GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

APRIL 19, 2024

GDA RESPONSE TO U.S. DEPARTMENT OF JUSTICE ADVANCE NOTICE OF PROPOSED RULEMAKING

ACCESS TO AMERICANS' BULK SENSITIVE PERSONAL DATA AND GOVERNMENT-RELATED DATA BY COUNTRIES OF CONCERN, *89 FED. REG. 15780, DOCKET NO. NSD 104*

OVERVIEW

The Global Data Alliance (GDA)[1] appreciates the opportunity to provide comments in response to the Federal Register notice published by the US Department of Justice (DoJ) in connection with the White House Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern[2] and the DoJ's Advance Notice of Proposed Rulemaking (ANPRM) regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern.[3]

Following these brief opening comments, we present a detailed Executive Summary below, followed by a section-by-section discussion of the ANPRM.

GDA broadly supports DoJ's planned publication in August 2024 of draft regulations relating to "government-related data transactions" and relating to "prohibited bulk data broker transactions," subject to the resolution of other legal questions raised herein. As regards "prohibited genomic data transactions," we urge DoJ to take steps to ensure that any proposed regulations are focused on demonstrated national security risks.

However, in the context of "restricted transactions," we have serious concerns regarding the civil rights, cyber, privacy, security, and other legal implications of the ANPRM's proposed approach. For these transactions, we strongly urge DoJ to take additional time to develop an effective regulatory framework to address national security-related risks associated with "restricted transactions," while accounting for the legal, civil rights, and feasibility concerns. As drafted, the ANPRM would require thousands or millions of American companies to engage in high-risk activities to be able to analyze whether and to what extent their (or their employees' or business partners') digital content contains enumerated types of sensitive personal information and whether they meet the "bulk thresholds." The high-risk activities that the ANPRM could require of companies include: (1) decrypting encrypted data, (2) accessing proprietary or private data without authorization, and/or (3) creating

[1] The Global Data Alliance is a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on the ability to transfer data around the world to innovate and create jobs. Alliance members are headquartered across the globe and are active in the advanced manufacturing, aerospace, automotive, consumer goods, electronics, financial services, health, media and entertainment, natural resources, supply chain, and telecommunications sectors, among others. BSA | The Software Alliance administers the Global Data Alliance. For more information on the Global Data Alliance, please see: https://www.globaldataalliance.org

[2] See 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/

[3] See https://www.federalregister.gov/documents/2024/03/05/2024-04594/national-security-division-provisions-regarding-access-to-americans-bulk-sensitive-personal-data-and

large data sets of sensitive personal data for analytics purposes. These features of the ANPRM are decidedly not privacy- or cybersecurity-protective, and risk making US sensitive personal data less – not more – secure.

We urge DoJ to reconsider this design of the "restricted transaction" category under the ANPRM. GDA and its members commit to work intensively with DoJ to identify alternative, safer approaches to meet DoJ's stated objectives. For example, DoJ could consider requiring all US-incorporated companies to implement relevant aspects of the NIST and CISA risk management frameworks based on a self-assessment process, a standard of reasonable care, and the risk-based principles found in those frameworks. Alternatively, DoJ could also consider setting such an expectation of all US companies above a certain market capitalization, or US companies above a certain size or billing in countries of concern. Another approach might be to impose such requirements on US companies based on the nature or quantity of their investments in countries of concern. GDA is prepared to work closely with DoJ to explore how other agencies – including the Department of Homeland Security (Customs & Border Protection), Department of the Interior, the Securities and Exchange Commission, and/or the Federal Trade Commission – have developed different legal compliance frameworks that have met with varying degrees of success and effectiveness. As regards the "bulk thresholds," DoJ might consider converting those into a new *de minimis* exemption framework, which could help shift the legal burden in a way that could ameliorate the compliance risks noted above. In any case, we would still urge DoJ to assess whether certain thresholds (e.g., for genomic data) would need to be raised.

While we can support DoJ's publication of rules in August relating to "prohibited transactions" and "government-related data transactions" (subject to clarifications and comments below), we strongly oppose DoJ's publication of the ANPRM's envisioned rules relating to "restricted transactions" until civil rights, legal, and feasibility concerns can be addressed. As regards "restricted transactions," it is crucial for DoJ to take the time to carefully evaluate and develop legal frameworks that are more protective of the United States' civil and human rights, privacy, cybersecurity, and national security than the current ANPRM's proposed design for "restricted transactions."

EXECUTIVE SUMMARY

GDA respectfully offers DoJ the following recommendations:

A. Prohibited Transactions / Government-Related Data Transactions: Limit scope of the NPRM to "prohibited transactions" and certain "US government-related data transactions."

B. Restricted Transactions: Take additional time to develop an effective regulatory framework to address national security-related risks associated with "restricted transactions," while accounting for the legal, civil rights, and feasibility concerns raised by the proposal outlined in the ANPRM. A streamlined process to determining applicability is important.

C. Definition of Data Brokerage: Revise definition of "Data Brokerage" to align with US state law definitions, including elements of actual knowledge, financial consideration, arm's length sale, and a clear exclusion or non-data broker service providers. We urge you NOT to adopt the definition in HR 7520, which fails to address these concerns.

D. Bulk Thresholds: Revise the approach to bulk thresholds – a concept imported from Chinese law that raises several concerns. For example, bulk thresholds could be converted into an additional *de minimis* exception in the context of a streamlined approach to applicability (See comment B above).

    a. *If DoJ does not agree to take more time to develop a robust and effective regulatory framework covering "restricted transactions," then we would recommend that DoJ significantly raise all bulk*

thresholds until DoJ is able to address various legal, civil rights, and feasibility concerns discussed below.

E. Genomic Data Transactions: Revise the approach to genomic data based on a better understanding of the normal commercial and research-related contexts involving genomic data and existing risk mitigating circumstances. Also, perform a more rigorous risk assessment process. If necessary, develop a process for a classified review process that includes experts from the private sector and health agencies (HHS, FDA, NIH, CDC, Office of Pandemic Preparedness) holding security clearances.

F. Anonymized, Pseudonymized, De-identified, and Encrypted Data: Exclude such technically obscured data (in which a person's identity and the data is effectively delinked) from "bulk US sensitive personal data."

G. Compliance re Government-Related Data Transactions: For US Government Related Data, ensure that there is a clear and straightforward path to private sector compliance. Broadly, we consider the focus on limiting communications from geofenced areas to be more feasible in certain circumstances than monitoring or restricting specific data sets or digital activities of current or former government employees, which could effectively require service providers to surveil those US citizens and interfere with their digital activities – creating significant legal risks for all involved.

H. Employment Agreements: Before publishing draft rules on "restricted transactions" involving employment agreements, take time for the proper development of a risk-based approach that is tailored to address demonstrated national security risks associated with such transactions, while also accounting for the legal, civil rights, and feasibility concerns. Alternatively/additionally, clarify that the intra-entity exemptions covers all employees of a US entity and its affiliates in countries of concern, as well as employees of trusted vendors.

I. Vendor Agreements: Before publishing draft rules on "restricted transactions" involving vendor agreements, take time for the proper development of a risk-based approach that is tailored to address demonstrated national security risks associated with such transactions, while also accounting for the legal, civil rights, and feasibility concerns , including with respect to the contemplated very broad scope of what defines a covered person. Alternatively,/additionally, clarify that vendors are responsible for the security of the systems and services that they control, but not for the content of the data that they do not own, control, and transfer. Revise the definition of "vendor agreement" for greater specificity.

J. Processor-Controller Issues: Duly account for the different roles and responsibilities of controllers and processors to avoid inadvertently mandating breach of access limitations or confidentiality obligations in contract or federal/state law.

K. FAQs, Informed Compliance Manuals, and Sector-by-Sector Guides: Because the ANPRM has such wide applicability across numerous sectors, the proposed framework could produce unintended and unforeseen consequences in different sectors. We urge the DoJ to begin mapping out a process to develop sector-by-sector FAQs and guides to help promote informed compliance, better self-assessments, and better data security outcomes.

L. Exemptions / Exclusions: GDA recommends that DoJ undertake the following revisions or additions:

1. *Intra-Entity*: Clarify that the intra-entity exemption applies to all employees in a country-of-concern, as well as "trusted vendors" and their employees.

2. *Intra-Entity*: Clarify that the intra-entity exemption encompasses data transfers made over systems that the company has contracted to store or process certain company data (e.g., accounting, ICT, or human resource services that contain the company's data and that the company has contracted for).

3. *Intra-Entity*: Clarify that the intra-entity exemption relates to data transactions that are "ordinarily incident to and part of administrative or ancillary business operations."

4. *International Agreements*: Clarify that the exemption for international agreements covers the following:

    a. "Data transfers that are incident to an international agreement recognized or signed by the United States. A non-exhaustive list of those agreements will be set forth in an Annex to the NPRM";

    b. "Data transfers conducted in support of activities relating to international standards-setting and/or in support of listed international standards development organizations. Relevant standards and standards-development organizations will be set forth in an Annex to the NPRM";

    c. "Data transfers that are conducted in support of, or incidental to the activities of, any inter-governmental organization; any international private sector organization in which US entities [actively] participate; or any international labor organization in which US labor unions [actively] participate. A list of those organizations will be set forth in an Annex to the NPRM."

