

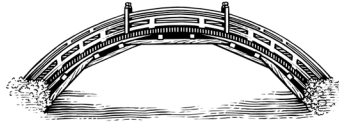
ESSAY SERIES ≈ TRADE POLICY

ADVANCE RELEASE

Page numbering is provisional

The Case for U.S. Leadership on Global Data Governance

Nigel Cory and Akanksha Sinha



NIGEL CORY is a Director at Crowell Global Advisors (United States), where he focuses on cross-border data flows, data governance, digital technologies, and how they each relate to digital trade and the governance of technology. He is also a Nonresident Fellow at the National Bureau of Asian Research. He can be reached at <ncory@crowellglobaladvisors.com>.

AKANKSHA SINHA is a Senior Consultant at Crowell Global Advisors (Singapore). She has expertise in digital economy, emerging technology, and international trade, especially as they pertain to the Asia-Pacific. She can be reached at <asinha@crowellglobaladvisors.com>.

NOTE: This is the second in a series of four essays in 2025–26 on trade policy made possible by the generous support of the Hinrich Foundation ≈ <https://www.hinrichfoundation.com>.

KEYWORDS: DATA GOVERNANCE; DATA POLICY; DATA FREE FLOW WITH TRUST; GLOBAL CROSS-BORDER PRIVACY RULES

EXECUTIVE SUMMARY

Without a bold and credible U.S.-led strategy for global data governance, U.S. technological and economic leadership faces mounting risks from fragmented digital rules and rival regulatory models, including from China.

MAIN ARGUMENT

Cross-border data flows are foundational to the technologies—cloud, software, search, social networks, and artificial intelligence—that demonstrate U.S. technology leadership. A U.S. technology strategy that fails to prioritize global data policy leaves U.S. firms and innovation exposed to rising digital protectionism and rival regulatory models, which undermine their market access and ability to set international standards. Existing global initiatives, such as the G-7's Data Free Flow with Trust (DFFT), the OECD's Declaration on Government Access to Personal Data Held by Private Sector Entities, the Global Cross-Border Privacy Rules (CBPR) Forum, and digital trade provisions in trade agreements, offer critical but partial building blocks. By building on and uniting these efforts, the U.S. can safeguard American innovation and technology leadership while also fostering innovation, trade, and trust with allies and trading partners.

POLICY IMPLICATIONS

- The Trump administration must build an agenda and coalition of like-minded partners for trusted data flows, such as via the Global CBPR Forum and the DFFT Initiative. The U.S. should use its diplomatic, economic, and technological leverage to bring more countries—especially key middle powers and emerging markets—into these initiatives, making participation a pillar of trade negotiations and technology cooperation.
- U.S. global data policy requires cooperation with allies and partners to prevent adversaries and untrustworthy actors from accessing sensitive data or controlling critical infrastructure. The U.S. should address national security and data privacy concerns in the cloud by working with partners to define “trusted” cloud providers and apply OECD principles for government data access. This approach would distinguish U.S. and allied providers from Chinese competitors on trust and security, while helping other countries assess cloud services on features beyond price.
- If the U.S. fails to lead on global data policy, divergent and protectionist regulations will continue to proliferate. This will create ever higher and costlier barriers to U.S. firms that otherwise depend on data flows and digital trade to access global markets. It will also undermine the international trust that is increasingly essential for digital commerce and innovation.

The Trump administration's international trade and technology policy balances a dual "protect and promote" philosophy: it aims to defend U.S. tech firms and innovators from unfair treatment in foreign markets, while strengthening U.S. global technology leadership in the face of growing competition with China. But shaping global data policy is a missing component in the administration's goal to maintain U.S. technology dominance. An enabling environment for cross-border data transfers remains as critical to U.S. leadership in new and emerging technologies as it was in past waves of U.S.-led tech innovation. The free, trusted flow of data is as foundational to artificial intelligence (AI) as it has been to internet search and cloud services, smartphones, software, and social media. Therefore, to maintain leadership, the United States needs to again be front and center in thinking creatively about a data policy strategy. A White House-led effort to coordinate global data governance would support the Trump administration's "America first" tech, trade, and economic policy agendas. Such an effort would also align with the deployment of the United States' AI and tech stack (as well as those of U.S. allies). Moreover, given the White House's current push toward deregulation, this initiative would not require new regulations or restrictions. It would instead focus on building frameworks and agreements with partners based off existing laws, regulations, and initiatives, as well as shared values and interests.

This essay argues that the Trump administration should seize the present opportunity to set a broad, clear vision and strategy for global data leadership. In furtherance of that goal, the essay is organized into the following sections:

- ≈ pp. 3–12 detail the state of play in global data governance.
- ≈ pp. 12–14 review data policy developments early in the second Trump administration.
- ≈ pp. 15–19 highlight the risks of inaction and offer recommendations on how the Trump administration can build a U.S.-led alliance for trusted global data governance.
- ≈ pp. 20 offers a conclusion.

