BR Business Roundtable

1000 Maine Avenue, SW, STE 500
Washington, DC 20024
202.872.1260
brt.org

November 26, 2024

U.S. Department of Justice
National Security Division, Foreign Investment Review Section
175 N Street NE, 12th Floor
Washington, DC 20002

RE: Comments on 89 Fed. Reg. 85976 (Oct. 29, 2024); RIN 1124-AA01; Docket No. NSD-104

Business Roundtable (BRT) appreciates the opportunity to submit comments on the Department of Justice's (DOJ) Notice of Proposed Rulemaking (NPRM) on Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons.[1]

BRT is an association of more than 200 chief executive officers (CEOs) of America's leading companies, representing every sector of the U.S. economy. BRT CEOs lead U.S.-based companies that support one in four American jobs and almost one-quarter of U.S. GDP.

As BRT member companies invest significantly in data privacy and security measures to protect sensitive information, we recognize the global risks to that information. BRT member companies operate in industries that rely on secure, cross-border data transfers and are committed to adhering to rigorous data protection standards. BRT supports policy efforts that aim to safeguard national security and consumer privacy while maintaining a regulatory framework that allows American businesses to operate effectively in a competitive global market.

However, BRT believes that the scope and obligations imposed on businesses through this rule should be calibrated to avoid overregulation of routine and legitimate business activities. BRT recommends that the DOJ focus its regulatory framework on the types of transactions, types of data and foreign relationships that pose material security risks to the United States, distinguishing them from routine transactions that present insignificant risk. The following comments outline key considerations regarding the NPRM, focusing on potential areas of impact for American businesses and recommendations for a balanced final rule.

I. Treatment of Sensitive Data

A. Anonymized, Pseudonymized, De-Identified and Encrypted Data

BRT reiterates its prior recommendation, consistent with comments submitted in response to DOJ's Advance Notice of Proposed Rulemaking (ANPRM), that the DOJ's final rule distinguish between

[1] 89 Fed. Reg. 86116 (2024).

cleartext data and data that has been sufficiently protected through anonymization, pseudonymization, de-identification or encryption.[2] Such distinctions would allow businesses to leverage secure data-handling practices without incurring unnecessary regulatory burdens, provided that these practices effectively minimize re-identification risks. Businesses frequently rely on advanced data protection techniques to enable secure data flows while safeguarding personal privacy. Moreover, numerous regulatory frameworks—including but not limited to state data protection laws and the Health Insurance Portability and Accountability Act—recognize the lower risks associated with data that are protected by such measures.

To align with global best practices for data protection, BRT recommends that the DOJ final rule exclude effectively encrypted data from the definitions of sensitive personal data and government-related data, provided that encryption keys and related data sets are stored securely. This should include, for example, data protected through industry-standard encryption methods such as the Advanced Encryption Standard (AES-256).

At minimum, BRT recommends the DOJ exclude data that is encrypted according to recognized post-quantum encryption standards. The DOJ's proposed rule states that a rationale for not differentiating between encrypted data and cleartext is that countries of concern may amass large quantities of encrypted data with the expectation that they will leverage advances in quantum technologies to decrypt that data in the future.[3] This issue can be mitigated by encrypting data using encryption algorithms designed to withstand attacks from quantum computers, such as those in alignment with the Federal Information Processing Standard 203 issued by the National Institute of Standards and Technology (NIST), provided that encryption keys and related data sets are stored securely.[4] Excluding quantum-encrypted data from the proposed rule would protect data against access by countries of concern, avoid barriers to commercial data flows and strengthen the digital ecosystem by encouraging U.S. persons to adopt stronger quantum cryptography.

