JENNER & BLOCK

White House Executive Order Seeks to Protect Americans' Sensitive Personal Data and US Government-Related Data in Cross-Border Transactions

Client Alerts

March 7, 2024
By: Shoba Pillay, Madeleine Findley

On February 28, 2024, President Biden issued Executive Order 14117 on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern (the EO).[1] The EO empowers the US government, led by the Department of Justice (DOJ), in coordination with other federal entities, to prevent US adversaries from accessing Americans' bulk sensitive personal data or US government-related data, which can be used for malicious purposes, including analysis and manipulation of such data to engage in espionage, influence, kinetic, and cyber operations against the United States.

Primarily, the EO:

- Prohibits and restricts transactions with certain US adversaries—"countries of concern"—that involve bulk US sensitive personal data or US Government-related data, subject to certain exemptions;
- Instructs DOJ, in coordination with the Department of Homeland Security (DHS) and in consultation with other federal agencies, to adopt regulations to prohibit specific classes of transactions that pose unacceptable national security risks by possibly enabling countries of concern to access bulk sensitive US personal data or US government-related data; and
- Instructs DOJ, in coordination with DHS and in consultation with other federal agencies, to adopt regulations to restrict other classes of such transactions by requiring compliance with security requirements established by DHS's Cybersecurity and Infrastructure Security Agency (CISA).[2]

As authorized by the EO, DOJ is contemplating, in coordination with DHS and in consultation with other federal agencies, the following:

- Proposing and adopting regulations to identify, prohibit, and restrict "covered data transactions," i.e., certain classes of transactions that involve transfers of bulk sensitive US personal data or US Government-related data to countries of concern or entities and individuals who are owned by, controlled by, or subject to the jurisdiction of such countries (covered persons);
- Defining six categories of bulk US sensitive personal data that covered data transactions may involve: US persons covered personal identifiers, personal financial data, personal health data, precise geolocation data, biometric identifiers, and human genomic data;
- Defining two categories of US government-related data that covered data transactions may involve: geolocation data for certain military, government, or other sensitive facilities and sensitive personal data linked to current or

former US employees, contractors, or senior officials; and

- Identifying China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba, and Venezuela as "countries of concern."[3]

DOJ has issued an Advance Notice of Proposed Rulemaking (ANPRM) pursuant to the EO and is seeking stakeholder input on the proposed regulations. This alert further overviews the categories of transactions targeted for regulation and highlights takeaways for public and private organizations to consider as DOJ prepares to establish and implement this new regulatory regime in the coming months.

Curbing National Security Risks Posed by Access to Sensitive US Personal and Government Data

The EO identifies "continuing efforts of countries of concern to access" Americans' bulk sensitive personal data and US government-related data as "an unusual and extraordinary threat … to the national security and foreign policy of the United States."[4]

Access to such sensitive data through "data brokerages, third-party vendors, employment and investment agreements … poses particular and unacceptable risks" to national security. Such "direct and unfettered access" can be used by countries of concern to intimidate, manipulate, or limit freedom of expression or civil liberties in ways that endanger US national security and undermine "democratic values, safeguards for privacy, and other human rights and freedoms." [5]

Among the many national security threats posed by countries of concern accessing bulk US sensitive personal data and US government-related data, the EO emphasizes four key areas of risk, among others, that it seeks to address:

- First, artificial intelligence (AI) capabilities of countries of concern may enable them to analyze and manipulate large amounts of US personal data and to build profiles on US persons, including US government and military personnel, for espionage, blackmail, and influence purposes. Moreover, countries of concern could use bulk US sensitive personal data and US government-related data to train and enhance their AI capabilities, allowing them to better exploit such data against US security interests.

- Second, access to bulk US sensitive personal data and US government-related data can be enabled through transmission of data via network infrastructure subject to the jurisdiction or control of countries of concern. This risk may be exacerbated where bulk sensitive data transits a submarine cable owned or controlled by or subject to the jurisdiction of a country of concern, and may be further exacerbated when a cable originates in the United States and terminates in a country of concern.

