THE GEORGE WASHINGTON UNIVERSITY

WASHINGTON, DC

Public Interest Comment[1] on

The Department of Justice's Advance Notice of Proposed Rulemaking

National Security Division; Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern

Docket ID No. DOJ-NSD-2024-0002

RIN: 1105-AB72

APRIL 19, 2024

Mark Febrizio[2]

REGULATORY STUDIES CENTER

The George Washington University Regulatory Studies Center improves regulatory policy through research, education, and outreach. As part of its mission, the Center conducts careful and independent analyses to assess rulemaking proposals from the perspective of the public interest. This comment on the Department of Justice's (DOJ) advance notice of proposed rulemaking does not represent the views of any particular affected party or special interest but is designed to evaluate the effect of DOJ's proposal on overall consumer welfare.

Background and Summary of Proposal

On February 28, 2024, President Biden signed Executive Order (EO) 14117 – titled "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern." The EO was published in the Federal Register on March 1, 2024. In

[1] This comment reflects the views of the author and does not represent an official position of the GW Regulatory Studies Center or the George Washington University. The Center's policy on research integrity is available at https://regulatorystudies.columbian.gwu.edu/about#integrity. This comment has been reformatted and lightly edited for clarity. The original version submitted to the agency is publicly available on Regulations.gov: https://www.regulations.gov/comment/DOJ-NSD-2024-0002-0062.

[2] Mark Febrizio is a senior policy analyst at the George Washington University Regulatory Studies Center.

Section 2, the order required DOJ to issue implementing regulations that prohibit or restrict U.S. persons from engaging in transactions that may facilitate countries of concern accessing bulk sensitive personal data or U.S. government related data.[3]

On March 5, DOJ issued an advance notice of proposed rulemaking (ANPRM) that delineated its initial formulation of what the implementing regulations may look like and requested public input on various topics, including 114 specific questions.[4] It also established preliminary definitions of multiple terms that guide the EO's implementation.

DOJ's ANPRM lays out a two-part framework of categorical rules that would identify two types of covered data transactions: "prohibited transactions" (classes of highly sensitive and prohibited transactions) and "restricted transactions" (classes of transactions that must comply with predefined security requirements).[5] DOJ is also considering establishing general and specific licenses for these two types of covered data transactions.[6] This categorical approach is distinct from the case-by-case review that is administered by the Committee on Foreign Investment in the United States (CFIUS),[7] although both processes may apply to the same transactions.

As established by EO 14117, the DOJ regulations are concerned with transactions between "U.S. persons"[8] and "covered persons"[9] that involve two categories of data: (a) bulk U.S sensitive personal data or (b) U.S. government related data. Covered persons is defined in the ANPRM as an individual or entity that meets any one of five criteria, with the common theme being the control or influence of a country of concern.[10] DOJ incorporates the Department of Commerce's

---

[3] 89 FR 15423, https://www.federalregister.gov/d/2024-04573/p-10.

[4] 89 FR 15780, https://www.federalregister.gov/d/2024-04594.

[5] 89 FR 15782, https://www.federalregister.gov/d/2024-04594/p-31.

[6] 89 FR 15783-4, https://www.federalregister.gov/d/2024-04594/p-42.

[7] 89 FR 15783, https://www.federalregister.gov/d/2024-04594/p-40.

[8] 89 FR 15788, https://www.federalregister.gov/d/2024-04594/p-137.

[9] 89 FR 15790, https://www.federalregister.gov/d/2024-04594/p-182.

[10] 89 FR 15790, https://www.federalregister.gov/d/2024-04594/p-183.

implementation of Executive Order 13873 of May 15, 2019[11] that identified China, Russia, Iran, North Korea, Cuba, and Venezuela as countries of concern.[12]

Covered data transactions may involve six categories of sensitive personal data:

- Covered personal identifiers, which involve eight classes of listed identifiers. Most classes of listed identifiers must be linked to another class, with several exceptions, to be considered covered personal identifiers. The classes of listed identifiers are as follows:[13]
    - Full or truncated government identification or account numbers
    - Full financial account numbers or personal identification numbers associated with a financial institutions or services
    - Device-based or hardware-based identifiers
    - Demographic or contact data
    - Advertising identifiers
    - Account-authentication data
    - Network-based identifiers
    - Call-detail data
- Geolocation and related sensor data
- Biometric identifiers.
- Human 'omic data.
- Personal health data.
- Personal financial data.

