November 29, 2024

Lee Licata, Deputy Chief for National Security Data Risks
Foreign Investment Review Section
National Security Division
U.S. Department of Justice

"Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons"

Docket No. DOJ-NSD-2024-0004-0001
RIN 1124-AA01
Submitted via regulations.gov

Dear Deputy Chief Licata:

The National Foreign Trade Council (NFTC) appreciates this opportunity to respond to the Notice of Proposed Rulemaking (NPRM) "Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons" [Docket No. NSD 104]. This proposed rule seeks to implement Executive Order 14117 "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern", issued February 28, 2024. E.O. 14117 directs the Attorney General to issue regulations prohibiting and restricting U.S. persons form acquiring, holding, using, transferring, transporting, exporting or dealing in property in which a foreign country or foreign national has an interest where the transaction involved U.S. government-related data or bulk U.S. sensitive personal data. This proposed rule follows an Advance Notice of Proposed Rulemaking (ANPRM) issued by The Department of Justice ("Justice", "DOJ") on March 5, 2024.

NFTC acknowledges the importance and supports the objectives of this rule to address concerns regarding data privacy and bulk data brokerage as well as to deter and prevent the ability of malign foreign actors to access bulk sensitive personal data and U.S. government-related data. We raise below specific definitional concerns and recommendations to more precisely tailor this rule to achieve stated national security objectives without also inadvertently harming broader public policy interests.

Executive Summary

NFTC seeks clarification with respect to intra-company transfers and seeks the exclusion of such on the basis that such transactions are overly inclusive without providing articulable national security benefits. Addressing this concern could involve greater definitional clarity around "data brokerage" and specific language exempting intra-company data transfers. We further believe that certain geo-location information falls outside the scope of this rule and should also be excluded.

We address the potential impact of this proposed rule on the healthcare industry through our discussion of certain relevant exemptions, seek clarification on specific definitional and scoping points, and offer specific recommendations for improving implementation.

We share concerns regarding the proposal to establish a licensing regime to review and approve certain transactions involving bulk data flows. We acknowledge that this has been carried over from the ANPRM and urge ongoing

Lastly, we suggest that the corresponding security requirements published by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) also be revised to align with the recommendations described below.

Concerns and Recommendations

Intra-company transactions

NFTC members believe that this rule should specifically exclude intracompany transactions. In particular, the DOJ should clarify the scope of "Data Brokerage" so as not to prohibit or burden intra-company transactions that pose no greater risk to national security than a restricted transaction. We believe that "Data Brokerage" is defined far more broadly than the common understanding of data broker. This proposed rule defines "data brokerage" as "the sale of data, licensing of access to data, or similar commercial transactions involving the transfer of data from any person (the provider) to any other person (the recipient), where the recipient did not collect or process the data directly from the individuals linked or linkable to the collected or processed data." (§ 202.214.) However, multinational corporations often have multiple legal entities that share personal data. The "recipient" of that data may be a corporate affiliate that accesses, stores, or processes that data on behalf of the U.S. "provider" more efficiently or effectively than the provider can, just as a vendor might.

We believe that DOJ intended to include within scope situations where the recipient receives a "transfer" of data for its own purposes, obtaining its own "right" to the data. (§ 202.254.) And, indeed, Example 6 is of a U.S. company that sells its bulk data to its parent company in a country of concern "to help [the parent company] develop artificial intelligence technology and machine learning capabilities." However, the use of "sale," "licensing," or "similar commercial transactions" is broadly inclusive language that reaches many intra-company transactions.

We seek clarification on whether a multinational corporation's global data sharing agreement would potentially be covered as a "similar commercial transaction." A conservative reading of the rule could prohibit any access by or transfer of covered data to a country of concern (even when the transaction might merely be restricted if it were pursuant to a vendor agreement) and would require U.S. companies to take on board contractual language, recordkeeping, and reporting requirements for intracompany transfers to other foreign persons. Accordingly, we recommend clarification, at least through an additional example, that "data brokerage" does not include intracompany transfers that do not involve a sale or license to access covered data or otherwise give the recipient a "right, remedy, power, privilege, or interest with respect to" the data.

Lastly and relatedly, NFTC is concerned that the exemption for transactions "ordinarily incident to business operations" is ill-defined and subjective. We urge DOJ to adopt a more precise definition including a range of examples and make this information available for further public comment.

Geolocation data

NFTC respectfully requests that DOJ confirms that de-identified precise geolocation data does not constitute sensitive personal data subject to the rule simply because it could be associated with other information about individuals. We note that "sensitive personal data" excludes information "that does not relate to an individual." However, the proposed rule does not address circumstances where de-identified geolocation data could be captured as relating to an individual based solely on the possibility of association with an individual should the information be linked to the data of another data set. Therefore, NFTC respectfully recommends that DOJ more precisely defines "relate to an individual" and provides clarifying example(s) to make clear that information does not "relate to an individual" merely because it can be associated with an individual with access to a separate data set.

Healthcare data

NFTC appreciates the exemptions set forth in this proposed rule to enable and facilitate the discovery and delivery of innovative medicines to U.S. patients and patients globally. We hope that as you continue to assess the impact of proposed U.S. data export restrictions, you address the potential human health impacts of preventing or delaying the discovery and availability of innovative medicines in addition to considering financial impacts. As part of this effort, it is critical that DOJ proactively engages with U.S. health agencies, as well as the healthcare industry, to further refine and implement data restrictions. We also take this opportunity to reiterate the importance of diversity and diverse data sets for success in clinical trials, and in many cases, diversity is required to meet requirements for clinical trials. Delays in meeting these objectives could deny U.S. patients new treatments.