- Third, the EO prioritizes prohibiting or restricting data transfers involving personal health and human genomic information, including from US healthcare providers and research institutions, to countries of concern, in recognition of technological advances that may enable such countries to de-anonymize the data and thereby access exploitable health information of US persons.

- Fourth, the data brokerage industry collects, assembles, analyzes, and disseminates bulk US sensitive personal data and certain US government-related data regarding US consumers, enabling access to such data by countries of concern. The EO encourages the Consumer Financial Protection Bureau (CFPB) to enhance data brokerage compliance with federal consumer protection law to address this angle of the national security threat.[6]

Recognizing these unique and increasing national security threats, the president has authorized DOJ to issue regulations, pursuant to the International Emergency Economic Powers Act (IEEPA), the National Emergencies Act, and 3 U.S.C. § 301, to prohibit or otherwise restrict certain cross-border transactions that could grant countries of concern

access to Americans' bulk sensitive data or US government-related data. Concurrently, on February 28, 2024, the DOJ National Security Division issued an ANPRM,[7] proposing specific organizational, transactional, and compliance requirements for transactions involving access to bulk US sensitive personal data.

Both the EO and DOJ reaffirm the United States' longstanding commitments "to promoting an open, global, interoperable, reliable, and secure internet" and a strong global economy in which "cross-border data flows [are] required to enable international commerce[,] trade [and] investment."[8] To that end, the EO expressly rejects "generalized data localization requirements to store Americans' bulk sensitive personal data or United States government-related data within the United States or to locate computing facilities used to process Americans' bulk sensitive personal data or United States government-related data within the United States."[9] The exchange of "financial and other data as part of the sale of commercial goods and services," including with entities and individuals subject to the jurisdiction of countries of concern, are also expressly protected.[10]

Covered Data Transactions

The DOJ, in coordination with DHS and in consultation with other federal agencies, is authorized to propose and adopt regulations to prohibit certain classes of transactions that involve transfers of bulk US sensitive personal data or US government-related data to countries of concern or entities and individuals who are owned by, controlled by, or subject to the jurisdiction of such countries—i.e., "covered persons"—where such transactions are initiated, pending, or completed after the effective date of the issued regulations (covered data transactions).[11] The proposed rulemakings will be promulgated over multiple rounds based on priority. To the extent practicable, DOJ will model regulations on "existing regulations based on IEEPA," such as those administered by the Department of the Treasury's Office of Foreign Assets Control (OFAC) and the Department of Commerce's Bureau of Industry and Security (BIS).[12] In this first tranche, the ANPRM identifies the classes of transactions that pose the greatest national security risks and that will likely be subject to prohibition or restriction. The first proposed rulemaking will "target only transactions between a US person and a country of concern (or a covered person). Domestic transactions between US persons, who are *not* covered persons, will *not* be subject to regulation pursuant to this Executive Order."[13] DOJ is considering defining a "covered person" consistent with OFAC's definition of persons subject to its designation actions, including its "50 percent rule."[14]

In consultation with the Departments of State and Commerce, DOJ will determine the list of "countries of concern." Currently DOJ is considering regulating cross-border data transactions that involve China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba, and Venezuela, as the US government has determined that these countries are "engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States."[15] These risks stem not only from direct access to data by countries of concern, but also through entities and individuals that are subject to their ownership, control, or jurisdiction, particularly if a country of concern has laws that obligate entities and individuals to provide its government's intelligence services with access to bulk US sensitive personal data or US government-related data in its possession, which is why covered persons will also be targeted for regulation.