5. *Regulatory Compliance*: Clarify that the exemption for purposes of regulatory compliance applies to all US laws and statutes with US persons are required to comply – not simply those relating to financial services and payment processing.

6. *Communications & Informational Materials*: Clarify that exclusions for personal communications and informational materials under IEEPA cover emails, voicemails, messaging, and similar communications in any medium, as well as books, music, film, software, and other published content in any medium.

7. *Personal Health Data*: Add an exemption for personal health data (similar to the exemption for personal financial data) to take into account the nature of how responsible and secure general and pre-clinical research, clinical trial practice, post-market surveillance, pharmacovigiliance, and other aspects of the healthcare supply chain work.

8. *Personal Financial Data:* Further refine the scope of the exemption for financial-services, payment processing and regulatory compliance-related transactions to take into account the nature of how financial and payment services work.

9. *Telecom Data:* Clarify that all data necessary and incidental to the provision and delivery of communications services remain outside the scope of any restrictions on personal sensitive data for consumers, enterprises and government. Global commerce relies on effective and efficient global communications. Communication services are the thread that connects families, communities, and businesses of all sizes to the world. Establishing barriers to communications risks disruptions to U.S. persons' ability to communicate and risks undermining U.S economic competitiveness.

10. *Non-Personal Data; Machine-to-Machine Data*; *Publicly Available Data*: Add exemptions to make clear that:

    a. "'Bulk US sensitive personal data' does not include non-personal data, including machine-to-machine data."
    b. "'Bulk US sensitive personal Information' does not include public record or publicly available data."

M. Safe Harbors and Indemnification: Add the following safe harbors and indemnification provisions.

1. *Safe Harbor & Indemnification for Breaches of US Law* Resulting from Efforts to Comply with the US Data Security Rules: Provide that a person shall not be held liable under any federal or state law, and shall be indemnified by the US government for any claims made against it under any such law as a result of that person's good faith efforts to comply with the requirements of these regulations.

2. *Indemnification for Breaches of Foreign Law* Resulting from Efforts to Comply with the US Data Security Rules: Provide that a person shall be indemnified by the US government for any claims made against it under any foreign law as a result of that person's good faith efforts to comply with the requirements of these regulations.

3. *Safe Harbor for Data Outside a Person's Control*: Provide that a person is exempted from any requirement that otherwise apply to that person in respect of 'bulk sensitive US personal data' over which that person lacks access, control, and a legal authority.

N. Fully Assess Privacy, Civil Rights, and Other Legal Implications of the Proposed "Restricted Transaction" Categories: As elaborated below, implementation of the "restricted transaction" categories would appear, in some cases, require private companies to surveil and monitor the content of digital transmissions within the United States between a US citizen and a person of a country of concern (and in some cases, US digital transmissions between two or more US citizens) – raising privacy, intellectual property, and other legal concerns. DoJ should take the time to evaluate how to eliminate this risk before publishing any draft regulations on "restricted transactions."

SECTION-BY-SECTION COMMENTS

Introduction

GDA recognizes and appreciates the dedication, creativity, and diligence of the National Security Division (NSD), the Department of Commerce (Commerce), the Department of Homeland Security (DHS), the National Security Council (NSC), and the National Economic Council (NEC), as well as other US departments and agencies, in preparing this ANPRM. It is evident that the US government committed significant time, resources, and attention to this effort. GDA also appreciates the efforts of these organizations to engage in advance consultation with the private sector regarding the ANPRM.

GDA strongly supports the US government and its commitment to addressing risks identified by the President in the EO. At the same time, GDA urges the US government to address those risks in ways that do not create unintended consequences that inadvertently increase security risks or undermine privacy for Americans, particularly as Congress considers comprehensive privacy legislation. We also urge the US government to implement the EO in a way that safeguards other interests that require ongoing cross-border data visibility and access to information, including those relating to cybersecurity, environment/climate, economic opportunity, health, human rights, safety, technological competitiveness, and US global leadership among allied democracies.

In short, the US government should issue draft regulations in August relating to "prohibited" data brokerage transactions and to "US government-related transactions." However, we strongly oppose its issuance of draft regulations in August relating to "restricted transactions." We present GDA's comments in greater detail below.

Section A – Overview and Identification of Risks

The GDA strongly supports the US government and its commitment to addressing risks identified by the President in the EO. This includes working to ensure that governments in countries of concern do not misuse their access to Americans' bulk sensitive personal data to: (1) engage in malicious cyber-enabled activities and malign foreign influence; (2) track and build profiles on US individuals, including members of the military, federal employees, and contractors, for illicit purposes such as blackmail and espionage; and (3) collect information on activists, academics, journalists, dissidents, political figures, or members of non-governmental organizations or diverse or marginalized communities in order to intimidate such persons; curb political opposition; limit freedoms of expression, peaceful assembly, or association; or enable other forms of suppression of civil liberties.

The ANPRM sets out an approach to mitigating these risks by prohibiting certain bulk US sensitive data sales by data brokers, and by restricting access to US government-related data. GDA offers several comments below that we believe will make the ANPRM's proposed approach more effective at achieving its stated aims.

However, GDA urges DoJ to undertake a more rigorous, evidence-based analysis, in consultation with private sector experts, regarding the nexus between the risks identified in the ANPRM and genomic data transactions, employment agreements, investment agreements, and vendor agreements. More specifically, we urge DoJ to work with counterparts in the private sector (if necessary, with security clearances) to better understand the specific case studies in which Americans' sensitive personal data is being misused to compromise national security. We also urge DoJ to conduct a meaningful technical feasibility analysis regarding effective countermeasures. Countermeasures should be tailored to address demonstrated real-world risks.

Taking a step back to view this issue more broadly, we urge the Administration to avoid implementing the ANPRM in ways that draw upon China's failed model of data export restraints. China's restrictive policies have not only proven ineffective, but have also been deeply damaging to China's own interests from an economic, health, safety, scientific, and technology perspective. We also observe that certain aspects of China's data transfer regime present particular concerns from a human rights perspective. We urge DoJ to take special care to ensure that none of the digitally authoritarian elements of China's data transfer framework are inadvertently incorporated into the US legal system.

Recommendation: GDA recommends that the DoJ undertake a full and comprehensive legal analysis of the concerns – including civil rights concerns – raised in the submissions by the GDA and other organizations.

Section B – Bulk Sensitive Data

GDA offers the following comments regarding Section B.

1. **"Sensitive personal data"** – The proposed definitional scope of "sensitive personal data" is broad and diffuse, encompassing dozens of "covered personal identifiers," "geolocation data," machine and IoT "sensor data," "personal health data", "personal financial data," and other types of data. This piecemeal scoping approach creates unnecessary ambiguity, increases risks of overbroad interpretation, and could lead to a lack of coherence in implementation. We observe that this piecemeal definitional approach – which appears to sweep in non-personal geolocation and sensor data – would appear to implicate a wider universe of data than is protected under even the EU's General Data Protection Regulation or other global data protection laws. The definition is also significantly broader than similar definitions found in comprehensive privacy laws enacted by US states and definitions used by various US federal agencies. The national security goals outlined in the EO and ANPR are best achieved by focusing on truly sensitive data types that pose the highest risk to US persons and US security interests.

   Recommendation: GDA recommends a more coherent and unified definition that is explicitly tied to a demonstrated national security risk based on specific use cases developed by DoJ. Data that does not meet this metric should not be covered.

2. **"Anonymized, Pseudonymized, De-identified, and Encrypted Data"** – The ANPRM initially proposes an overbroad definition of "bulk US sensitive personal data," by including such obscured data types as part of this definition. In the data privacy and data security context, data anonymization, pseudonymization, de-identification, and encryption are technical means to obscure or eliminate personally identifying characteristics of data by removing the relationship between the data and any specific person.

   Anonymized data is, by definition, data that has rendered an individual "unidentifiable". Anonymization techniques enable data to be leveraged for analysis and insights, help protect trade secrets and intellectual property, and prevent competitors from accessing sensitive information while protecting individuals by preventing their identification. The ANPRM itself acknowledges the benefits of anonymized data by identifying classes of listed identifiers and the rules on their combination that aim to identify an individual from a data set or link data across multiple data sets to an individual. The ANPRM also excludes from the definition of sensitive personal data any public or nonpublic data that does not relate to an individual. However, this guidance appears in direct contradiction with a proposal to wholesale include "anonymized" data within the definition.

   Encryption means that identification of an individual or linkability to other listed identifiers is only able to occur where an entity is in possession of the encryption key or has the means necessary to obtain the encryption key. Therefore, without access to encryption keys, encrypted data is unavailable and unexploitable, and therefore does not pose a national security risk. Further, encryption is proposed as one of the four security conditions permitting Restricted Transactions (Section I), so it is already recognized as a security control sufficient to mitigate the identified national security risk. The reference to encrypted data may also curtail the usefulness of privacy enhancing technologies such as homomorphic encryption which rely on cryptographic techniques.

   DoJ's proposed approach appears to defeat the purpose of these data security protocols. DoJ's proposed approach may ultimately weaken US national security and US data security by failing to differentiate between data that is encrypted or otherwise protected, and data that is not. DoJ's approach could de-incentivize the adoption of these important data security measures. Furthermore, requiring companies to decrypt or de-anonymize data in order to assess whether they have filled bulk thresholds is a high-risk activity that would undermine data privacy and security. Accordingly, these types of data should be excluded from scope of "bulk US sensitive personal data."