BRT also recommends that DOJ's definitions of sensitive personal data and government-related data exclude anonymized, pseudonymized and de-identified information protected in compliance with internationally recognized industry standards that prevent re-identification. De-identified data is central to research, analytics and other legitimate data-driven business models across sectors, enabling innovation and operational efficiencies while preserving privacy. Rather than treating de-identified data the same as data that is linkable to an individual, we believe a more appropriate approach would be to require the necessary level of de-identification that addresses the re-identification risk that the rule seeks to control. We also note that the DOJ's proposed rule appears inconsistent with the Cybersecurity and Infrastructure Security Agency's data security requirements, which explicitly require

[2] Comments of the Business Roundtable to the Department of Justice on the Advance Notice of Proposed Rulemaking on Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern, pg.1, Apr. 19, 2024, https://s3.amazonaws.com/brt.org/Business-RoundtableResponsetoDOJANPRMonDataSecurity_FINAL_4.19.24.pdf. (Hereinafter "BRT ANPRM comments.")
[3] 89 Fed. Reg. 86127.
[4] NIST, Federal Information Processing Standard 203, Module-Lattice-Based Key Encapsulation Mechanism Standard, Aug. 13, 2024, https://csrc.nist.gov/pubs/fips/203/final.

the same data masking techniques that the DOJ's rule considers inadequate.[5] It would be more effective to recognize that strong security measures, combined with organizational and contractual restrictions, can provide sufficient protection such that a complete block on data transfer is unnecessary.

Data protection processes such as encryption and de-identification are widely used across industries and governments to prevent unauthorized access, significantly reducing the risks associated with loss or unauthorized acquisition of data. By distinguishing protected data from cleartext data, the DOJ can foster practices that align with established global privacy frameworks and support businesses in securely storing and transferring data.

B. Bulk Thresholds and Geolocation Precision

Bulk thresholds for covered data as well as a carefully considered definition of geolocation data will be critical for helping ensure compliance with DOJ's proposed rule. Collection and storage of covered data at higher volumes is increasingly common for a variety of business, technical and administrative purposes. A wide variety of common applications such as ride-sharing services, delivery tracking and location-based advertising depend on geolocation information for functionality.

The DOJ's proposed rule sets specific bulk thresholds for different categories of sensitive personal data, such as personal identifiers, and financial and health data. Though BRT appreciates efforts to create a tailored approach by establishing bulk thresholds, we believe the bulk thresholds should be adjusted to align more closely with real-world business practices and minimize operational impacts. This recommendation is all the more important in light of the NPRM's inclusion of encrypted data and the compliance obligations on U.S. persons that transact with third parties – including cloud vendors – to maintain and process covered data.

BRT continues to recommend that the DOJ adopt the higher bulk thresholds identified in the ANPRM.[6] The covered data are commonly processed for legitimate business purposes that provide valuable services to Americans and strengthen economic competitiveness, such as Wi-Fi at hospitality establishments, retail loyalty and rewards programs, and healthcare research and product development. In many cases, this data is de-identified, pseudonymized or otherwise protected against re-identification. At minimum, we recommend that the DOJ's NPRM distinguish bulk thresholds for cleartext data and data protected with such processes.

BRT further recommends that the DOJ establish a process to review and, if appropriate, adjust bulk thresholds over time to reflect changes in data protection technology, commercial data utilization and industry standards. Periodic threshold reviews can ensure that regulations keep pace with evolving data privacy and security practices, as well as emerging risks without overburdening businesses.

---

[5] Cybersecurity and Infrastructure Security Agency, Proposed Security Requirements for Restricted Transactions, Oct. 2024, pg. 4, https://www.cisa.gov/sites/default/files/2024-10/Proposed-Security-Requirements-EO-14117-21Oct24508.pdf.
[6] 89 Fed. Reg. 15786 (2024).

BRT also continues to recommend that the DOJ's level of precision in defining geolocation should establish a radius equivalent to or greater than existing state laws. A uniform definition that restricts data showing location at a radius under 1,850 feet, as under California law, [7] would provide more consistency in compliance obligations and continue enabling the provision of valuable location-based services, while protecting individual geolocation privacy. The DOJ's proposed rule sets a much wider radius of under 1,000 meters (approximately 3,281 feet), which is not precise and considerably broader than other regulations.[8] While location information related to government personnel and facilities may carry a higher degree of sensitivity, BRT does not believe the broader radius of geographic information should apply to the general definition of personal identifiers for other data transactions.