The classes of transactions that DOJ is currently considering for prohibition include:

- Data-brokerage transactions "between US persons and countries of concern (or covered persons)" involving "bulk US sensitive personal data or government-related data;" and
- Transactions that would provide "a country of concern or covered person with access to bulk human genomic data" or "human biospecimens from which that human genomic data can be derived."[16]

The classes of transactions that DOJ is currently considering for restriction include the following types of agreements to the extent they involve countries of concern or covered persons and bulk US sensitive personal data or US government-related data:

- Vendor agreements, including "agreements for technology services and cloud-service agreements;"
- Employment agreements; and
- Investment agreements.[17]

Restricted classes of data transactions will require compliance with certain security requirements developed by CISA. These requirements could include organizational cybersecurity measures, data minimization and masking, privacy controls, and audits.[18] Such security requirements will likely be based on the CISA Cybersecurity Performance Goals[19] and the National Institute of Standards & Technology ("NIST") Cybersecurity Framework,[20] Privacy Framework,[21] and SP 800-171 Rev. 3 ("Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations").[22][23]

All covered data transactions would necessarily involve defined categories of bulk US sensitive personal data and US government-related data, regardless of volume, as noted above.[24]

The EO requires the DOJ, in consultation with other federal agencies, including DHS and the Departments of Defense, Treasury, Commerce and State, to effectively protect these categories of sensitive American data in covered transactions. Additionally, DOJ will coordinate with the Departments of Defense, Health and Human Services (HHS), Veterans Affairs, and the National Science Foundation to "ensure that federal grants, contracts, and awards" do not enable countries of concern to access Americans' sensitive personal health data.[25]

However, unlike the Committee on Foreign Investment in the United States (CFIUS) or the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (Team Telecom), which review individual foreign investment transactions on a case-by-case basis for national security concerns in certain types of US businesses, the program that DOJ is charged with creating will take a categorical approach to prohibiting and restricting categories of transactions involving the classes of data identified above.[26] As a result, DOJ does not anticipate significant overlap between new regulations and current CFIUS and Team Telecom authorities because existing authorities do not authorize "prospective, categorical rules to address the national-security risks posed by transactions between US persons and countries of concern [or covered persons]" through which countries of concern may gain access to bulk US sensitive personal data or US government-related data.[27]

Exempt Data Transactions

DOJ is also proposing to establish certain classes of covered data transactions that would be exempt from prohibition or restriction and would create a process similar to OFAC's licensing regime by which DOJ would issue general and specific licenses.[28]

The ANPRM proposes creating five categories of exempted data transactions from the above prohibitions and restrictions. Those would include transactions that are:

- Ordinarily incident to and part of financial services, payment processing, and related regulatory compliance;
- Ordinarily incident to and part of ancillary back-office business operations, such as payroll or human resources within multinational US companies;

- US government activities, including those of its employees, contractors, and grantees, such as "federally funded health and research activities;"
- Required or authorized by federal law or international agreements, such as passenger-manifest information exchanges, INTERPOL requests, and public health monitoring; and
- Involving "personal communications" or "information or information materials."[29]

Compliance and Enforcement Regime

DOJ has proposed a compliance and enforcement regime modeled on OFAC's IEEPA-based economic sanctions compliance and enforcement regime.[30]

Compliance Program. US persons subject to the regulations would be required to develop, implement, and update a compliance program tailored to the US person's individualized risk profile, including its "size, sophistication, products and services, customers and counterparties, and geographic locations."[31] Such US persons would also be required to maintain records of their due diligence to comply with the regulations.[32]

Record Retention and Reporting Requirements. DOJ is also considering requiring US persons to keep complete records of information related to a covered data transaction and provide that information to DOJ pursuant to reporting requirements or upon request.[33] However, with regard to data privacy concerns such reporting requirements might give rise to the EO and implementing regulations do *not* provide the US government with new authority to access or monitor US persons' sensitive personal data or communications or US government-related data.[34]

Enforcement. Finally, DOJ is contemplating establishing a process for imposing civil monetary penalties modeled on the processes employed by OFAC and CFIUS, including "mechanisms for pre-penalty notice, an opportunity to respond, and a final decision."[35] To provide clarity for all entities and individuals potentially affected by these new regulations, DOJ would also establish an interpretive guidance program similar to those used by OFAC and BIS.[36]

Key Takeaways

The contemplated regulations could affect transactions across a wide range of industries, including transactions involving industry investors, including large institutional investors. Affected industries include but are not limited to: healthcare providers; research institutions; information technology service providers; technology companies that collect large amounts of users' personal information, including big-data analytics and artificial intelligence companies; social media companies; large online marketplaces; insurance providers; biotechnology companies; and ancestry and DNA testing companies; along with the employees, vendors, and other third parties with whom companies in such industries do business.