   Recommendation: We strongly urge DoJ not to treat anonymized, pseudonymized, de-identified, and encrypted and similarly obscured data as falling within scope of "bulk US sensitive personal data."

3. **"Covered Identifiers" –** The definition of "covered identifiers" includes various data types that are not considered sensitive under other laws or regulations, and in many cases are actually necessary to provide technology services (such as device IDs and information necessary to authenticate). Companies regulated by global data protection laws and regulations have already completed data categorizations and risk assessments aligned to standard international definitions of sensitive personal data. So focusing on truly sensitive data aligned to global standards would decrease the compliance burden on companies and bring definitional consistency across various countries, US states, and US federal agencies.

   More specifically, the proposed definition of "listed identifier" includes truncated versions of government IDs. It is unclear why such truncated and largely de-identified data would be considered to implicate national security. For example, use of the last four digits of a social security number is extremely common in many commercial contexts.

   Similarly, the proposed definition of "Biometric Identifiers" differs from its common understanding and usage. Such "identifiers" are normally constructed around a unique set of data that is used to identify people, such as a numerical representation of a retina scan, fingerprint, or facial geometry. However, the ANPRM's definition goes further, and includes actual facial images, even if the image hasn't been analyzed and reduced to a numerical value. Basically, any picture or photo would fall under this ANPRM definition. This seems legally and technically incorrect.

   Recommendation: We urge DoJ to review the definition, scope, and examples of "covered identifiers." Many of these appear not to clearly implicate national security concerns. Several of them appear to be defined in terms that are not technically accurate. Finally, there appears to have been no economic impact analysis of the different case studies and scenarios in which such identifiers are restricted. We urge the DoJ to undertake that analysis.

4. **"Geolocation and Related Sensor Data" –** GDA observes that geolocation data is used in innumerable contexts, including weather forecasting, pandemic preparedness, air traffic control, and numerous other environmental, health, and safety contexts. GDA also observes that "sensor data" is used in an even wider range of contents, across supply chains and in various industrial IoT applications. The proposals to restrict impose ANPRM restrictions on any transactions involving combinations of data of more than 100 US persons or US devices could effectively imply an embargo on any and all "geolocation" and "sensor"-related data transfers to China and other countries of concern. This data category is overbroad given that many of the contexts involving geolocation or sensor data do not involve an association between the data at issue and any identifiable person. Any cases that exclusively or predominantly involve non-personal data should not be covered within the scope of the ANPRM.

5. **"Personal Health Data" and "Genomic Data."** The US healthcare sector – including healthcare providers and researchers in the medical device and biopharmaceutical sector – rely on personal health and genomic data to improve the lives of Americans and people around the world. For example, in the biopharmaceutical context, such data are collected and analyzed for: (1) research to identify candidates for innovative medicines and vaccines; (2) testing and establishing the safety and efficacy of medicine and vaccine candidates through clinical trials; (3) establishing compliance with the US and other government's safety and efficacy requirements to be authorized for use; and (4) meeting the US and other government's requirements to identify existing products' safety performance. Thus, access to and sharing of relevant personal health and genomic data in a secure environment is necessary for promoting open, responsible scientific collaboration to drive innovation that contributes to public health. It is also critical to the competitiveness of US industry, the industry's contribution to US innovation leadership and health security, and US economic growth.

   US industry supports addressing the national security threats posed by certain data transactions. However, the industry is concerned that the proposed restrictions could inadvertently and unnecessarily prevent the

industry's legitimate and practicable use of relevant personal health and genomic data. Depending on the interpretation of the proposed restrictions, the restrictions could:

- Potentially prevent US companies from leveraging the best global talent to conduct research and enable the development of innovative technologies, diagnostics, medicines, and vaccines, undermining global health and the competitiveness of US industry.
- Potentially prevent the conduct of global or multi-regional clinical trials, while imposing regulatory burdens for including US persons in clinical trials. The proposed data restrictions could also create impracticable impediments to much of the safe and responsible clinical research that is conducted today. An example is potentially having to determine if data collected outside of the US contains data from US persons when the nationality of a clinical trial participant may not be recorded or is otherwise not known due to existing anonymization practices. The industry further notes that it can be required to submit biospecimens containing genomic data (such as blood, serum, and plasma) to a government to obtain regulatory approval to conduct a clinical trial.
- Potentially prevent submission of clinical trial and other data for government regulatory authorization, denying patients access to innovative medicines and vaccines, putting public health at risk, and undermining US biopharma competitiveness by limiting market entry. Also, if a US biopharmaceutical company cannot obtain regulatory authorization and enter a market, the company could potentially lose related patent protection for the product due to "failure to work" requirements, thereby possibly giving away US innovation.
- Potentially prevent 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.
- Potentially prevent submission of pharmacovigilance data to governments in accordance with globally accepted Good Pharmacovigilance Practices (GVP), diminishing safety monitoring and putting public health at risk.

Recommendations: To address these concerns, the Department should take additional time to develop a framework that does not require US companies to undertake "high risk" activities, such as (1) decrypting or de-anonymizing data in order to tally up data types or numbers of persons, (2) creating sensitive personal data pools for analytics purposes that would provide a priority target for adversaries, and (3) accessing propriety data without authorization.

Furthermore, in respect of Prohibited Genomic Transactions, the Department should focus on identifying discrete classes of transactions that raise the highest national-security risks and that pose direct risks, as well as on taking calibrated actions to minimize the risks associated with access to Americans' bulk sensitive genomic data. The Department's approach should be revised based on a better understanding of the normal commercial and research-related contexts involving genomic data and existing risk mitigation techniques that are already being applied to address the concerns raised in the EO. The personal genomic data at issue is anonymized, pseudo-anonymized, or otherwise deidentified, that is, not personally identifiable on its own. The industry would note that such genomic data is not accompanied by other information that would allow it to be used to identify an individual. As a result, this data is not suitable for conducting the activities, influencing, tracking, profile building and other information collection activities that are identified as of concern.

As noted above, we recommend that the Department should:

- *Take additional time to develop a safe and effective approach to addressing national security risk for Restricted Transactions. Such an approach should not inadvertently increase privacy risks and data security risks (as the current proposal would appear to do). Instead, we urge the Department to develop a more streamlined and simplified approach to determine which companies must comply with security requirements for Restricted Transactions. Those requirements should adopt the risk management and self-assessment principles of the NIST and CISA risk management frameworks discussed.*

- *Exclude anonymized, pseudo-anonymized, and otherwise deidentified personal health and genomic data that is not personally identifiable on its own. Data that is anonymized, pseudonymized, or de-identified by its nature is not identifiable to a US person without other data that are not included or otherwise available. At the very least, any restrictions on such data should reflect its deidentification.*
- *Exclude transfers of personal health and genomic data between a US company and its foreign subsidiary for the conduct of business activities.*
- *Exclude transfers of personal health and genomic data that is not personally identifiable on its own through data sharing platforms for the purposes of secondary use research.*
- *Exclude transfers of personal health and genomic data that is not personally identifiable on its own for the purposes of obtaining regulatory approval to conduct a clinical trial, submitting clinical study reports and similar submissions to obtain regulatory authorization (i.e., demonstrating safety and efficacy), or complying with pharmacovigilance reporting requirements.*
- *Any security requirements should be practicable, risk-based and reflect current practice, valuing the importance of enabling biopharmaceutical research and developing innovative medicines and vaccines for public health and the competitiveness of US industry.*
- *The industry encourages the Department and other relevant agencies to meet with the US biopharmaceutical industry, medical device, diagnostics, healthcare delivery, and health insurance industries to further discuss the above concerns and obtain further information.*
- *Finally, if some of the concerns described in the EO are based on classified information, then we would urge the Department to develop a formal process for a classified review process that includes experts from the private sector holding appropriate security clearances, as well as representatives from health agencies (HHS, FDA, NIH, CDC, Office of Pandemic Preparedness) holding security clearances. It is critical that the health-related aspects of the ANPRM be: (1) based on accurate information, (2) informed by a complete and clear understanding of how governments and the private sector already do – and can – work together to achieve the best possible health outcomes for Americans, and (3) carefully weigh all relevant health-related considerations to arrive at a carefully calibrated approach that does not sacrifice health or security.*

6. **Controller/Processor Distinction –** Distinguishing between controllers and processors is a foundational aspect of data privacy and security rules worldwide and in every state. Laws that recognize these different roles better protect personal data privacy by crafting different obligations for different types of businesses based on their different roles in handling personal data. The DoJ's proposed framework would be improved by reflecting this important distinction. The framework should make clear what safeguards are applicable to data controllers, which are the companies that determine the purpose and means of processing consumers' personal data. The framework should also make clear what safeguards are applicable to processors (sometimes called service providers), which are companies that process data on behalf of a controller and pursuant to its instructions. Failing to make this clarification would infuse unintended ambiguity regarding the respective responsibilities of various entities in relation to various types of data transactions, thus impeding compliance. Furthermore, failing to make this clarification could imply government obligations on controllers to surveil, monitor, or access their customers' data in ways that are prohibited by contract and that may produce unintended breaches of privacy, personal data protection, regulatory data protection, trade secret, or other confidentiality-related laws.
   Recommendations: The framework should distinguish between controllers and processors.