THE STATE OF PLAY ON U.S. AND GLOBAL DIGITAL POLICY

The Challenge: Trusted Global Data Governance Is at Risk of Being Overlooked and Overwhelmed by Geopolitics, Distrust, and Other Issues

The Trump administration's economic and technology strategy—and its aim for a "golden age of American innovation"—depends in no small part on

a U.S. global data policy that leads to open and trusted data governance and market access.¹ In line with this, U.S. Trade Representative (USTR) Jamieson Greer stated in testimony: “Advancing digital trade is a key objective of U.S. trade policy....USTR will address new and existing barriers to digital trade, particularly those that discriminate against U.S. companies.”² Michael Kratsios, director of the White House Office of Science and Technology Policy, has stated that the United States “must not only dominate in the development of frontier AI capabilities, but also must ensure the American AI stack—from chips, to models, to applications—is adopted worldwide.”³ Similarly, in congressional testimony on AI, U.S. commerce secretary Howard Lutnick declared that the United States “will allow our allies to buy AI chips, provided they’re run by an approved American data center operator, and the cloud that touches that data center is an approved American operator.”⁴ In essence, open and trusted data flows support the administration’s efforts to retain global technology leadership.

Dominance in this space, however, will not be a solo effort. Global U.S. tech leadership is only possible as a shared endeavor alongside trusted allies. The White House’s new AI action plan, introduced in July 2025, provides a foundation for a global data policy, given that one of its three core pillars is to “lead in international AI diplomacy and security.”⁵ No one country completely controls the AI tech stack, and U.S. partners and allies obviously want a collaborative partnership that allows them to both use and integrate U.S. and indigenous AI and associated services.⁶ In the face of a closed U.S. approach to global tech leadership, partners and allies are more likely to limit U.S. firms’ market access and focus on pursuing their own “sovereign” AI initiatives. This is critically important as global market access provides the revenue to drive U.S. domestic research and development.

¹ Michael Kratsios, “The Golden Age of American Innovation” (remarks to the Endless Frontiers Retreat, Austin, April 14, 2025) ~ <https://www.whitehouse.gov/articles/2025/04/remarks-by-director-kratsios-at-the-endless-frontiers-retreat>.

² Jamieson Greer, “The President’s 2025 Trade Policy Agenda,” testimony before the U.S. Senate Committee on Finance, Washington, D.C., April 8, 2025.

³ Michael Kratsios, post on X, July 2, 2025 ~ <https://x.com/mkratsios47/status/1940416662752416111>.

⁴ Mackenzie Hawkins, “U.S. Plans AI Chip Curbs on Malaysia, Thailand over China Concerns,” Bloomberg, July 4, 2025 ~ <https://www.bloomberg.com/news/articles/2025-07-04/us-plans-ai-chip-curbs-on-malaysia-thailand-over-china-concerns>.

⁵ White House, *Winning the Race: America’s AI Action Plan* (Washington, D.C., July 2025) ~ <https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf>.

⁶ Hodan Omar, “The Hard Part Won’t Be Exporting U.S. AI—It’ll Be Making It Stick,” Center for Data Innovation, August 15, 2025 ~ <https://datainnovation.org/2025/08/the-hard-part-wont-be-exporting-us-ai-itll-be-making-it-stick>.

If the Trump administration does not take a leading role in shaping global data policy, other critical goals and interests will suffer. China and other countries will be more willing to enact restrictions on data transfers to disadvantage U.S. tech firms and products, which tend to rely on centralized IT and cloud infrastructure to serve markets around the world. China is leading a growing trend whereby countries mandate firms to only store specific categories of data within a country (a concept known as data localization).⁷ Localization raises the cost and complexity for U.S. firms to enter and compete in foreign markets, giving local firms an advantage as they are more likely to use local IT services. This is why data flows and by extension data localization have become major digital trade issues.

Similarly, countries like China that allow governments broad, discretionary access to data held by private firms undermine the trust that other governments and their consumers have in allowing data flows to these countries. Chinese tech firms see their comfort with both data localization and broad government access to data as a competitive advantage in their competition with U.S. firms in third-country markets. This is especially relevant when policymakers consider these policies as part of public procurement requirements and other projects. In contrast, U.S. firms tend to use legal and human rights criteria to assess government requests for data on a case-by-case basis to comply with privacy and other laws.

Failing to address these data policy trends and issues will not make them go away. Data localization will continue to grow and spread. For example, between 2017 and 2021, the number of data localization measures in force around the world more than doubled from 67 such barriers in 35 countries to 144 localization restrictions in 62 countries.⁸ Similarly, without further efforts to create common approaches for trusted government access to data, more governments will feel free to compel firms to hand over data. Limited counteraction by only the United States or a small group of other countries is unlikely to make a mark. To be successful, global data governance must involve a critical mass of countries, as cross-border data flows underpin the global internet's operation. In the absence of U.S. leadership, U.S. partners

⁷ Nigel Cory and Luke Dascoli, "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them," Information Technology and Innovation Foundation (ITIF), July 19, 2021 \approx <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost>; and Nigel Cory, "Data Localization vs. Data Governance: Why China Should Support Open, Clear, and Binding Rules on Data Flows and Digital Trade" (presentation at 2nd International Cyberspace Governance Forum, Beijing, June 9, 2022) \approx <https://itif.org/events/2022/06/09/data-localization-vs-data-governance>.