II. Scope of Prohibited and Restricted Transactions

A. Covered Persons and Government Locations Lists

The DOJ's list of covered persons and government locations would provide more authoritative guidance on persons and locations considered security risks, which will help U.S. businesses avoid unintended noncompliance. BRT continues to urge the DOJ to issue list updates in a regularly scheduled cadence to further enable companies to coordinate compliance.

As noted in BRT's comments to the ANPRM,[9] BRT supports the DOJ's proposal to establish and periodically update a list of covered persons.[10] BRT recommends that this list be as comprehensive as feasible and include aliases and technical identifiers of covered persons to aid business compliance efforts and automated due diligence. The fluid nature of global affiliations and the use of shell companies to obfuscate ownership pose challenges to businesses avoiding transactions with covered persons.

Similarly, BRT supports DOJ's establishment and maintenance of a geo-fenced Government-Related Location Data List.[11] As with the covered persons list, BRT urges the DOJ to structure this list in formats that support automated scanning to streamline compliance while dealing with large data sets.

B. Prohibited and Restricted Transactions

BRT appreciates that the DOJ clarified when a transaction "involves" government-related data or bulk U.S. sensitive personal data, as BRT had requested in comments to the ANPRM.[12] BRT also reiterates its recommendation that the DOJ revise the scope of "data brokerage" to reduce uncertainty and more

---

[7] Cal. Civ. Code section 1798.140(w).

[8] 89 Fed. Reg. 86126 (2024).

[9] BRT ANPRM comments, pg. 9.

[10] 89 Fed. Reg. 86150-86151.

[11] 89 Fed. Reg. 86129.

[12] 89 Fed. Reg. 86122. DOJ's clarification that the transaction "involves any access to the data by the counterparty to a transaction," rather than any transaction that involves government-related data or bulk U.S. sensitive personal data. *See also*, BRT ANPRM comments, pg. 6.

appropriately target transactions that give rise to a national security risk. BRT continues to urge the DOJ to strike the open-ended phrase "similar commercial transactions" from the definition of "data brokerage" to clarify that "data brokerage" is limited to the sale or licensing of data rather than all data sharing transactions. This change would help ensure that the rule avoids covering an unnecessarily broad class of transactions that do not pose a national security risk. In BRT's view, this should exclude from the scope of the definition:

- Marketplace sales, in which a third-party seller that is located in a country of concern or that is a covered person provides items for sale to U.S. persons on platforms owned by U.S. companies;
- Retail advertising networks that are owned by U.S. companies and that feature advertisers who are covered persons or that are based in a country of concern;
- Personal health data and human genomic data for scientific research and regulatory purposes; and
- Provisions of services to U.S. individuals abroad.[13]

BRT urges the DOJ to clarify the extent to which the proposed definition of "data brokerage" includes transferring demographic information, such as name and email address, to a covered recipient that did not collect the information.[14] Companies often share demographic data, such as name and email address, with third parties for co-promotion purposes. Since demographic data is excluded from the definition of "covered personal identifier," we encourage DOJ to clarify whether this exempts these transaction types from the definition of "data brokerage."[15]

BRT further urges the DOJ to clarify whether personal financial history's inclusion of purchases and payment history relates only to financial institutions or to any purchase and payment history.[16]

BRT also urges the DOJ to amend several definitions related to health data to better scope the rule. We encourage the DOJ to narrow the definition of "personal health data" to information that "identifies," rather than information that "relates to" a physical or mental health condition. Information that is related to, but does not identify, an individual's health condition has a low potential to cause harm but is essential to commerce and the access to goods and services. For example, selling health products on an online marketplace requires the sharing of information that may be related to, but does not identify, a consumer's health condition; as drafted, the proposed rule could, in practice, prevent U.S. consumers from accessing affordable products from global markets. We also encourage the DOJ to limit the definition of "human biospecimens" to raw human samples and clarify that the definition does not include biospecimens that are included in or partially processed for use in finished medical products.