7. **Bulk Thresholds** – The decision to adopt bulk thresholds for data should be reconsidered. This is a concept pioneered in China without seeming consideration of the human rights implications, the effectiveness in addressing data security, and the feasibility of implementation, and to the ultimate detriment of the China's economy, competitiveness, and security.

   Recommendation: Our ultimate recommendation is three-fold:

   a. *Take additional time to develop an effective regulatory approach to "restricted transactions" in the form of "employment agreements," "vendor agreements," and "investment agreements," pending resolution*

of the many questions relating to bulk thresholds and legal, civil rights, and feasibility questions with respect to "restricted transactions" more generally. GDA members commit to working diligently and expeditiously with DoJ to assist in the development of information regarding the threats to national security and the appropriate countermeasures within the "restricted transaction" category.

i. *One possible approach would be to convert the bulk thresholds from an affirmative element of a legal framework that must be fulfilled to determine applicability to a de minimis exemption for transfers that fall below those thresholds. Combining a simpler and more streamlined approach to determining applicability – coupled with a de minimis exemption below certain thresholds – would relieve companies from government mandates to engage in high-risk activities in order to determine whether the framework applies. Instead of needing to focus resources on pooling sensitive data, decrypting encrypted data, and accessing sensitive data (possibly without authorization) to determine whether they fall within the scope of bulk thresholds for each of the six data types, companies could instead rely on a more straightforward way of determining applicability, allowing them to direct their resources on risk-based compliance with the NIST Risk Management Frameworks. Adding a de minimis exemption would offer the added benefit of avoiding an undue burden on those companies that have a high degree of confidence that they fall within the de minimis exemption or another exemption. This offers a safer and more secure way to establish a program that promotes compliance and allows companies to invest in data security – rather than a complex and risky data analytics framework.*

ii. *If DoJ does not agree to take additional time to develop its "restricted transaction" approach, then we recommend that DoJ apply a single threshold of "more than 1,000,000 US persons" or "more than 10,000,000 US devices" for each of the following data types – i.e., geolocation data or sensor data, personal health data, personal financial data, biometric identifiers, and covered personal identifiers. We recommend that DoJ apply a single threshold of "more than 1,000 US persons" for human genomic data.*

b. *As regards "prohibited transactions" involving "genomic data," we urge DoJ to raise the threshold for human genomic data to be the same as the threshold for biometric identifiers and geolocation data, pending a more comprehensive assessment of risks.*

c. *As regards, "prohibited transactions" that deal exclusively with data brokerage sales, GDA would be less concerned with the thresholds outlined in the ANPRM, provided that DoJ is able to refine the definition of "data brokerage" in the ways that we recommend in Section D.3 below. We would note as a general matter, however, that a single threshold may be more reasonable to administer than the current bifurcated "low" and "high" thresholds. We would generally recommend that DoJ simply apply the "high" threshold to provide the public and regulated entities with a clear rule.*

GDA outlines several concerns regarding the Bulk Threshold proposal below.

d. **Legality under Federal Law** – With respect to the application of "bulk thresholds" to "restricted transactions," we request that the DoJ NSD provide responses to the following questions:

i. Have the NSD, DoJ Civil Rights Division (CRD), DoJ Office of Legal Policy (OLP), the DoJ Criminal Division, the DoJ Antitrust Division (ATR), the Department of Treasury (Treasury), the Department of Health & Human Services (HHS), and the Federal Trade Commission (FTC) analyzed whether – for purposes of assessing whether the ANPRM's bulk thresholds are met and whether any of the six types of sensitive personal information are implicated – it is legally permissible for private enterprises to review US citizens' protected data sets that would be necessary to that assessment? If so, will DoJ make the results of that legal research public? If not, can DoJ commit to make that legal guidance publicly available?

ii. For purposes of questions (d)(i) above, the analysis should address requirements under the US Constitution and federal law (Computer Fraud & Abuse Act (CCFA), Graham-Leach-Bliley Act (GLB), Children's Online Privacy Protection Act (COPPA), Health Insurance Portability and Accountability Act (HIPAA), the Defend Trade Secrets Act (DTSA), the Trade Secrets Act (TSA), the Stored Communications Act (SCA), the Food, Drug & Cosmetics Act (FDCA), the Federal Communications Commissions' Customer Proprietary Network Information (CPNI) Rules, and any other US federal and state rules that impose data confidentiality obligations that may be implicated.[4]

iii. Has DoJ undertaken a comprehensive assessment of any other federal rules that might be implicated or breached through efforts to comply with the ANPRM bulk threshold requirements or other aspects of the ANPRM? If so, will DoJ make the results of that legal research public? If not, can DoJ commit to generate that public research and make it public?

iv. If DoJ is not prepared to take additional time to address the aforementioned legal concerns before publishing rules with respect to "restricted transactions," DoJ and other relevant departments should ensure that private enterprises are given effective legal safe harbors from liability for any legal violations of the laws noted in (d)(ii) that the US government's "restricted transaction" mandates would facilitate or require. We request that DoJ provide a detailed explanation and proposal for how such a safe harbor from liability would work. We also ask that DoJ clarify whether such a safe harbor require a legislative amendment to the statutes noted in (d)(ii), or would DoJ regulations suffice to provide such a safe harbor from liability.

e. **Legality under State Law** – With respect to "restricted transactions," has DoJ secured legal analyses from the 16 US states that have recently enacted state privacy legislation regarding the legality of requiring private enterprises to track US citizens and monitor the content of their communications in order to assess compliance with the bulk threshold requirements? Has DoJ undertaken a comprehensive assessment of any other US state laws that might be implicated or breached through efforts to comply with the ANPRM bulk threshold requirements or other aspects of the ANPRM? If so, will DoJ make the results of that legal research public? If not, can DoJ commit to generate that public research and make it public?

f. **International Legal Concerns / Interoperability Concerns –** With respect to "restricted transactions," has DoJ evaluated how a government requirement to monitor content for the presence of the six protected data types in excess of the bulk thresholds can be conformed with limitations on processing of personal information of EU Data Subjects under the General Data Protection Regulation and/or with similar requirements in other country laws? Has DoJ sought input from the Office of Legal Counsel or relevant offices within the Department of Commerce, the Department of State, and the Federal Trade Commission? If so, will DoJ make the results of that legal research public? If not, can DoJ commit to generate that public research and make it public?

g. **Feasibility** – For restricted transactions, as a practical matter, how are companies expected to determine whether a bulk threshold is met? For example, many companies do not have mechanisms to tallying up the number of persons (let alone specific subcategories of personal information) involved in any particular transaction – and the review of employee or customer data for that purpose will be

[4] Relevant US state privacy rules include the California Consumer Privacy Act (amended by CPRA), Virginia Consumer Data Protection Act, Connecticut Data Privacy Act, Colorado Privacy Act, Utah Consumer Privacy Act, Oregon Consumer Privacy Act, Florida Digital Bill of Rights, Texas Data Privacy and Security Act, Montana Consumer Data Privacy Act, Iowa Consumer Data Protection Act, Nebraska Data Privacy Act, New Hampshire Privacy Act, Delaware Personal Data Privacy Act, New Jersey Privacy Act, Tennessee Information Protection Act, Maryland Online Data Privacy Act, Indiana Consumer Data Protection Act, and Kentucky Consumer Data Protection Act.

prohibited in many cases under contract, commercial, tort, unfair competition, or criminal laws; intellectual property laws (e.g., trade secrets); privacy and personal data protection laws; regulatory data protection laws; and others.

A discussion of what should be a fairly simple scenario involving business communications highlights how difficult it will be to administer the bulk thresholds. The body of a business email and any attachments may contain other "listed identifiers"[5] or "sensitive personal data" types covered by the ANPRM.[6] This scenario raises the following questions:

i. How are companies to determine whether the 10,000-unit bulk threshold for such linked identifiers is satisfied?

ii. For example, should every US company hire a new team of IT engineers to aggregate all of the corporate emails from one corporate domain (used by thousands, or tens or hundreds of thousands of employees) to a country of concern, and then have those IT engineers review all of those emails and attachments to segregate and tally up all of the different types of personal information across all of those emails?

iii. Because the ANPRM requires an assessment of multiple covered data transactions across a course of dealing between the same or related parties, would each US company's IT engineering team also need to develop multiple decrypted data sets for analysis – aggregating thousands of employee and business partner emails over time and with different counterparties in countries of concern?

iv. Would each US company's IT engineering team also develop analytical filters based on the six major data types and the dozens of different personal identifier types, and develop a data analytics and reporting mechanisms for each of these personal data and personal identifier typologies?

v. Will this data analysis requirement be imposed on all 6.1 million US private sector firms and any US citizens who engage in data transmissions or transactions with China or any other five countries of concern?

vi. Has the DoJ undertaken any economic assessment of the cost of such requirements on these firms and citizens? If so, could you please publicize the results of those assessments? If not, could you please make that clear and develop a framework of questions to be addressed, consistent with EO 12866?

The questions above – which apply exclusively to business email communications and not any of the other transaction types that may be implicated by the ANPRM – provide a glimpse into the complexity presented by the current ANPRM. We observe the other scenarios involved cross-border services (especially those that are not point-to-point as email transmissions are) could present even greater compliance challenges.

[5] See ANPRM, 89 Fed. Reg. 15780, at 15784.

