GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

Response to OSTP Request for Information on Regulatory Reform and Artificial Intelligence
Docket ID: OSTP–TECH–2025–0067

The Global Data Alliance (GDA)[1] respectfully submits these comments in response to the Office of Science and Technology Policy's (OSTP) Request for Information on Regulatory Reform and Artificial Intelligence (AI). GDA is a cross-industry coalition of companies committed to the secure and responsible movement of data, which is critical to innovation and job growth in the United States.

Given the essential role in AI development of continuing cross-border access to knowledge, information, and data, the GDA's submission identifies regulatory and policy challenges—including foreign localization mandates, legal ambiguities in data security programs, and improper state-level cross-border barriers—that risk undermining US access to data and US leadership in AI. Finally, the submission outlines a positive AI and cross-border data agenda to sustain US national and economic security into the future.

I. Cross-Border Data Transfers as the Foundation of US AI Leadership

The US AI ecosystem is inherently global. Every major AI breakthrough depends not only on domestic innovation but also on real-time access to know-how, data, and information from around the world. Without the ability to seamlessly participate in transnational digital networks and the broader AI development ecosystem, the United States risks losing its AI development edge.

It is widely understood that cross-border data transfers are integral to the effective deployment of AI solutions to enhance economic growth, help advance scientific progress, promote cutting-edge R&D, protect networks and information systems, and solve pressing national challenges. Science- and innovation-oriented organizations consistently emphasize that computational analytic capabilities depend on data drawn from globally distributed sources.

[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 transfer of data around the world to innovate and create jobs.
The GDA promotes sensible cross-border data policies that support innovation, science, security, and economic opportunity. *See* https://globaldataalliance.org/

From developing predictive models to deploying AI-based systems, these systems are “trained” by ingesting large, heterogeneous data sets that reveal latent patterns, relationships, and trends. These models then generate predictions when new data are introduced. Because training data frequently originate from geographically dispersed sources, it is imperative to ensure that data can move seamlessly and securely across borders.

The United States cannot realize AI’s full potential if it is isolated from trusted international data inputs. Policies must preserve open, secure, and interoperable frameworks that allow AI systems to learn from global experience.

II. Illustrative Use Cases for AI and Cross-Border Data

We offer below illustrative use cases for AI in several sectoral contexts in which GDA members are active.

A. AI-Grounded Healthcare, Medical Technology, and Biopharmaceutical R&D

AI is transforming innovation across therapeutics, diagnostics, devices, imaging, and monitoring systems. These AI systems depend on access to diverse datasets from around the world—genomic databases, imaging archives, clinical trial outcomes, sensor data from devices, diagnostic assay results, population health studies, and phenotypic registries.

- Diagnostic imaging, surgical video and algorithmic interpretation: AI models built from imaging datasets (MRI, CT, PET, X-ray) and surgical video drawn from multiple countries improve generalizability and training, reduce error rates, and adapt to diverse patient populations.

- Device calibration and optimization: Smart devices, wearables, and implantables generate streams of sensor data. AI models refined with global datasets improve accuracy across different physiological and environmental conditions.

- Assay and diagnostic development: AI models trained on biomarker, proteomic, and genomic data sourced internationally detect early disease signatures with greater robustness.

- In silico trials and simulations: AI-based modeling of drug-device interactions or device performance is strengthened by integrating global performance datasets.

- Real-world evidence and regulatory readiness: AI-driven analysis of international registries and post-market device data improves regulatory submissions and post-market safety monitoring.

Restricting cross-border flows—through localization mandates, vague data export rules, or restrictive transfer regimes—directly constrains AI innovation, slows time to market, degrades accuracy, and risks introducing unintended error or outcomes into AI-driven solutions.

B. AI and Agriculture & Environmental Predictive Systems

AI models in environmental science and agricultural planning rely on integrating global geospatial, remote sensing, weather, soil, hydrological, and satellite datasets.

- Climate and extreme event forecasting: Global satellite and atmospheric data improve predictive accuracy for droughts, floods, and heat waves.
- Precision agriculture: AI integrates soil, crop, and climate data from multiple regions to optimize farming practices and resource use.
- Pest and disease monitoring: AI trained on global datasets enables early detection of outbreaks and rapid cross-border response.
- Carbon and ecosystem modeling: AI integrates international land and forestry data to improve carbon accounting and inform climate policy.
- Cross-regional learning: AI trained on data from one agroecological zone can suggest adaptive innovations in another.