In its proposed rule, the DOJ considers expanding the definition of human genomic data to include all 'omic data. BRT recommends narrowing the definition of genomic data and increasing the threshold to

[13] BRT ANPRM comments, pg. 7.
[14] 89 Fed. Reg. 86207.
[15] 89 Fed. Reg. 86206.
[16] 89 Fed. Reg. 86125.

better reflect the varying degrees of sensitivity and identifiability of 'omic data. The DOJ should not expand the definition of human genomic data to include other data types, such as transcriptomics, proteomics and metabolomics. These categories of 'omic data are critical for conducting clinical trial research and should not be included in the scope of this rule. Furthermore, the proposed rule provides a low threshold for genomic data and prohibits transactions above the threshold. BRT recommends increasing the threshold to better reflect the sensitivity of 'omic data.

BRT urges the DOJ to amend the definition of "covered personal identifiers" to exclude the combination of low-risk identifiers. When advertising or device identifiers are combined with low-risk identifiers like IP addresses or contact data but not combined with any other information, it is unclear that any additional risk of identifying sensitive data is created.

It is critical for the DOJ to clarify that the rule's restrictions on vendor contractual agreements apply to agreements after the effective date of the final rule. It would be burdensome and costly for industry to re-negotiate contracts that were executed prior to the final rule taking effect.

Regarding investment agreements, BRT continues to urge the DOJ to adopt a de minimis threshold of indirect ownership interests that would be covered in otherwise passive investments. BRT urges the DOJ to consider an ownership stake of less than 25 percent as de minimis, rather than the NPRM's proposed 10 percent.[17] This threshold aligns more closely with the annual reporting requirement in the proposed rule, as well as the Financial Crimes Enforcement Network rules for reporting beneficial owners under the 2024 Corporate Transparency Act.[18] An investor with an ownership interest under 25 percent is unlikely to possess a degree of control over the investment to give rise to a national security risk.

C. Exempted Transactions

BRT strongly supports the proposed exemption for "corporate group transactions" (formerly "intra-entity transactions" in the ANPRM).[19] BRT urges the DOJ to clarify its definitions of "subsidiary," "affiliate" and "branch."[20] BRT also appreciates that the proposed exemption includes examples of activities that fall within the exemption, such as employees' internal and external communications.[21] BRT urges the DOJ to add to this list of examples additional routine, low-risk transactions that should fall under this exemption, including:

- Fulfillment of goods or services requested by the customer, such as travel reservations, that must be filled in country;
- Transactions with a local subsidiary for the purpose of carrying out an activity that would be exempt if done by the U.S. parent company;
- Internal collaboration and review platforms;

[17] 89 Fed. Reg. 86133-86134.
[18] 89 Fed. Reg. 86225. *See also* 31 CFR § 1010.380.
[19] 89 Fed. Reg. 86135-86136.
[20] 89 Fed. Reg. 86218.
[21] 89 Fed. Reg. 86218.

- Pricing and billing systems;
- Customer and vendor relationship management tools, including technical assistance centers; and
- Expense monitoring and reporting.[22]

In addition, we urge the DOJ to clarify that the "corporate group transactions" exemption includes data sharing required for global operations of services related to U.S. persons and is not limited to data sharing that is ordinarily incidental to and part of certain administrative or ancillary business functions. As drafted, this exemption has a very narrow scope and would not include many of the transactions necessary to seamlessly perform global business operations.

BRT urges the DOJ to remove or at minimum lessen burdensome requirements under the corporate group transactions exemption to establish additional access protocols to ensure employees in countries of concern only have access to pseudonymized, anonymized or de-identified data. Many companies, especially those in highly regulated sectors, have robust security and data governance measures in place, have mechanisms for intra-affiliate data transfers in place, and may have contractual or other legal obligations to comply with when storing or safeguarding data.

BRT appreciates the DOJ's added exclusion of transactions incidental to the provision of telecommunications services.[23] However, while the inclusion of an exemption for telecommunications services is a step in the right direction, it may be too narrow to adequately address the scope of modern communications, which involves networking, IT infrastructure and related services. Telecommunications is just one component of a much larger ecosystem of interconnected services, and regulators should clarify that telecommunications exemptions extend across the ecosystem. For example, the DOJ should clarify that related services, such as broadband and text messaging, are also exempted. BRT recommends expanding the exemption to "transactions that are ordinarily incident to and part of telecommunications, networking, and related communications services."