Potentially affected businesses should prepare for the proposal, adoption, and enforcement of these new DOJ regulations:

- Potentially affected businesses should monitor the rulemaking proceedings and consider filing or joining comments to better inform DOJ's proposed rules. DOJ is seeking public comment on all aspects of the proposed regulations and is particularly interested in comments from potentially affected businesses and industries on definitions of key terms, the scope of the data categories identified above, appropriate bulk thresholds for the identified data categories, and the scope of covered data transactions.
- Potentially affected businesses should consider reviewing whether their operations involve cross-border data transactions with any countries of concern or covered persons that include bulk amounts of US sensitive personal

data or US government-related data in anticipation of regulation.

- Potentially affected businesses should similarly consider reviewing their vendor, employment, and investment agreements in anticipation of regulation.

Potentially affected businesses should also be aware of the additional related developments likely to occur in the coming months in connection with the EO and this new regulatory regime:

- The EO encourages the CFPB to use its existing authorities to take further steps "to protect Americans from data brokers that are illegally assembling and selling extremely sensitive data, including that of US military personnel," to foreign persons. In line with that call to action, the CFPB has announced that it will propose such a rule later this year "to restrict certain activities by data brokers under the Fair Credit Reporting Act."[37]

- The EO also instructs Team Telecom to (1) prioritize "reviews of existing licenses for submarine cable systems that are owned or operated by persons owned by, controlled by, or subject to the jurisdiction or direction of a country of concern, or that terminate in the jurisdiction of a country of concern;" and (2) consider the national security risks specifically related to bulk transfers of Americans' sensitive data or US government-related data identified in this EO in reviewing any new applications or existing licenses. The EO further instructs Team Telecom to issue policy guidance to inform new applicants and current license holders of these new considerations, including assessment of third-party risks, concerning bulk US sensitive personal data or US government-related data.[38]

- The EO further instructs the Departments of Defense, HHS, Veterans Affairs, and the National Science Foundation to consider taking action, including issuing regulations consistent with existing authorizations of relevant federal assistance programs, to prohibit or restrict providing assistance that could enable countries of concern or covered persons to access bulk US sensitive personal data, including personal health and human genomic data. Additionally, these agencies, along with the State Department, FBI, and the Office of the Director of National Intelligence (ODNI), will consult with the White House to determine whether transactions involving other types of "human 'omic data," such as human proteomic, epigenomic, and metabolic data, should also be regulated.[39]

- Finally, the EO requests that DOJ, DHS, and ODNI recommend to the White House any "appropriate actions to detect, assess, and mitigate national security risks arising from prior transfers of United States persons' bulk sensitive personal data to countries of concern."[40] This recommendation contemplates that the US government may take action and/or issue regulations that implicate prior transfers of sensitive data to countries concern. As such, businesses should be aware that their prior transactions and agreements involving transferring sensitive data to countries of concern or covered persons could be subject to new scrutiny by the federal government.

We will continue to monitor developments and provide updates as new regulations are proposed and adopted and as US federal agencies begin to implement and enforce this new data transaction regulatory regime.

Footnotes

[1] Executive Order 14117, *Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern*, 89 FR 15421 at Sec. 1 (Feb. 28, 2024), https://www.whitehouse.gov/briefing-room/presidential-actions/2024/02/28/executive-order-on-preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related-data-by-countries-of-concern/.