[6] GDA respectfully submits that emails qualify as "communications" under IEEPA (cite) and therefore are not "US sensitive personal data." If DoJ were to adopt a different interpretation, the email address alone would likely be treated as "US sensitive personal data" because email addresses are typically linked within the email metadata to a person's name and often the person's phone number or address. This example shows how a broad interpretation of "personal identifiers" could produce the (unintended) result that every email is "US sensitive personal data" simply because the email address metadata contains "linked" "covered personal identifiers." This example also highlights the importances of the DoJ's maintaining a broad interpretation of "communications" under the IEEPA exemption.

Recommendation: GDA underscores that these questions are not merely rhetorical. To the extent that DoJ intends to proceed with publication of regulations regarding "restricted transactions," we would appreciate the DoJ's responses to these questions for each of the "restricted transaction" categories and for each of the six sensitive data typologies.

8. **Encryption –** How should companies analyze the six personal data types in encrypted data sets? Are companies expected decrypt encrypted data sets to perform this analysis? Such a process would undermine data security and data privacy – creating more vulnerabilities and exposure points, as large data sets are decrypted and made more vulnerable to exfiltration and interception. It would also create serious legal concerns for companies to the extent that it would effectively require companies to engage in the unauthorized decryption and analysis of customer trade secrets, customer information protected from access or disclosure by contractual provisions, and/or customer information protected by privacy and personal data rules. Has DoJ consulted internally within the NSD, with the DHS Cybersecurity & Instructure Security Agency (CISA) and with other cybersecurity focused agencies to assess the security implications of such a decryption mandate? Has DoJ consulted with relevant offices at Commerce and State to assess the IP, commercial, trade, and other international legal ramifications of such a requirement? If so, will DoJ make the results of that legal research public? If not, can DoJ commit to generate that public research and make it public?
   Recommendation: Exclude encrypted, anonymized, de-identified, and other obscured data sets from the scope of the framework.

Section C – Government-Related Data

The ANPRM prohibits two categories of transactions involving government-related data: (1) the communication of "precise geolocation data, regardless of volume, for any location within any area enumerated on a list of specific geofenced areas associated with military, other government, or other sensitive facilities or locations;" and (2) "any sensitive personal data regardless of volume, that a transacting party markets as linked or linkable to current or recent former employees or contractors, or former senior officials, of the US government."

GDA requests the following clarifications from DoJ:

1. **Geofencing Proposal –** With respect to DoJ's geofencing proposal, restricting data outflows from such a facility may be possible through secured private networks and physical access controls in the facility. However, devices that connect to commercial networks while in that facility may not be covered and could be very difficult to control. We urge DoJ to clarify its intentions and narrow the scope to put the burden on the facility to control how people within that facility connect with commercial networks.

   Specifically, GDA requests that DoJ consider what layered cyber-defense approaches may be appropriate. Among other things, this could include employment- or contract-based:

   a. Prohibitions on government employees bringing or using devices capable of online communication when transiting to or within restricted areas; and
   b. Prohibitions on government employees logging into any personal email, shopping, software or other online accounts on any government device within a geofenced area.

   Such employment- or contract-based restrictions on online access by government employees or contractors in or around geofenced areas are likely to be among the most effective means of obscuring any association between a particular government employee or contractor and a particular location or device.

2. **Data Brokerage Proposal –** With respect to prohibitions relating to "any sensitive personal data regardless of volume, that a transacting party markets as linked or linkable to current or recent former employees or contractors, or former senior officials, of the US government," GDA understands that this prohibition relates to data broker transactions specifically designed to offer government employee or contractor-related data sets. GDA has questions and concerned regarding the breadth of what may be "linkable" and recommends that this prohibition be limited to data that is "marketed" as "linked" to government employees or contractors.

   In any case, GDA understands that focus of this prohibition is on the "marketing" of such data sets for sale. GDA requests that DoJ make clear that this prohibition relates specifically to this data broker context. If this prohibition were expanded beyond the data broker marketing context, it would raise significant privacy, security, and feasibility concerns in implementation. However, if this prohibition remains focused in the way that the ANPRM suggests, GDA does not see the same level of concern.

3. **Legality / Privacy Risks –** The government-mandated surveillance and civil rights/privacy concerns raised by DoJ's proposed bulk thresholds and other data rules in other contexts do not appear to be implicated in the context of its rules relating to government-related data, which GDA understands would require either: (1) a deactivation of all devices (or all devices save for a limited subset of identified devices) within a geofenced area; or (2) a prohibition on the marketing for sale by data brokers of data sets relating to government employees or contractors.

4. **Security Risks –** Because DoJ's proposals do not appear to require service providers to collect and maintain a comprehensive data set of government or contractor personal data, many of the security-related concerns that arise in respect of other aspects of the ANPRM do not appear to be implicated in the context of this subsection of the ANPRM.

Section D – Covered Data Transactions

The ANPRM identifies "prohibited" and "restricted" categories of transactions. As noted above, GDA respectfully submits that DoJ should focus on promulgating effective rules regarding prohibited transactions.

We urge DoJ not to yet promulgate rules on restricted transactions, given that the current formulation of those restrictions appears to be overbroad and poorly tailored to address any identified risk. DoJ should devote additional time to work with government, industry, and other stakeholders to determine the appropriate scope of such restrictions and any associated remedial measures.

GDA offers the following comments on several of the concepts introduced in this Section.

1. **Covered data transaction –** The definition of "Covered data transaction" is broad and includes "any transaction that 'involves' any bulk U.S. sensitive personal data or government-related data". We seek clarification on how 'involves" should be interpreted for further legal certainty. Such clarity would be beneficial for example in situations where the US person is an intermediary in a transaction involving bulk US sensitive data, but such intermediary services would not involve the actual transfer of the bulk US sensitive data from the data broker to a covered person because the data broker would execute its services directly, on the covered person's behalf without transferring or disclosing the US bulk sensitive data to the intermediary. This situation could be used to deliver certain marketing services to covered persons without providing them with access to the underlying data, thereby achieving the Administration's aim of interoperability and without hindering commercial transactions that don't pose a security risk. Where the intermediary or a covered person does not access or receive the US bulk sensitive data, it should be confirmed that such transactions are out of scope.

   Recommendation: GDA recommends that DoJ clarify how "involves" should be interpreted.

2. **US Device –** The definition of "US device" is overbroad to the extent that it does not reference any digital communications capability and to the extent that it includes any device "linkable" to a US person. First, we understand that the ANPRM does not intend to capture a mechanical or physical "device" that lacks digital communications capability. The ANPRM definition should be clearly limited to devices possessing that capability. Second, any device capable of digital communications anywhere in the world may be potentially "linkable" to a US person – including an unactivated iPhone on an assembly line or in the possession of a non-US person. The ANPRM does not intend to capture such devices that are not actually "linked" to a US person, so the definition should be amended accordingly.

   Recommendation: We recommend that the ANPRM adopt the following definition:

   > *US Device means "any device used for communications over digital networks in the United States that is linked ~~or linkable~~ to a US person."*

3. **Data Brokerage** – The definition of "data brokerage" in the ANPRM is much too broad and it would likely unintentionally sweep into scope a range of service providers that process data on behalf of business customers. These may include cloud service providers, telecommunications service providers, Internet service providers, software service providers, and other service providers that process data on behalf of business customers and pursuant to their instructions. Service providers may fall into this definition because they may provide access to data the service provider did not collect directly from individuals; rather, the service provider's business customers collected the information from consumers and then provided the information to the service provider for processing. We strongly recommend the scope of this definition be narrowed to avoid capturing service providers within the ANPRM's prohibited restrictions. Because DoJ has identified cloud service agreements and similar agreements as "restricted" vendor agreements, we understand that DoJ does not intend to treat these agreements as "prohibited" data brokerage transactions.

Recommendation: We recommend that DoJ change the definition to "data broker" and change predicate it upon the following:

a. Actual knowledge (i.e., the data must be knowingly collected and sold);
b. Financial consideration for the sale (i.e., that the sale of data is in exchange for monetary or other value);
c. Arm's length sale (i.e., that the sale of the data is made in an arm's length transactions that involves the relinquishment of ultimate control over the data by the data broker). This would ensure that the mere "access" to data – e.g., in service provider or related party context – would not be inadvertently swept up in the definition.
d. Exception for service providers. The definition of a data broker should expressly state that it does not include other service providers. We recommend defining such service providers as any entity that processes covered data on behalf of, and at the direction of, a business customer that determines the purposes and means for which the data will be processed.

In totality, these changes would help ensure that the definition of "data brokerage" does not unintentionally sweep in a large number of service providers that do not engage in the data broker industry. We outline below a possible alternative definition drawn (in part) from California and Vermont state law definitions of data brokers:

> *"Data broker" means a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship. "Data broker" does not include an entity to the extent it is acting as a service provider and processing covered data on behalf of, and at the direction of, a business customer that determines the purpose and means for which the covered data is processed.*

The definition above is drawn from Vermont[7] and California law.[8] Among other things, GDA's proposed revised definition would align the ANPRM definition more closely with Vermont and California law by: (1) removing the reference to mere "access or similar commercial transactions" (which would have extended the scope of this definition to a wider array of service providers than intended); (2) adding the element of a data sale in exchange for financial consideration; (3) adding the element of an arm's length (unrelated party) transaction, and (4) expressly stating that service providers who process data at the direction of their business customers are not data brokers. Such service providers include Software-as-a-Service companies in engaged in human resources

---

[7] The Vermont Data Broker Law, 9 V.S.A. ch. 62, subch. 5 provides as follows: "A Data Broker is a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship. 9 V.S.A. § 2430(4)(A).
Examples of a direct relationship with a business include if the consumer is a past or present; 9 V.S.A. § 2430(4)(B):

- customer, client, subscriber, user, or registered user of the business's goods or services;
- employee, contractor, or agent of the business;
- investor in the business; or
- donor to the business.

