GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

JULY 2024

GDA SUPPLEMENTAL RESPONSE TO JUSTICE DEP'T 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

Following up on the comments submitted on April 19, 2024,[1] the Global Data Alliance (GDA)[2] appreciates the opportunity to provide these supplemental comments to US Department of Justice (DoJ) and other agencies in connection with 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]

This supplemental submission does not supplant the various concerns raised in our April 19 comments. However, we broadly understand that DoJ is attempting to address several of those other concerns, as discussed in the endnotes hereto.[4]

This July 2024 submission seeks to address three questions that have arisen in the course of our ongoing discussions:

1. How the current "bulk threshold" design may increase data security and national security risks, and what a safer and more secure scoping framework would be.
2. The definitional scope of "data broker" and "data brokerage."
3. The treatment of genomic data and personal health data.

GDA supports DoJ's planned publication in August 2024 of a Notice of Proposed Rulemaking, subject to the resolution of the issues raised herein.

PROGRAM SCOPE / BULK THRESHOLDS

The GDA continues to have serious concerns regarding the civil rights, cyber, privacy, security, and other legal implications of an approach that could require companies to tally up data types and volumes by *inter alia* decrypting private citizen and other electronic transmissions, engaging in unauthorized access to data in their custody that they are not legally permitted to access, and creating large pools of Americans' most sensitive personal data for data analytics purposes. It is inadvisable to require thousands or millions of American companies to engage in such high-risk activities – many of which may breach existing US privacy, trade secret, or other data security laws – simply to determine whether quantitative "bulk thresholds" are met. These thresholds, which resemble similar quantitative thresholds in China's data control system, are decidedly not privacy- or cybersecurity-protective, and risk making US sensitive personal data less – not more – secure.

We urge DoJ to consider the following (safer and more secure) scoping framework:

1. Require US companies – based on publicly or readily available information about their level of commercial interactions in countries of concern – 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.
2. Convert the "bulk thresholds" 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.

DEFINITION OF DATA BROKERAGE

The GDA would be very concerned with any definition of "data broker" or "data brokerage" that is intended to sweep up companies that are not, in fact, data brokers. This concern is made more acute by the stringent licensing requirements and the risk of severe (criminal and other) sanctions that apply to prohibited data brokerage transfers.

An overbroad definition that seeks to classify non-data brokers as "data brokers" risks creating confusion, legal uncertainty, and unintended consequences. We strongly recommend that you adopt a definition based in current law, such as the GDA suggested definition, or the definition found in Vermont law.[5]

Reliance on accepted and well-understood legal frameworks will give the government and stakeholders greater transparency regarding the entities that are subject to the data broker prohibitions under the NPRM.[6] For example, Vermont maintains a public registry of covered entities, thus easing administrability and enforcement (for the government), as well as transparency and compliance for companies and individuals – whether they are classified as data brokers or not.

TREATMENT OF GENOMIC DATA AND PERSONAL HEALTH 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, as well as for meeting regulatory requirements to authorize conducting 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. These data may also be transferred in connection with healthcare services or insurance services provided to US patients and US persons receiving treatment outside the United States, including in countries of concern.

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.[7]

The consequences of failing to recognize these various fact patterns are significant, as discussed in our April 2024 submission. Accordingly, we urge DoJ to establish a clear exemption for health data transactions in these contexts. Below is a draft of such an exemption to be included in the NPRM.

Draft Exemption Covering
Transfers of Health-Related Data for Safeguarding Public Health and Regulatory Compliance

Transfers of health-related data to safeguard public health and regulatory compliance. The NPRM exempts any transaction that is ordinarily incident to and part of: (1) pandemic preparedness and response; (2) the provision of healthcare services, including diagnosis, treatment, surgery, and patient monitoring, as well as the provision of life, health and related insurance services; (3) health R&D, including for purposes of meeting regulatory requirements to demonstrate the safety and efficacy of diagnostics, biopharmaceutical treatments, and medical devices and technologies, including through the conduct of clinical trials and to obtain authorization to conduct clinical trials; and (4)) post-marketing surveillance of safety and efficacy of health products, including for purposes of meeting adverse event regulatory reporting requirements and pharmacovigilance standards.

Health data transfers that are exempted to the extent that they are ordinarily incident to and part of the conduct of the foregoing activities include but may not be limited to:

- Transfers of personal health and genomic data between a US company and its foreign subsidiary for the conduct of business activities.
- 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.
- Anonymized, pseudo-anonymized, and otherwise deidentified personal health and genomic data that is not personally identifiable on its own.
- Legal compliance with any US or foreign laws or regulations that require the submission of data for purposes of: (1) pandemic preparedness and response; (2) the provision of healthcare or health insurance services; (3) meeting regulatory requirements to demonstrate the safety and efficacy of diagnostics, biopharmaceutical treatments, and medical devices and technologies; and (4)) post-marketing surveillance of safety and efficacy of health products, including for purposes of meeting adverse event regulatory reporting requirements and pharmacovigilance standards post-marketing surveillance of safety and efficacy.
- Legal compliance with the following federal laws and regulations, including the Food Drug & Cosmetics Act; the Drug Price Competition and Patent Term Restoration Act of 1984; the Biologics Price Competition and Innovation Act or any notes, guidance, orders, directives, or additional regulations related thereto.

The Department of Justice will consult the Department of Health & Human Services, the Food & Drug Administration, and other relevant agencies in interpreting and applying this exemption, including through guidance, or advisory opinions.

[1] *See* Global Data Alliance, *Response to DOJ Advance Notice of Proposed Rulemaking* (April 19, 2024), https://globaldataalliance.org/wp-content/uploads/2024/04/04192024gdaussensdata.pdf

[2] 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

[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

[4] For example, we urge DoJ to seek to duly account for the different roles and responsibilities of controllers and processors to avoid inadvertently mandating breach of access limitations or confidentiality obligations found in contract or federal/state law. We also urge DoJ to recognize, in principle, that the intra-entity exemption should apply to an affiliated entity's employees (and potentially trusted contractors) that have been duly vetted in the onboarding process, regardless of those persons' nationalities. We also urge DoJ to consider establishing an exemption for data that is necessary and incidental to the provision and delivery of communications services. We also urge DoJ to establish clarifying exemptions for machine-to-machine data transmissions, and to exempt geolocation data that is not clearly connected to sensitive personal data. For these and other issues, please see our April 2024 submission.

[5] GDA suggested definition:

"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.

Vermont definition:

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."

[6] *See e.g.,* Vermont Registry - Corporations Division (https://bizfilings.vermont.gov/online/DatabrokerInquire/?isStartUpAction=False).

[7] 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.