[2] *Id.*, Sec. 2.

[3] *Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern,* Dep't of Justice Nat. Sec. Div., 12–14, 40 (Feb. 28, 2024), https://www.justice.gov/d9/2024-02/unofficial_signed_anprm.pdf, (hereinafter "ANPRM").

[4] EO 14117, Sec. 1.

[5] Fact Sheet, *President Biden Issues Executive Order to Protect Americans' Sensitive Personal Data,* White House (Feb. 28, 2024), 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/, (hereinafter "White House Fact Sheet").

[6] EO 14117, Secs. 1, 3.

[7] *Foreign Investment Review Section: Data Security*, U.S. Dep't of Just., https://www.justice.gov/nsd/data-security (last updated Feb. 29, 2024).

[8] EO 14117, Sec. 1.

[9] *Id.*

[10] *Id.*

[11] *Id.*, Sec. 2; ANPRM at 46-47.

[12] ANPRM at 12.

[13] *Id.* at 12.

[14] *Id.* at 42; *Entities Owned by Blocked Persons,* U.S. Dep't of the Treasury Office of Foreign Assets Control, https://ofac.treasury.gov/faqs/topic/1521#:~:text=OFAC%27s%2050%20Percent%20Rule%20states,blocked%20persons%20are%20considered%20blocked.

[15] ANPRM at 40.

[16] *Id.* at 13.

[17] *Id.* at 13.

[18] *Id.* at 10.

[19] *Cross-Sector Cybersecurity Performance Goals*, U.S. Dep't of Homeland Security Cybersecurity & Infrastructure Agency, https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf (last updated March 2023).

[20] *Cybersecurity Framework*, U.S. Dep't of Commerce Nat. Institute of Standards & Tech., https://www.nist.gov/cyberframework (last updated Feb. 26, 2024).

[21] *Privacy Framework,* U.S. Dep't of Commerce Nat. Institute of Standards & Tech., https://www.nist.gov/privacy-framework (last updated Jan. 16, 2020).

[22] Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, U.S. Dep't of Commerce Nat. Institute of Standards & Tech., NIST SP 800-171 Rev. 3, https://csrc.nist.gov/pubs/sp/800/171/r3/fpd (last updated Nov. 9, 2023).

[23] ANPRM at 59.

[24] *Id.* at 13–14; *supra* Executive Summary & n.3.

[25] White House Fact Sheet, *supra* n.5.

[26] ANPRM at 15.

[27] *Id.* at 74.

[28] *Id.* at 15, 61–64.

[29] ANPRM at 53–54 (noting that "personal communications" and "information or information materials" data are "statutorily exempt from regulation under IEEPA"); *see also* 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, Dep't of Justice, 4 (Feb. 28, 2024), https://www.justice.gov/opa/media/1340216/dl.

[30] ANPRM at 68.

[31] *Id.*

[32] *Id.* at 69.

[33] *Id.* at 69–70.

[34] *Id.* 70–71.

[35] *Id.* at 71.

[36] *Id.* at 65.

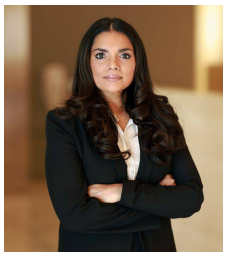
[37] Katy O'Donell, *CFPB to propose rule restricting data brokers this year,* POLITICO Pro (Feb. 28, 2024), https://subscriber.politicopro.com/article/2024/02/cfpb-to-propose-rule-restricting-data-brokers-this-year-00143999?source=email.

[38] EO 14117, Sec. 3(a).

[39] *Id.*, Secs. 3(b), 6.

[40] *Id.*, Sec. 4.

Related Attorneys



Shoba Pillay
Partner
spillay@jenner.com
+1 312 923 2605

Madeleine Findley
Partner
mfindley@jenner.com
+1 202 639 6095

Related Capabilities

Data Privacy and Cybersecurity

National Security and Crisis

Stay Informed →