BRT urges the DOJ to clarify the scope of the exemption for transactions ordinarily incidental to travel in proposed section 202.503.[24] While the exemption includes transactions for payment of living expenses and arrangement or facilitation of travel, BRT recommends that the DOJ clarify that the exemption applies to the fulfilment of travel plans, including reservation data and other information used to facilitate hotel stays.

BRT additionally appreciates the DOJ's clarification that the scope of the exemption for financial services encompasses services ancillary to processing payments and funds transfers.[25] We agree that the scope of examples 4 and 12 should not be considered exempt for the purposes of the financial services exemption but should otherwise be in scope of the corporate group transactions exemptions.

[22] BRT ANPRM comments, pg. 11.
[23] 89 Fed. Reg. 86137.
[24] 89 Fed. Reg. 86216.
[25] 89 Fed. Reg. 86134-86135.

We otherwise urge inclusion of this clarification, which BRT had requested in comments to the ANPRM, in the final rule.[26]

BRT also appreciates the DOJ's proposed exemptions for "drug, biological product, and medical device authorizations" and "other clinical investigations and post-marketing surveillance data."[27] BRT urges the DOJ to ensure that the final language implementing these exemptions practically and effectively enables these important objectives. This includes enabling the entire biomedical innovation journey, including that not directly relating to the conduct of clinical trials. DOJ should not adopt a bright-line rule or categorically define what data might be reasonably necessary under this exemption. It is particularly important that the DOJ's definition of de-identified data is consistent with U.S. Food and Drug Administration standards for postmarketing de-identification and includes key-coded data, such that the rule allows the exemption of clinical trial and other related data. The exemption should include vendor transactions with local agents that may be required for regulatory approval in certain jurisdictions.

Finally, BRT believes that the DOJ's proposed interpretation of "information or informational materials" under the Berman Amendment likely exceeds the President's authority under the International Emergency Economic Powers Act.[28] The phrase "information or informational materials" cannot reasonably be limited to expressive materials. The plain text of the statute contains no such limitation and includes purely technical storage media alongside traditionally "creative" works.[29] Indeed, legislative history supports a broad reading of this exemption to data not typically characterized as expressive.[30] Scientific and technical data exchange has long been included within the ambit of the Berman Amendment, subject only to restrictions on export of information subject to the Export Administration Regulations.[31] BRT recommends that the DOJ ensure its interpretations of "information or informational materials" closely align with the use of this exemption in the Office of Foreign Assets Control (OFAC) sanctions. This will avoid confusion and enable organizations to rely on OFAC's existing guidance regarding the scope of the term. Further, it would be consistent with the proposed rule's modeling of due diligence obligations after OFAC sanctions compliance.

III. Compliance and Reporting Requirements

A. Due Diligence, Reporting and Auditing Requirements

BRT understands that effective due diligence, recordkeeping and reporting requirements are common components of a compliance regime. However, the DOJ's proposed requirements, while well-

[26] BRT ANPRM comments, pg. 7.
[27] 89 Fed. Reg. 86220.
[28] 89 Fed. Reg. 86165.
[29] 50 U.S.C. § 1702(b)(3) (e.g., "microfilms, microfiche, tapes, compact disks, CD ROMS").
[30] H.R. Conf. Rep. No. 103-482 at 239 (intending the exemption to "facilitate transactions and activities incident to the flow of information and informational materials without regard to the type of information, its format, or its means of transmission")
[31] OFAC Letter to IEEA, No. IA-209747-a; see also https://legal.ieee.org/images/files/Compliance/IEEE_Specific_Activities.pdf (permitting dissemination of scientific and technical information to embargoed countries).

intentioned, impose a substantial administrative burden, especially for businesses that already implement high standards in security and data governance. BRT appreciates the DOJ's recognition that the due diligence requirements should be based on a variety of factors, including the U.S. person's size and sophistication, products and services, customers and counterparties, and geographic locations.[32] BRT reiterates its recommendation that the DOJ view due diligence requirements in proportion to the degree of risk associated with a covered data transaction and that due diligence for lower-risk transactions should be achieved through more streamlined measures such as contractual safeguards and automated review of the counterparty's technical indicators (such as IP address location).[33] BRT also urges the DOJ to provide general interpretive guidance contrasting due diligence under the NPRM with due diligence requirements under sanctions and export regulations.