The following activities conducted by a business, and the collection and sale or licensing of brokered personal information incidental to conducting these activities, do not qualify the business as a data broker; 9 V.S.A. § 2430(4)(C):

- developing or maintaining third-party e-commerce or application platforms;
- providing 411 directory assistance or directory information services, including name, address, and telephone number, on behalf of or as a function of a telecommunications carrier;
- providing publicly available information related to a consumer's business or profession; or
- providing publicly available information via real-time or near-real-time alert services for health or safety purposes.

The phrase "sells or licenses" does not include; 9 V.S.A. § 2430(4)(D):

- a one-time or occasional sale of assets of a business as part of a transfer of control of those assets that is not part of the ordinary conduct of the business; or
- a sale or license of data that is merely incidental to the business."

[8] See Cal. Civ. Code § 1798.99.80.

management, customer relations management, accounting, enterprise resource planning, productivity, design (CAD/CAM), BIM, industrial automation, and other digital transformation tools.

4. **Vendor Agreements** – Given the above-referenced concerns regarding legality, feasibility, and unintended consequences of "restricted transactions," it is premature for DoJ to publish draft rules on restricted transactions involving vendor agreements.

   Among other things, GDA is concerned with the broad definition of vendor agreements, which includes any agreement in which "any person provides goods or services to another person in exchange for payment or other consideration, including cloud computing services." It is important to make clear that the service provider in a cloud service agreement (as well as agreements involving IaaS, PaaS or SaaS) is typically legally precluded from accessing, reviewing, or controlling the data of its customers. Accordingly, while such vendors maintain based on a risk management framework cybersecurity and other data security protocols at a systemic level, those vendors do typically not have knowledge of, or control over, the customer data stored on its systems. We urge DoJ to clarify that the responsibilities for compliance with respect to these contents reside with the customer who owns that data. Cloud service agreements will typically have in place requirements that govern the security and handling of that data. Both vendor and customer have a role in compliance, with the customer, in this example, knowing the type of data that they are transferring to the cloud provider.

   Recommendation: GDA respectfully urges DoJ to take more time to develop its approach to "restricted transactions." It is appropriate to allow additional time for proper development of a risk-based approach that addresses actual national security risks associated with such transactions, while also accounting for the legal, civil rights, and feasibility concerns raised by the ANPRM.

   If DoJ does not adopt the recommendation to take additional time before published rules on "restricted transactions," then GDA recommends that DoJ clarify that vendors are responsible for the security of the systems and services that they control, while data owners are responsible for the content of the data that they own, control, and transfer. Clarify that vendors are not responsible or expected to surveil their own customers or to access customer data, particularly given that (in most cases) vendors would lack visibility into such data, would be contractually precluded from accessing or exfiltrating this data, and would be subject to severe penalties for such acts under various legal frameworks, including those relating to cybersecurity, privacy, trade secrets, regulatory data protection, securities law, and contract, tort, or criminal provisions.

   Additionally, GDA recommends that the definition of "vendor agreement" be narrowed to provide greater specificity regarding the types of goods or services being provided.

5. **Employment Agreements –** GDA is concerned that the ANPRM's proposal for ex ante access restrictions to be imposed on foreign employees in countries of concern will effectively render inutile the intra-entity transfer exemption. GDA respectfully submits that DoJ has not demonstrated any clear need to impose – in the broad commercial settings covered by the ANPRM – restrictions akin to "deemed export" limitations that apply to national security and dual use technologies in the export controls context. DoJ has not demonstrated the existence of any national security risk that would necessitate the denial of access via logical and physical access controls for covered data types for all foreign nationals from a country-of-concern. Such a broad presumption that all (for example) Chinese national employees of a US enterprise cannot be trusted and must be denied access to data is not only unjustified, but also raises significant legal concerns from a workplace discrimination (i.e., discrimination based on nationality or race) and from a human rights perspective.

   While GDA understands that DoJ may have an interest in ensuring that employees that will be handling covered personal data are properly vetted prior to their being hired, the proposed safeguards outlined in Section I (e.g., data minimization, data masking, privacy enhancing technologies, access controls, etc.) do not relate to such pre-employment vetting procedures.

For all of the foregoing reasons, GDA does not believe that DoJ has fully evaluated all of the unintended consequences that may result from the treatment of employment agreements as "restricted transactions" as suggested by the ANPRM. Nor does GDA believe that DoJ has properly scoped the types of risks that it seeks to mitigate or the types of remedial measures would effectively mitigate such risks. Simply deeming all employees of a particular nationality (e.g., all Chinese nationals) as a security risk is not a proportionate or reasonable articulation of any risk.

Recommendation: GDA respectfully urges DoJ to take more time to develop its approach to "restricted transactions." It is appropriate to allow additional time for proper development of a risk-based approach that addresses actual national security risks associated with such transactions, while also accounting for the legal, civil rights, and feasibility concerns raised by the ANPRM.

If DoJ does not adopt the recommendation to take additional time before published rules on "restricted transactions," then GDA recommends that DoJ clarify that the intra-entity exemptions cover all employees of a US entity and its affiliates in countries of concern, as well as employees of trusted vendors.

6. **US Legal Concerns:** With respect to US-based activities, GDA is concerned that the DoJ has not fully considered potential implications under the Equal Employment Opportunity Act – particularly to the extent that covered entities include persons located in the United States who are normally resident in a country of concern, or persons who work for US corporate entities owned/controlled by an entity incorporated in a country of concern.

   Recommendation: We urge DoJ to consider and address the following questions. Has DoJ NSD conferred with CRD and the Equal Employment Opportunity Commission (EEOC) to whether the ANPRM would represent an impermissible governmental mandate under the Equal Employment Opportunity Act or other relevant federal or state legislation to discriminate in the workplace vis-à-vis certain groups of persons based on their nationality/race in the absence of a substantiated evidence that the particular individual presents a demonstrable national security risk? If so, will DoJ make the results of that legal research public? If not, can DoJ commit to generate that analysis?

Section E – Countries of Concern

Additional Due Process is Required for the Designation of Countries of Concern: GDA is concerned by the open-ended criteria outlined to determine countries of concern in future – i.e., "long-term pattern or serious instances of conduct…." or "significant risk of exploiting US sensitive personal data or US Government-related data…"

Recommendation: We urge DoJ to develop additional guardrails through an interagency process involving the Departments of Commerce, State, Treasury, and Homeland Security and elements of the intelligence community regarding the substantive and procedural aspects of future designations of countries of concern. The procedural aspects of those designations should also include opportunities for public comment; consultations with Congress; and consultations with relevant agencies. This process should also include opportunities for administration and judicial review of any such designations.

Section F – Covered Persons

1. **US Company Employees and Trusted Vendors Should be Subject to the Intra-Entity Exemption:** GDA is concerned with the highly disruptive effects of any proposal to treat US company employees and trusted vendor employees as "covered persons" based solely on their "country of concern" nationality and residence.

   Recommendation: GDA strongly recommends that the intra-entity exemption be clarified so that all employees of US companies and all trusted vendors of US companies unequivocally benefit from that exemption, regardless of whether those employees are citizens and residents of a country of concern.

2. **Persons Who are Temporarily Located in the United States Should Not Be Treated as Covered Persons:** GDA is also concerned with the serious due diligence challenges associated with determining whether a large range of persons located in the United States may be "covered persons." The definition of "covered person" extends to natural persons who are temporarily traveling in the United States, but who legally reside in a country of concern. To comply with the "bulk threshold" assessment mandates and to determine whether any of the six types of personal data are at issue, the ANPRM would effectively impose a requirement to surveil and track communications between US citizens and these persons in the United States, raising legal questions.[9]

   Recommendation: GDA urges that the "covered person" definition be narrowed to exclude persons who are temporarily located in the United States, even if those persons are otherwise residents of a country of concern.

3. **US Affiliates of Entities Organized in a Country of Concern Should Not Automatically be Treated as Covered Persons:** The definition of "covered person" extends to US affiliates of entities that are legally organized or have a principal place of business (PPB) in a country of concern. Accordingly, large US employers – like Smithfield Foods, Terex, Riot Games, GE Appliances, Ingram Micro, and Motorola – are "covered persons" because they are majority-owned by entities incorporated in a country of concern. To comply with the "bulk threshold" assessment mandates and to determine whether any of the six types of personal data are at issue, the ANPRM will effectively impose a requirement to surveil and track communications between US citizens and these US legal entities (including their US citizen employees). Serious legal issues are presented by a US governmental mandate to surveil and track US citizen-to-US citizen communications simply because one of those US citizens works for a large (or small) US company subject to country-of-concern corporate ownership.

   Recommendation: GDA urges that the definition of "covered entity" not include US affiliates of country-of-concern legal entities pending: (1) resolution of legal questions regarding government mandated surveillance of US citizens; and (2) the development of a more nuanced approach to identifying US domestic data transfer transactions that present national security risk, based on substantiated case studies.