§ 202.510 Drug, biological product, and medical device authorizations

- We seek clarification and confirmation that the definition of "de-identified" data for the purposes of the exemptions aligns with DOJ's stated aim of the exemptions covering data typically required by the U.S. Food and Drug Administration (FDA).

- We caution against limiting the types of data subject to the exemptions. Narrowing the scope of data excluded could delay clinical research, create lags in improving clinical trial design, disrupt data transparency objectives to further research, hinder the return to clinical trial participants of their own data, undermine data sharing activities where anonymized study data that includes US participants is available to the research community through appropriate platforms and ultimately prevent or delay drug development in the US and globally.
- We recommend extending the scope of exemptions to include access to relevant data by internal personnel and third-party vendors in a country of concern to prepare the data for submission to relevant authorities. Local resources are necessary because every country has specific submission requirements that are best understood by local experts and often submissions must be made by a local agent. Submissions must also be made in the local language with the support of local personnel experienced in preparing submission documents and supporting material.

§ 202.511 Other clinical investigations and post-marketing surveillance data

- Existing FDA and regulatory frameworks protecting privacy already mitigate the national security risk associated with the transfer of bulk U.S. sensitive personal data. For example, clinical trial data submitted to FDA is subject to and has been acquired through FOIA requests with only participants' birthdates removed. DOJ should confer with FDA on this to accurately assess the potential effectiveness of the proposed US data export restrictions to protect the security of such data.
- It is not possible to identify or predict beforehand particular transactions as more important than other transactions to the conduct of a clinical investigation and that cannot otherwise be feasibly avoided without jeopardizing the clinical investigation. As a result**, exemptions must cover the full range of relevant transactions for the successful completion of a clinical trial.**
- Hundreds of clinical investigations would be disrupted if the proposed US data export restrictions were immediately applicable, causing overall end-to-end disruptions and critical delays from study planning and start up through to study completion and reporting. Any immediate re-structuring would not minimize disruption, as transition of activities would take multiple years to complete.
- The proposed data restrictions could create impracticable requirements for conducting clinical trials. For example, requiring a determination whether data collected outside of the U.S. contains data from U.S. persons when the nationality of a clinical trial participant may not be recorded or is otherwise not known due to existing de-identification practices could cause clinical trial work to stall. **NFTC respectfully recommends the creation of a safe harbor or extend an exemption to include scenarios in which data is collected outside of the U.S. with voluntary consent and it is not practicable to identify if a participant is a U.S. national.**
- **NFTC respectfully recommends permanent regulatory exemptions for certain health data** as the most effective, predictable and efficient means for both the US government and the US biopharmaceutical industry to enable the

development and delivery of innovative medicines while addressing US national security needs versus time-limited exemptions or licenses.

- We urge care in avoiding scenarios that would inhibit the sharing of R&D and clinical trial data for secondary use through voluntary, non-profit public-private data sharing platforms, such as Vivli, Transcelerate HTD and IMI. Secondary use of data is a key driver of further innovation and discovering new medicines and vaccines. Such data is also used to improve clinical trial design and learn more about a disease. **NFTC recommends creating an exemption to cover such secondary use of data after further conferring with relevant U.S. agencies, the data sharing platforms and the U.S. biopharmaceutical industry.**

Implementation of licensing program

NFTC recognizes and appreciates the extensive consultative process that DOJ has engaged in with other agencies to understand how licensing programs are set up and maintained. Nonetheless, we remain concerned about the ability of the DOJ to take on this monumental task that has such significant consequences across many government agencies in the U.S. and abroad as well as to other stakeholders including industries across many sectors and ordinary citizens and other U.S. persons. **We encourage DOJ to continue seeking more input from industry groups as such stakeholders have extensive experience with the licensing processes of different agencies. We further recommend carefully testing any licensing scheme before going live.**

NFTC draws attention to the creation of general licenses covering multiple transactions involving multiple parties. While such a measure is both necessary and welcome, we are concerned that this is not as well-defined as the provisions for specific licenses. **NFTC recommends further consideration of the scope and implementation of general licenses.**

About NFTC

The NFTC, organized in 1914, is an association of U.S. business enterprises engaged in all aspects of international trade and investment. The NFTC supports open, rules-based trade, including a level and competitive playing field. Our membership covers the full spectrum of industrial, commercial, financial, and service activities. Our members value the work of the Departments of Treasury and Homeland Security, and other agencies, in implementing E.O. 14117 to protect bulk sensitive data and U.S. government-related sensitive data from malign foreign actors.

Our goal is to always strengthen U.S. industries and their global supply chains as well as to help protect national security and economic security interests. Robust trade relationships are central to economic and national security. NFTC's National Security Policy Initiative brings the voice of business to policymakers on global security issues affecting international trade. Companies play a vital role in promoting American values, including human rights and democracy. Our data driven recommendations support American competitiveness and technology leadership that is central to our national security.

Thank you again for this opportunity to comment on this NPRM. We welcome the opportunity to discuss this important matter and answer any questions that you may have regarding these comments or recommendations. I can be reached at (202) 887-0278 or via email at jchu@nftc.org.

Sincerely,

Jeannette L. Chu
Vice President for National Security Policy