The ANPRM identifies bulk U.S. sensitive personal data as data that involve one or more categories of sensitive personal data when it exceeds a bulk threshold of a certain number of U.S. persons within a particular window of time. The ANPRM identifies government-related data as data that either contain precise geolocation data on a place that will appear on a forthcoming list of sensitive facilities or locations or involve sensitive personal data "linked or linkable to current or recent former employees or contractors, or former senior officials, of the U.S. government, including the military and Intelligence Community."[14]

This public comment on the DOJ's ANPRM does not represent the views of any particular affected party or special interest but is designed to evaluate the effect of DOJ's proposal on overall

---

[11] 84 FR 22689, https://www.federalregister.gov/d/2019-10538; EO 13873 declared the national emergency that EO 14117 expands upon.

[12] 89 FR 15790, https://www.federalregister.gov/d/2024-04594/p-178.

[13] 89 FR 15784, https://www.federalregister.gov/d/2024-04594/p-50.

[14] 89 FR 15787, https://www.federalregister.gov/d/2024-04594/p-120.

consumer welfare. The following sections discuss the proposal's regulatory analysis and several of the specific questions asked in the ANPRM.

II. Regulatory Analysis

II.A. Problem Identification

DOJ is responding to directives from an executive order as a starting point for its rules, rather than beginning from an empirical assessment of the problem. Nevertheless, the ANPRM establishes that a degree of risk exists and provides several anecdotes indicating that transactions involving sensitive data on U.S. persons could create significant national security risks when falling into the wrong hands.[15]

A core component of regulatory analysis is identifying the problem that needs to be addressed and assessing the significance of that problem.[16] This step is valuable even for rules that would otherwise be required, because it helps clarify the potential effects of a regulatory action and facilitates the consideration of alternative regulatory approaches. Even in the instance of this rulemaking, where DOJ is required to take a regulatory approach of proposing prohibited and restricted transactions, such a step can help DOJ evaluate the tradeoffs between different bulk thresholds by providing a baseline assumption of the expected impacts.

Recommendation 1: In its subsequent proposed rule, DOJ should identify the scope and significance of the problem relating to countries of concern accessing sensitive U.S. data.

II.B. Retrospective Review

Executive Order 12866 also directs agencies to review their significant regulations in order to determine whether they are meeting their objectives and how those regulations could be modified to better meet those objectives.[17] In its section of economic impact, DOJ discusses how it expects the primary economic effects of the rule to fall under a set of direct or indirect costs, but that it lacks sufficient data to thoroughly evaluate and accurately measure these costs.

Given the uncertainty DOJ is dealing with in these regulations, it should proactively prepare for retrospective review of these rules, to ensure that it can adjust and refine the regulations at a later date to be more effective. Currently difficult to estimate effects will be easier to evaluate once DOJ

---

[15] 89 FR 15781, https://www.federalregister.gov/d/2024-04594/p-20.

[16] Executive Order 12866, Sec. 1(b)(1), https://www.archives.gov/files/federal-register/executive-orders/pdf/12866.pdf.

[17] Executive Order 12866, Sec. 5(a).

has incoming information on the number and types of covered data transactions that occur each year (as well as which countries of concern seem to pose the greatest threat in this area).

Recommendation 2: In its subsequent proposed rule, DOJ should plan for retrospective review, including by collecting data on covered data transactions across relevant dimensions (e.g., time, country of concern, type of transaction, etc.).

II.C. Compliance with Regulatory Analysis Requirements

DOJ's ANPRM was designated a significant regulatory action and was reviewed by the Office of Information and Regulatory Affairs (OIRA).[18] Given the potential size of just the data brokerage industry[19] – which is only one component of the proposed regulations – DOJ's rule is likely to reach the $200 million annual threshold that is used to classify rules as significant under Section 3(f)(1) of Executive Order 12866.[20]

Recommendation 3: DOJ should identify its rulemaking as a Section 3(f)(1) Significant regulation, prepare a regulatory impact analysis, and have OIRA review its subsequent proposal.

