the Federal Register for public comments. After considering the comments during the NPRM, the DOJ will then issue a final rule.

* * *

ENDNOTES

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

2 *Id.*

3 White House, *Fact Sheet: President Biden Issues Executive Order to Protect Americans' Sensitive Personal Data* (Feb. 28, 2024), *available at* https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/28/fact-sheet-president-biden-issues-sweeping-executive-order-to-protect-americans-sensitive-personal-data/.

4 Department of Justice, *Unofficial ANPRM: Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern* (Feb. 28, 2024) (the "ANPRM"), *available at* https://www.justice.gov/d9/2024-02/unofficial_signed_anprm.pdf.

5 *Id.* at *40.

6 Department of Justice, *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* (Feb. 28, 2024) (the "DOJ Fact Sheet"), *available at* https://www.justice.gov/d9/2024-02/data_security_eo_fact_sheet.pdf.

7 Executive Order § 2(c).

8 Executive Order; 50 U.S.C. § 1701 et seq.

9 Executive Order § 1.

10 *Id.*

11 *Id.*

12 *Id.* at § 2(a).

13 DOJ Fact Sheet at *7-8.

14 Department of Justice, *Justice Department to Implement Groundbreaking Executive Order Addressing National Security Risks and Data Security* (Feb. 28, 2024) (the "DOJ Press Release"), *available at* https://www.justice.gov/opa/pr/justice-department-implement-groundbreaking-executive-order-addressing-national-security.

15 *Id.*

16 DOJ Fact Sheet at *2.

17 ANPRM at *32.

18 *Id.* at *11.

19 *Id.*

20 *Id.*

21 *Id.* at *41.

22 *Id.* at *41-42.

23 *Id.* at *42.

24 *Id.* at *41-43.

25 DOJ Fact Sheet at *2.

ENDNOTES (CONTINUED)

26 ANPRM at *43-45.

27 It should be noted that the term "covered personal identifiers" would be narrower than the categories covered by many other laws and policies aimed at protecting personal privacy. The ANPRM specifically disclaims categories such as employment history, educational history, organizational membership, criminal history, and web-browsing history from the definition of covered personal identifiers.

28 ANPRM at *17-22.

29 *Id.* at *22.

30 *Id.* at *22-23.

31 *Id.* at *23; Executive Order § 6.

32 ANPRM at *23.

33 *Id.*

34 Executive Order § 7(l); ANPRM at *23-24, 54.

35 Executive Order § 7(m).

36 ANPRM at *30.

37 ANPRM at *25.

38 *Id.* at *32.

39 *Id.* at *53-54.

40 *Id.* at *24.

41 *Id.* at *24-25.

42 ANPRM at *25.

43 ANPRM at *24.

44 *Id.* at *50.

45 DOJ Fact Sheet at *6.

46 *See* 50 U.S.C. § 1702(b)(1).

47 *See* 50 U.S.C. § 1702(b)(3).

48 ANPRM at *53-56.

49 *Id.* at *12-13.

50 *Id.* at *48-49.

51 *Id.* at *50-51.

52 *Id.* at *13-14.

53 *Id.* at *61-63, 65-66.

54 *Id.* at *61-63.

55 *Id.* at *63.

56 *Id.* at *61.

57 *Id.* at *65.

ENDNOTES (CONTINUED)

58 *Id.* at *71.

59 *Id.*; DOJ Fact Sheet at *7-8.

60 ANPRM at *68-69.

61 *Id.*

62 Executive Order § 3(a).

63 *Id.* § 3(b).

64 *Id.* § 3(c); Consumer Financial Protection Bureau, *Remarks of CFPB Director Rohit Chopra at White House Roundtable on Protecting Americans from Harmful Data Broker Practices* (Aug. 15, 2023), *available at* https://www.consumerfinance.gov/about-us/newsroom/remarks-of-cfpb-director-rohit-chopra-at-white-house-roundtable-on-protecting-americans-from-harmful-data-broker-practices/.

65 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).

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.