Without open global flows, models become parochial, less accurate, and less resilient.

C. AI and Financial- and Cyber-security

Cyberattacks and fraudulent financial activity are inherently transnational. AI-driven cybersecurity tools are necessary to meet this challenge, but such tools are only as effective as the global data available to train them.

- Threat intelligence: Malicious actors reuse infrastructure globally. AI trained on attack patterns abroad can recognize emerging variants before they reach the U.S.
- Fraud detection: AI that integrates diverse international transaction data detects anomalies more effectively than models trained on domestic-only inputs.
- Critical infrastructure defense: Energy, telecom, and financial networks require AI-powered cybersecurity tools that are informed by global threat data.

- Supply chain security: AI detection of anomalous behavior in software or hardware requires global inputs.

Cybersecurity is global by necessity. Restrictions on cross-border data flows undermine resilience, hurt national security, and weaken AI-enabled protection.

D. AI and International Trade and Customs Clearance

The United States needs a wider range of logistics options to improve the efficiency of international supply chains to enhance the economic competitiveness of US importers and exporters. In this cross-border data policy area, the private sector is developing new AI-based technologies that have the promise to transform the cross-border trade process.

- There is room for greater administrative efficiency and streamlining in respect of US Customs and Border Protection's (CBP) treatment of "customs business." The current regulatory approach stifles consumer choice increases costs throughout the supply chain, and artificially impedes the flow of goods across borders. For example, the deployment of technological solutions by non-broker logistics providers such as AI/ML and Optical Character Recognition (OCR) – areas ripe for innovation of this kind – is hamstrung by these restrictions.
- The Government needs to create a new regulatory framework which allows wide application of AI tools in the cross-border data-dependent customs clearance process. For example, AI would be particularly useful in assigning harmonized tariff system (HTS) codes to products to facilitate the collection of tariffs on the full range of goods, an essentially manual process currently performed by a broker. Drawing on cross-border data sources, AI could also assist the risk assessment process and allow for the more rapid release of goods before their arrival in the United States. Moreover, AI could also allow for "brokerless" entries of low value shipments.
- Wider use of AI would improve the economic competitiveness of US companies in this cross-border data-intensive area, while accelerating US leadership in innovative logistics processes.

III. Regulatory & Policy Barriers to Cross-Border AI

A. Foreign Data Localization and Transfer Restrictions

Because we understand that the OSTP's solicitation is focused on regulatory barriers in the United States, we do not dedicate significant attention to foreign data localization mandates or improper data transfer restrictions. Suffice to say that such cross-border data barriers are prevalent and increasing rapidly (by over 500% in the Asia-Pacific alone in just the last few years). Such restrictions have a direct impact on US-based AI development and innovation, because they fragment networks, reduce dataset diversity, inhibit the flow of cyber threat data, and increase the risk of error or other unintended outcomes. As discussed below, a robust US engagement agenda with trading partners to remove such barriers is critical to the future health and resilience of AI development in the United States.

B. US Data Security Programs – Focusing National Security Objectives Without Unnecessarily Harming US AI Leadership

The Global Data Alliance strongly supports the national security objectives underlying both the DOJ's Data Security Program (28 C.F.R. Part 202) and the Federal Trade Commission's Protecting Americans' Data from Foreign Adversaries Act (PADFAA). Protecting U.S. national security is a core prerogative of the federal government, and focused restrictions help prevent adversarial exploitation of US sensitive personal data and technology.

However, overreach risks undermining US AI leadership and – therefore – US national security. US AI leadership relies to a significant degree on responsible cooperation and collaboration with allies. If regulatory restrictions are interpreted too aggressively, they may inadvertently chill legitimate and beneficial data transfers with trusted partners.

For example, under the broad scope of 20 CFR § 202.211, U.S. data transfers could be restricted to a Canadian person working in Toronto for a Canadian company that is a contractor to another Canadian company—if there is some degree of ownership, as little as 25 percent, by a country-of-concern entity further up the corporate chain. Such policies may sweep in allied partners in unintended ways, with the unfortunate consequence of isolating the United States from its closest allies in AI development.