III. Addressing Specific Questions from the ANPRM

Question 3

> *3. Should the Department of Justice consider amending the definitions applicable to any of the six categories of sensitive personal data? If the definition should be elaborated or amended, why?*

First, DOJ should clarify several matters related to its discussion of listed identifiers for covered personal identifiers. Specifically, it defines "covered personal identifiers" as "any listed identifier that is linked to any other listed identifier" with two exceptions:[21]

> (a) The term covered personal identifiers does not include demographic or contact data that is linked only to other demographic or contact data; and
> (b) The term covered personal identifiers does not include a network-based identifier, account-authentication data, or call-detail data that is linked only to other network-based

---

[18] 89 FR 15802, https://www.federalregister.gov/d/2024-04594/p-397.

[19] 89 FR 15799-800, https://www.federalregister.gov/d/2024-04594/p-353.

[20] Executive Order 12866 Section 3(f)(1), as amended by Executive Order 14094, https://www.federalregister.gov/d/2023-07760.

[21] 89 FR 15784, https://www.federalregister.gov/d/2024-04594/p-47.

identifier, account-authentication data, or call-detail data as necessary for the provision of telecommunications, networking, or similar services.

Based on the definitions and examples contained in the ANPRM, it seems clear that transactions involving any or all of the types of demographic or contact information listed (i.e., name, birth date, birthplace, address, phone number, email) would not be prohibited or restricted under the rules, unless those information were linked to government identification numbers, financial account numbers, device-based identifiers, advertising identifiers, account-authentication data, network-based identifiers, or call-detail data.[22]

However, the second exception is less clear. Does the exception for network-based identifier, account-authentication data, or call-detail data mean that these data would not be covered if they are linked to information of *the same class* (e.g., a network-based identifier linked to a network-based identifier) or that these data would not be covered if they are linked to information in *any of these three classes* (e.g., a network-based identifier linked to account-authentication data) when providing telecommunications, networking, or similar services?

Second, DOJ should elaborate on how to determine which data are exploitable by a country of concern. Rather than having entities independently determine whether sensitive U.S. data are exploitable by a country of concern, DOJ "intends to identify specific classes of data that, when combined, would satisfy this standard."[23] More clarity on the application of this standard is needed, especially when relating to Examples 6, 7, 8, and 9.

Examples 6 and 7 illustrate situations where a single class of listed identifiers are distributed in a transaction without being linked to another class (e.g., MAC addresses, full names), yet the transaction would be covered because they come with a disclosure that "makes the list of [MAC addresses or names] exploitable by a country of concern."[24]

Examples 8 and 9 give similar situations but conclude that the transacted data would not be covered by DOJ's rules.

According to DOJ, these disclosures make the data exploitable:

- "devices that have connected to the wireless network of a U.S. fast-food restaurant located in a particular government building"
- "members of a country of concern's opposition political party in New York City"

---

[22] 89 FR 15785, https://www.federalregister.gov/d/2024-04594/p-70.

[23] 89 FR 15785, https://www.federalregister.gov/d/2024-04594/p-74.

[24] 89 FR 15785, https://www.federalregister.gov/d/2024-04594/p-75.

- "active-duty LGBTQ+ military officers"

These disclosures do not make the data exploitable:

- "any American who visited a Starbucks in Washington, DC in December 2023"
- "'Americans who watched more than 50% of episodes' of a popular TV show"

DOJ should provide more clarity on how parties should distinguish between such edge cases. For the above examples, would simply disclosing "active-duty military officers" make the data exploitable? Alternatively, what about just "LGBTQ+ individuals"? How about "active-duty military officers that visited any Starbucks in Washington DC during December 2023"? These are not clearly delineated by DOJ's provided examples.

Example 10 suggests that identifying sensitive personal data as linked to military personnel makes it government-related data.[25] Is this central to the distinction being made?

In short, DOJ should provide additional clarity to how to interpret the standard for what it means for data to be exploitable by a country of concern.

Question 8

> *8. Are there other factors or characteristics that the Department of Justice should evaluate as part of the proposed analytical framework for determining the bulk thresholds?*

Because thresholds are necessarily difficult to establish in a non-arbitrary manner, DOJ should engage in sensitivity analysis of the bulk thresholds. Even if DOJ is unable to engage in empirical analysis of different thresholds, it can qualitatively assess the risk present under different thresholds and get a sense of the direction of the risk and other important effects.