BRT strongly opposes the DOJ's proposed requirement that U.S. persons must file a report within 14 business days for any offer to engage in a prohibited data brokerage transaction, particularly when the offer is automatically rejected using software, technology or automated tools.[34] Modern businesses are inundated with communications of dubious origin, including spam and fraudulent proposals through email, post, text and other channels, that are not seriously considered and do not pose a risk to national security when rejected. When businesses use automated tools to affirmatively reject such offers, the business' personnel may not be actively aware of the offer and rejection. DOJ's proposed reporting requirements should not impose a detailed reporting requirement on U.S. businesses for such routinely ignored offers. BRT recommends the DOJ significantly narrow this proposed requirement to encourage voluntary reporting of credible offers to engage in high-risk, prohibited transactions.

BRT urges the DOJ to consider clarifying that reporting requirements for suspected or known violations of contractual obligations do not apply for inadvertent, good faith or de minimis violations, especially where there is no evidence of acquisition of the data by a covered person or country of concern.[35] BRT recommends that the DOJ ensure the final rule exempts reports due on demand from the Freedom of Information Act.[36] BRT further encourages the DOJ to consider narrowing reporting requirements to submissions upon request, rather than periodically in all cases, and to consider accepting reports created under separate reporting obligations that contain similar information.

With regard to auditing, BRT urges the DOJ to clarify the scope of the audit to cover the U.S. person's data transactions regulated under the proposed rule. As written, the proposed rule would require the audit to examine all data transactions of the U.S. person.[37] This scope is unnecessarily broad, intrusive and challenging to achieve for large organizations and strays beyond the national security concerns driving the proposed rule. BRT further suggests DOJ consider a risk-based approach to auditing that takes into account the sensitivity of the data and the nature of the transaction and counterparties,

[32] 89 Fed. Reg. 86152-86153.
[33] BRT ANPRM comments, pg. 8.
[34] 89 Fed. Reg. 86225.
[35] 89 Fed. Reg. 86214.
[36] 89 Fed. Reg. 86154.
[37] 89 Fed. Reg. 86224.

rather than a uniform annual auditing cadence for all restricted transactions.[38] In addition, DOJ should permit any required audits to be carried out by either external auditors or those internal audit functions that are sufficiently independent, in accordance with the relevant accounting standards.

B. Interaction with Other Regulations

BRT recognizes the DOJ's efforts to distinguish compliance requirements under the Protecting Americans' Data from Foreign Adversaries Act (PADFAA).[39] However, BRT urges the DOJ to consider altering the proposed rule's scope in light of PADFAA restrictions, which are redundant of the proposed rule. While the types of transactions and entities regulated under PADFAA are narrower than the DOJ's proposed rule, the same transactions and entities are regulated under the proposed rule. BRT appreciates the DOJ's expressed intention to coordinate with the Federal Trade Commission on enforcement and guidance but urges DOJ to formalize this commitment by incorporating provisions in the final rule that clarify primary jurisdiction of activities that violate both PADFAA and the proposed rule.[40]

Lastly, BRT recommends that compliance with the DOJ's final rule count toward safe harbor remedies for disclosure. This approach would incentivize proactive participation in compliance mechanisms.

C. Effective Date

To ensure U.S. persons have adequate time to integrate the processes and technical controls necessary to comply with the final rule, BRT encourages the DOJ to establish the effective date to be at least 18 months after the date of publishing the final regulation.[41]

* * *

BRT members have a strong commitment to collaborative solutions balancing national security, privacy and business innovation. We appreciate the DOJ's engagement with the private sector on this important issue for cross-border commercial data flows. [42] If you have any questions regarding these comments, please contact Amy Shuart, Vice President, Technology & Innovation, at AShuart@brt.org.

[38] *Id.*
[39] 89 Fed. Reg. 86155, citing Pub. L. 118-50, div. I 138 Stat. 895, 960 (2024)
[40] *Id.*
[41] 89 Fed. Reg. 86208.
[42] 89 Fed. Reg. 86116.