4. **International Legal Concerns:** Obligation to seek nationality- or other personal information from counterparty enterprises regarding their employees.

   Recommendation: GDA urges DoJ to consider and provide information on the extent to which these government mandates could create unintended foreign law compliance risk (e.g., in the European Union or other countries with similar privacy laws) for US enterprises that are engaged in good faith efforts to meet DoJ's regulatory requirements.

[9] See discussion infra at Section **. See also related recommendations to: (1) raise the "bulk threshold" limits so that they are only implicated by the largest data transfer scenarios; and (2) to suspend consideration of the "restricted transaction" category pending further analysis).

Section G – Prohibitions

1. Prohibitions with respect to "Data Brokerage." Please see comments in Section D above.

2. Definition of "Directing": The ANPRM includes a definition of "directing" to mean "that a US person has the authority (individually or as part of a group) to make decisions on behalf of a foreign entity, and exercises that authority to order, decide, or approve a transaction that would be prohibited under these regulations if engaged in by a US person." We believe this definition is overly broad and could result in unintended consequences that don't further the goal of securing US persons' data. US-based service providers should retain the ability to transparently sell their services as part of an arm's length transaction through a reseller or other entity that is a covered person to end customers who are also covered persons – especially where the US service provider doesn't know or expect their services to be used as part of a covered data transaction. Under global data protection laws and regulations, US-based service providers have limited ability to proactively monitor or limit their customers' use of the services. However, US-based service providers do generally retain broader contractual rights with resellers or other entities that allow them to stop providing the services through those entities. For example, a US-based service provider may decide to no longer provide a certain service to its customers globally, to no longer sell any services in a particular market at all, or no longer wants the reseller or other entity to sell to a specific customer (e.g., in the event there are documented complaints of that customer using the services to violate the law) – it should have the ability to make that determination.

   Recommendation: Clarify that such scenarios involving US-based service providers would not constitute "directing" under these rules.

Section H – Exempt Transactions

GDA recommends that DoJ make the following revisions to Section H on Exempt Transactions:

1. Clarify that the intra-entity exemption applies to all employees in a country-of-concern, as well as "trusted vendors" and their employees.

2. Clarify that the intra-entity exemption encompasses data transfers made over systems that the company has contracted to store or process certain company data (e.g., accounting, ICT, or human resource services that contain the company's data and that the company has contracted for).

3. Clarify that the intra-entity exemption relates to data transactions that are "ordinarily incident to and part of administrative or ancillary business operations." (The use of the term "ancillary" may be construed as narrower than intended. The activities listed in the ANPRM's discussion of the exemption are all part of a business' normal administrative functions and should be clearly exempted under the proposed rules. If a company cannot engage in human resources, accounting, data and word processing, or other typical administrative activities, then the business cannot function).

4. We welcome the clarification that passenger manifest data and other data transferred per an international agreement is exempt. However, there are a large number of relevant agreements. All such agreements should be specified. Clarify that the exemption for international agreements covers the following:

   a. "Data transfers that are incident to an international agreement recognized or signed by the United States. A non-exhaustive list of those agreements will be set forth in an Annex to the NPRM";
   b. "Data transfers conducted in support of activities relating to international standards-setting and/or in support of listed international standards development organizations. Relevant standards and standards-development organizations will be set forth in an Annex to the NPRM";

c. "Data transfers that are conducted in support of, or incidental to the activities of, any inter-governmental organization; any international private sector organization in which US entities [actively] participate; or any international labor organization in which US labor unions [actively] participate. A list of those organizations will be set forth in an Annex to the NPRM."

5. Clarify that exclusions for personal communications and informational materials under IEEPA cover emails, voicemails, and similar communications in any medium, as well as books, music, film, software, and other published content in any medium.

6. Add an exemption for purposes of regulatory compliance that applies to all US laws and statutes with US persons are required to comply – not simply those relating to financial services and payment processing. In other words, a separate "regulatory compliance" exemption should be broken out from the financial services exemption.

7. Add exemptions to make clear that:

   a. "'Bulk US sensitive personal data' does not include non-personal data, including machine-to-machine data."
   b. "'Bulk US sensitive personal information' does not include public record or publicly available data."

8. Add an exemption for health-related data transactions that do not raise national security concerns. The GDA would like to work with the Department to draft that exemption language.

9. Further refine the scope of the exemption for financial-services, payment processing and regulatory compliance-related transactions to take into account the nature of how financial and payment services work. It should be clarified that it also encompasses services that are subordinate and ancillary to processing payments and funds transfers that are critical to the safety, resiliency, and security of transactions in the financial and payment ecosystem. Such operations involve payment dispute resolution, payor authentication, tokenization, payment gateway, payment fraud detection, payment resiliency, mitigation and prevention, and payment-related loyalty point program administration.

   We therefore suggest that the scope of this exemption be further refined. To that end, we would suggest including such clarifications to the following points (suggested revisions in ***Bold & Italics***):

   (i) Banking, capital-markets, or financial insurance services;

   (ii) An activity authorized ***for national banks*** *by 12 U.S.C. 24 (Seventh) and rules and regulations* ***and written interpretations of the Office of the Comptroller of the Currency*** *thereunder;*

   (iii) An activity that is ''financial in nature or incidental to a financial activity'' or ''complementary to a financial activity,'' as set forth in section 4(k) of the Bank Holding Company Act of 1956 and rules and regulations ***and written interpretations of the Board of Governors of the Federal Reserve System*** *thereunder;*

   (iv) The provision or processing of payments involving the transfer of personal financial data or covered personal identifiers for the purchase and sale of goods and services (such as the purchase, sale, or transfer of consumer products and services through online shopping or e-commerce marketplaces); ***the provision or processing of funds transfers (such as person-to-person, business-to-person and government-to-person funds transfers) involving the transfer of personal financial data or covered personal identifiers; the provision of services ancillary to processing payments and funds transfers (such as services for payment dispute resolution, payor authentication, tokenization, payment gateway, payment fraud detection, payment resiliency, mitigation and prevention, and payment-related loyalty point program administration);*** *other than data transactions that involve data brokerage; and*

10. As DoJ is considering with Financial Services, it should clarify that all data necessary and incidental to the provision and delivery of communications services remain outside the scope of any restrictions on personal sensitive data for consumers, enterprises and government, including, but not limited to, international calling, mobile voice, and data roaming. This will include any sensitive personal data provided by the consumer, enterprise, or government while using those services. Furthermore, communications and broadband service providers should be able to use, disclose, or permit access to customer proprietary network information obtained from its customers, either directly or indirectly through its agents to initiate, render, bill, and collect for communications services. Ensuring that communications services are enabled is a long-held policy of the United States, most recently affirmed in relation to Russia by the U.S. Treasury Department, Office of Foreign Assets Control General 25C - Authorizing Transactions Related to Telecommunications and Certain Internet-Based Communications.[10]

Section I – Security Requirements for Restricted Transactions

Section I contains the security requirements for restricted transactions that, if undertaken would allow for an otherwise prohibited transaction. This approach may not provide sufficient flexibility based on risk, but instead provide a checklist of requirements that may or may not be an appropriate way to manage the risk of any specific transaction.

Further, we note that the EO states "these requirements shall be based on the Cybersecurity and Privacy Frameworks developed by the National Institute of Standards and Technology" but the ANPRM contemplates expanding that foundation to "existing performance goals, guidance, practices, and controls, such as the Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Performance Goals (CPG), National Institute of Standards & Technology (NIST) Cybersecurity Framework (CSF), NIST Privacy Framework (PF), and NIST SP 800–171 rev. 3 (''Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations''). Adding additional foundations for these security requirements exceeds the scope of these norms and may not be consistent with risk-based approach.

Security requirements would be ill-suited as a one-size-fits-all approach to data security. Given the breadth of business models that would be captured under the DOJ's proposed rules, it is critical that data security requirements are risk-based, proportionate, outcome-focused, and can be adapted to a business's specific context. We note, for example, that "tokenization," one technique specifically listed in the ANPRM, may not be suitable and effective to improve security in some contexts, but may be completely unworkable in others.

Generally speaking, the aforementioned NIST and CISA legal authorities are risk management frameworks, yet – as we read the ANPRM – we are concerned that the intention may be to mandate across-the-board implementation of many of these controls regardless of risk profile.

[10] The United States generally supports the free flow of information globally as facilitated by telecommunications and certain internet-based communications. Accordingly, GL 25C authorizes — with certain exceptions and exclusions — (i) all transactions ordinarily incident and necessary to the receipt or transmission of telecommunications involving the Russian Federation that are prohibited by the Russian Harmful Foreign Activities Sanctions Regulations, 31 CFR part 587 (RuHSR) and (ii) the exportation or reexportation, sale, or supply from the United States or by U.S. persons, wherever located, to the Russian Federation of services, software, hardware, or technology that are incident to the exchange of communications over the internet and that are prohibited by the RuHSR (see FAQ 1040).