Question 13

> *13. Should the classes of listed identifiers, such as for government identification numbers and financial account numbers, include truncated versions of the full numbers? If so, how should "truncated" be defined?*

Yes, truncated versions of full numbers are worth including in the classes of listed identifiers if they can be used in an actionable manner. For example, the last four digits of a social security number (SSN) are valuable, even if less valuable than a full SSN, because they are regularly used to validate a person's identity (e.g., communications with a banking institution).

---

[25] 89 FR 15787, https://www.federalregister.gov/d/2024-04594/p-123.

Question 27

> *27. Are there other factors or considerations relating to the abilities of the proposed countries of concern to access and exploit bulk sensitive personal data or government-related data to engage in nefarious activities that the Department of Justice should take into account when determining whether to identify the same countries as countries of concern?*

In addition to establishing this base list of countries of concern, DOJ should identify a process for adding or removing countries from the list, along with criteria that might trigger such an addition or removal. Further, it is worth considering whether there is a situation in which DOJ would depart from the conclusions of the Department of Commerce on the list of countries of concern.

Question 28

> *28. How would the U.S. party to a data transaction ascertain whether a counterparty to the transaction is a covered person as defined above? What kind of diligence would be necessary?*

First, DOJ should offer guidance on how to evaluate an individual or entity's status as a covered person.

Second, DOJ should consider how readily available it is for U.S. persons to access ownership information on an entity. What information is needed for a U.S. person to determine whether an entity is "50 percent or more owned, directly or indirectly, by a country of concern" or owned by an entity that meets these criteria? Is this information publicly available?

Question 32

> *32. How should the list [of covered persons] be published? How should it be organized? In what format should the Department of Justice publish it?*

DOJ should publish the list in a machine-readable format and organize it in a sensible way (e.g., by country, name, other identification information including aliases). The list should be publicly available from a stable website, so that U.S. persons have clarity and consistency on where to find the list. Ideally, this website should not change when an administration changes. Thus, publishing a notice in the Federal Register would be a natural place to disseminate the list.

Question 33

> *33. How would industry monitor this list? Would it be more costly for industry if the list were updated continually or only at certain points in time? If updates were made on an individual basis or in batches? Please be specific.*

Updating the list at certain points in time (e.g., quarterly) that are clearly delineated and consistent would be ideal. Some companies with sufficient technical sophistication could set up an automated way to retrieve this information and be notified of a change, but not all companies would or could follow this approach. DOJ should also consider ways to identify and proactively reach out to industry organizations that have had past dealings with an individual that is to be added to the list.

Question 59

> *59. Should some or all advisory opinions [on whether actual transactions are considered covered data transactions] be published? How might the possibility of publication affect a request (noting that any publication would comply with applicable laws regarding confidential business information and similar topics)?*

Yes, it seems worthwhile for DOJ to publish advisory opinions both for other industry organizations that seek to comply with the regulations and for the general public's understanding of the administration of these regulations. Further, making such information publicly available allows academics and other researchers to study the process and evaluate how it is functioning.

Question 60

> *60. If the Department of Justice decides to publish some or all advisory opinions, how should it do so?*

DOJ could publish the opinions on a dedicated agency website (whether managed by DOJ or a third agency such as GSA); however, these often change when administrations change. Instead, DOJ should opt to publish its opinions to the Federal Register, since such notices are durable and contained in a single location.

Question 61

> *61. How should the Department of Justice address circumstances in which an advisory opinion no longer applies (e.g., the relevant country of concern at the time the opinion was issued no longer meets the requirements for being a country of concern).*

In this situation, if notices are published to the Federal Register, issuing a new notice and linking it to the prior notice through metadata would be beneficial.

If the notice is also provided on an agency website, DOJ should, to the extent feasible, amend the outdated notice with markings or a note on the change and ensure that the notices and changes are clearly dated.

Question 107

> *107. How could the Department of Justice mitigate the costs of compliance, particularly for small- and medium-sized enterprises? Are there measures that could be taken to reduce the economic impact of the regulatory regime without altering the fundamental scope or thresholds associated with the regulation?*

DOJ should consult with the Small Business Administration on this matter.

Question 110

> *110. What additional costs and benefits should the Department of Justice consider, and how should they be estimated? Is there additional data on the economic costs and benefits that the Department of Justice should examine?*

DOJ should consider estimating the costs and benefits related to forgone transactions that are not covered data transactions but might be perceived as covered data transactions.