US national security must never be compromised, but regulations should not impose restrictions for their own sake. Instead, such regulations should be designed in the most effective manner to achieve their objectives—consistent with Executive Order 12866 and associated administrative legal requirements, which require agencies to:

- Design regulations considering innovation incentives, predictability, flexibility, costs, and equity.
- Assess costs and benefits and adopt regulations only upon a reasoned determination that benefits justify costs.

- Base decisions on the best reasonably obtainable scientific, technical, and economic information.

In this regard, the Bureau of Industry and Security (BIS) mission statement offers a model for balance. That statement underscores that protecting US security includes not only supporting national defense but also ensuring the health of the US economy and the competitiveness of US industry. BIS explicitly commits to avoiding “unreasonable restrictions on legitimate international commercial activity that is necessary for the health of U.S. industry,” recognizing that actions which compromise competitiveness without appreciable national security benefit should be avoided.

Applying this approach to AI-related data security programs would:

1. Focus enforcement against adversarial exploitation, not trusted allied collaboration.
2. Provide clarity, safe harbors, and exemptions for transfers with close allies.
3. Promote consistency and predictability for regulated entities.
4. Avoid chilling innovation or undermining US competitiveness.

Done correctly, this balance will strengthen both US national security and AI leadership.

C. State-Level Fragmentation & Localization Threats

Proposals at the state level to mandate local data storage threaten fragmentation of US digital policy in unexpected ways. One example of such a measure was (now withdrawn) Illinois HB 3574, which would have required certain data handled by state agencies to be stored within the State of Illinois or the United States. Likewise, Texas SB 1188, effective September 1, 2025, requires that certain health records be stored locally.

Such mandates, if replicated, would fragment US networks, undermine interstate and foreign commerce, and set a damaging precedent for global data restrictions that could undermine US AI innovation. Such state actions should be discouraged, given that less restrictive approaches—such as improved cybersecurity, encryption, and other industry best practices—are available to achieve legitimate cyber- and data security policy objectives without mandating localization.

These two illustrative state-level measures highlight the broader challenge of fragmented and variant regulation across 50 US states in an area – such as AI – where a single coherent and consistent national policy is critical to our long-term success.

IV. A Positive, Forward-Looking U.S. Agenda

We urge the OSTP – and other White House components and federal agencies – to build a strong, positive AI policy agenda that includes pillars focused on removing cross-border data barriers, while advancing a forward-looking agenda with partners. This includes:

1. Regulatory Sandboxes: Federal agencies should expand the use of regulatory sandboxes and pilot programs to enable real-world testing of AI tools in partnership with the private sector, academia, and civil society, including in an international context that relies on cross-border data transfers. Such frameworks can allow innovators to demonstrate compliance with core safeguards—such as privacy, security, and accountability—while identifying where existing regulations unintentionally constrain responsible cross-border data use. Well-designed sandboxes can also improve cross-border data access and exchange, by strengthening international regulatory interoperability by aligning U.S. innovation practices with those of trusted allies and partners.

2. Technology Partnership Agreements: To include strong safeguards against localization mandates and unjustified transfer restrictions, while promoting regulatory interoperability.

3. Multilateral Norm-Setting: Lead in bilateral or regional negotiations with allies to advance AI norms that recognize the critical role of cross-border data to AI development.

4. Allied Trusted Data Corridors: Where allied economies have erected improper or questionable data barriers that impede secure AI developments, negotiate to establish interoperable frameworks for cross-border flows in health, finance, climate, and security sectors.

5. Monitoring & Coordination: Establish an interagency team to monitor and address unnecessary and improper proposals to restrict data transfers, whether at the US state or local level or by international partners.

V. Conclusion & Recommendations

Cross-border data flows are essential to US AI leadership across all sectors of the US economy. Recognizing their importance can help ensure that US domestic and international policymakers advance cross-border data policies optimized to promote AI that US cyber, economic, health, safety, and national security objectives.

Respectfully submitted,

Joseph Whitlock
Executive Director
Global Data Alliance