Thus, we urge the DoJ and DHS to respect and maintain the risk management focus of these legal authorities. In selecting specific data security frameworks, standards, or practices, we also encourage DoJ and DHS to allow for flexibility and to consider other respected standards, including, ISO 27001, ISO 27017, ISO 27018, and the SOC-2 Trust Principles (security, confidentiality, availability, privacy, and processing integrity). These examples are widely adopted in the marketplace and offer support for independent assessments or certifications. Using existing frameworks, standards, and practices would avoid unintended commercial disruptions and reduce burdens on regulated entities. The DoJ and DHS may also wish to learn from or otherwise leverage established international transfer mechanisms, such as the Cross-Border Privacy Rules System and the US-EU Data Privacy Framework.

Recommendation: Beyond baseline organizational cybersecurity posture – companies should be expected to exercise reasonable care in determining their own risk profiles and in implementing appropriate risk management and risk mitigation practices.

Section J – Licenses

The GDA believes that extensive and close consultation with the private sector is critical to establish an effective licensing and compliance framework. We urge the DoJ to take the time to develop this framework over time and suggest that it consider the adoption of pilot programs, subsequent Federal Register requests for comments, and a staged approach to implementation that allows for a reasoned, informed, and nuanced approach to effective compliance.

Furthermore, as a general matter, we observed that, while a licensing framework based on the Commerce/BIS and Treasury/OFAC process may be reasonable for "prohibited transactions" or "US government-related data transactions," such an approach may be neither reasonable nor effective in the case of "restricted transactions." Licenses should not be required in any scenario involving "restricted transactions," where a "reasonable care" standard would be more suitable. GDA is prepared to work closely with DoJ and DHS to explore how other agencies – including the US Customs & Border Protection, the Department of the Interior, the Securities and Exchange Commission, and/or the Federal Trade Commission – have developed different legal compliance frameworks that have met with varying degrees of success and effectiveness.

Recommendation: Take the time to develop this framework over time via staged approach that allows for a reasoned, informed, and nuanced approach to effective compliance. Distinguish between circumstances suitable to licensing (in the case of prohibited data broker transactions) vs. self-assessment, risk management, and informed compliance programs built on a standard of reasonable care (in the case of restricted transactions).

Section K – Interpretative Guidance

GDA notes that an advisory opinion process will be useful, because it can: (1) help all US companies better understand their rights, responsibilities, and potential consequences of their actions under the regulations; (2) help companies ensure that they are in compliance with the law when they seek and secure such advisory opinions; and (3) promote compliance given that resolution of legal questions through an advisory opinion process will be more timely, efficient, and cost-effective for both the DoJ and US companies as compared to litigation.

Recommendation: Develop a robust advisory opinion process; ensure that these opinions are published; and also, all advisory opinions should be published.

Section L – Compliance and Enforcement

The GDA urges the DoJ to take additional time to develop a proper compliance and enforcement framework. This would include:

- Due Process Safeguards / Rights of Appeal: Building in additional due process safeguards, including right to secure administrative reconsideration/appeal, as well as judicial appeal rights;
- Compliance and Enforcement Guidelines: Request the adoption of specific guidelines on the calculation of administrative fees and all the elements considered to calculate the fines. This could be a framework along the lines of five-step methodology considered by the European Data Protection Board in their guidelines on the calculation of administrative fees under GDPR: taking into account the number of instances of sanctionable conduct, possibly resulting in multiple infringements; the starting point for the calculation of the fine; aggravating or mitigating factors; legal maximums of fines; and the requirements of effectiveness, dissuasiveness and proportionality. Examples of practical application do not hurt.
- FAQs, Informed Compliance Manuals, and Sector-by-Sector Guides: Because the ANPRM has such wide applicability across numerous sectors, the proposed framework could produce unintended and unforeseen consequences in different sectors. We urge the DoJ to begin mapping out a process to develop sector-by-sector FAQs and guides to help promote informed compliance, better self-assessments, and better data security outcomes. FAQs for sectors including the automotive, aerospace, consumer products, finance/insurance, hospitality, biopharmaceutical, healthcare delivery, medical technology, ICT services, telecom services, and so forth.[11]

Safe Harbors and Indemnification: In addition to the Exemptions outlined above, we urge the DoJ to consider the following safe harbors and indemnification provisions.

- Safe Harbor & Indemnification for Breaches of US Law Resulting from Efforts to Comply with the US Data Security Rules: Provide that a person shall be not be held liable under any federal or state law, and shall be indemnified by the US government for any claims made against it under any such law as a result of that person's good faith efforts to comply with the requirements of these regulations.
- Indemnification for Breaches of Foreign Laws Resulting from Efforts to Comply with the US Data Security Rules: Provide that a person shall be indemnified by the US government for any claims made against it under any foreign law as a result of that person's good faith efforts to comply with the requirements of these regulations.
- Safe Harbor for data outside a person's control: Provide that a person is exempted from any requirement that otherwise apply to that person in respect of 'bulk sensitive US personal data' over which that person lacks access, control, and a legal authority.
- Safe Harbor for the processing of US person data that's incidental to a company operating their business in a country of concern.
- Safe harbor that allows multinational companies to operate in CoCs, where absent actual knowledge or gross negligence, they will not be in violation of law simply because they receive U.S. persons data incidentally in the course of their ordinary business operations.[12]

[11] For example, if an enterprise (a controller) collects information on a person's meal preferences or accessibility needs or the geolocation data of a conveyance, and some of that data is stored in a conveyance transiting a country of concern, how would that be treated? This is just one of many examples that might be implicated by the framework that should be considered, evaluated, and addressed prior to any enforcement action being taken.

[12] US-based enterprises have an interest in operating in and selling their services to multinational companies who operate in countries of concern (where otherwise permitted by US law). Due to existing security and data governance concerns,

Section M – Coordination with Other Regulatory Regimes

We appreciate the DoJ's analysis of the relationship between the ANPRM's proposed legal framework and legal reviews conducted by the US Committee on Foreign Investment in the United States (CFIUS).

Nevertheless, we believe that the ANPRM does not discuss numerous cross-cutting systemic legal interoperability concerns that are raised by the ANPRM's proposals in relation to "restricted transactions." In that regard, we ask that DoJ address broader industry concerns relating to ensuring coherence across numerous national security and data-focused legal regimes. With respect to "restricted transactions," we also ask that DoJ provide a detailed explanation as to how it proposes to deconflict measures ANPRM requirements vis-à-vis US sanctions and export control requirements that cover many of the same predicate activity.

Recommendations: We offer the following specific recommendations.

1. Fully Assess Privacy, Civil Rights, and Human Rights Implications of the Proposed "Restricted Transaction" Categories: Implementation of the "restricted transaction" categories would appear, in some cases, require private companies to surveil and monitor the content of digital transmissions within the United States between a US citizen and a person of a country of concern (and in some cases, US digital transmissions between two or more US citizens). DoJ should fully assess and eliminate this unacceptable risk from its proposal before publishing any rules on "restricted transactions." and determine clear approaches to mitigate DoJ should develop and publicize legal analyses (including the DoJ Civil Rights Division (CRD), DoJ Office of Legal Policy (OLP), and the DoJ Criminal Division) to assess the legality of mandating that the private enterprises monitor the communications of private US citizens in the United States in ways that would arguably be illegal for the US government to do. DoJ should also secure and publish legal analyses regarding these human rights and privacy concerns from the Offices of General Counsel of the Department of Treasury (Treasury), the Department of Health & Human Services (HHS), and the Federal Trade Commission (FTC), the Department of Commerce (Commerce), and the Department of State (State). For purposes of questions (d)(i) and (d)(ii) above, the analysis should address requirements under the US Constitution and federal law (Computer Fraud & Abuse Act (CCFA), Graham-Leach-Bliley Act (GLB), Children's Online Privacy Protection Act (COPPA), Health Insurance Portability and Accountability Act (HIPAA), the Defend Trade Secrets Act (DTSA), and the Stored Communications Act (SCA). This is not a comprehensive list of relevant laws. We ask DoJ to undertake a full assessment of potential legal impacts.

2. Fully Assess Other Legal Implications of the Proposed "Restricted Transaction" Categories: Under the "restricted transaction" category, the DoJ's proposes to require private enterprises to monitor, surveil, and/or access proprietary, trade secret, or other protected content in order to determine whether the six sensitive data types are contained therein, and in order to determine whether the bulk thresholds have been satisfied also raises significant legal concerns under other US laws, including laws relating to trade secrets, regulatory data protection, antitrust, unfair competition, contracts and torts. DoJ should develop and publicize legal analyses (including the DoJ Antitrust Division (ATR), the FTC, the US Patent & Trademark Office, HHS, the Food & Drug

---

multinational companies often utilize CoC-specific instances of technology services that are intended to process the data of their Chinese customers. In such scenarios, data on their U.S. and other global customers is generally processed in a completely separate non-CoC, global instance. However, it's difficult to completely prevent any U.S. person data from ending up in a CoC-specific instance. For example, a CoC-specific instance may include sensitive personal data of:

- US person employees who are system administrators and whose data is needed by the CoC-specific instance for them to manage the service;
- US persons who are expats or tourists in a CoC;
- US persons originally from a CoC or who speak a CoC language who may browse the company's website in their native language and provide their data on that website without realizing it will be stored in a CoC-specific instance.)

Administration (FDA), the Securities Exchange Commission (SEC), and others) to determine the legality of any governmental mandates for unauthorized non-personal data access and review.

Section N – Economic Impact

We appreciate DoJ's recognition that the ANPRM would involve an economically significant rule. We plan to provide detailed economic analysis at the NPRM stage of the process.