⁸ Cory and Dascoli, "How Barriers to Cross-Border Data Flows Are Spreading Globally."

and allies such as Australia, Japan, Singapore, and the United Kingdom will continue to advocate for trusted data flows. But these states lack the economic, tech, diplomatic, and political influence to truly shape global data norms and policies. Conversely, U.S. efforts to convince these and other allies to join efforts to counter China's efforts to export regressive and restrictive digital technologies and policies will inevitably fall short without an affirmative and cooperative agenda for shared global digital governance.

Building robust global data governance and flows between the United States and its friends and allies depends on trust. All partners must respect and protect the privacy and security of data from another partner and treat their respective firms and data fairly as part of integrated, cooperative digital trade and a shared approach to data governance. While trust and trustworthiness are only mentioned in passing in the Trump administration's AI action plan, they are foundational to its efforts to induce partners to support the use of the U.S. AI tech stack.

Trust appears to be in short supply, however, given current geopolitical competition and conflicts over trade and technology. U.S. allies in Europe and elsewhere are increasingly concerned that they could be arbitrarily cut off from accessing cutting-edge AI chips and U.S. digital services. Adopting the U.S. tech stack is increasingly being viewed as a critical dependency.⁹ The Trump administration should not simply look to allay these concerns but must build on existing U.S. data policies to enable trusted data flows. The salience of global data policy to the United States' and its allies' domestic and global interests means it should, ideally, be compartmentalized from other disputes. The United States and its allies need to come together to create a new framework to govern trusted, open, and fair trade and exchanges in data and technology.

Major Data Policy Initiatives and Approaches

To date, the United States and its partners have created a halting patchwork of bilateral and plurilateral policies and agreements that, taken together, represent their best effort to build trusted global data and technology governance. The process has been challenging and slow going, but this is to be expected. While how to manage data flows has been debated

⁹ Sam Clark, "Microsoft Didn't Cut Services to International Criminal Court, Its President Says," *Politico*, June 4, 2025 ~ <https://www.politico.eu/article/microsoft-did-not-cut-services-international-criminal-court-president-american-sanctions-trump-tech-icc-amazon-google>; and Pieter Haeck, "EU Gets a Win as U.S. Revokes AI Chips Caps," *Politico*, May 14, 2025 ~ <https://www.politico.eu/article/eu-win-us-revoke-ai-chips-caps>.

for decades, building genuine global data governance is still relatively new.¹⁰ Despite the rapid expansion of comprehensive domestic privacy laws around the world, there are only a few regional, plurilateral, and global initiatives to create a clear, trusted, and interoperable approach to data governance. Major initiatives include the G-7 trusted data agenda, the European Union's adequacy framework, the Global Cross-Border Privacy Rules (CBPR) Forum, and data governance provisions in trade and digital economy agreements. Looming to one side is China's restrictive and state-controlled approach to data governance. Ironically, while China has taken half-hearted steps to allow data flows, the United States and others have adopted elements of China's restrictive approach in reaction to China-related national security and cyber threats. This points to the challenge of balancing openness, trade, privacy, and cyber and national security interests.

The G-7 trusted data agenda. Trust is the defining lens that the United States, Japan, the EU, and others at the G-7 and elsewhere have applied to global data and technology governance, highlighted by the Data Free Flow with Trust (DFFT) Initiative. Since Japan launched DFFT in 2019, however, the G-7 and its partners have struggled to define what the concept means in practical policy terms.¹¹ Informally, many officials define the initiative by what it is set against, which is Chinese digital policies. The DFFT secretariat, the Organisation for Economic Co-operation and Development (OECD), has taken several steps in the right direction to change this. It is building a work agenda focused on three core issues: privacy-enhancing technologies, cross-border payment data transfers, and enhanced legal transparency around data rules.¹²

Thus far, the Trump administration appears generally supportive of the DFFT agenda, although it has not made a clear statement to that effect. Most recently, in June 2025, the G-7 Data Protection and Privacy Authorities (DPAs) met and reaffirmed the group's shared commitment to fostering trust as the foundation for a robust digital economy.¹³ The DPA roundtable specifically cited "privacy in the design, development, and deployment of new

¹⁰ Nigel Cory, "How the G7 Can Use 'Data Free Flow with Trust' to Build Global Data Governance," ITIF, June 27, 2023 ~ <https://itif.org/publications/2023/07/27/how-g7-can-use-data-free-flow-with-trust-to-build-global-data-governance>.

¹¹ Francesca Casalini and Shihori Maeda, "Moving Forward on Data Free Flow with Trust: New Evidence and Analysis of Business Experiences," Organization for Economic Cooperation and Development, OECD Digital Economy Papers, no. 353, April 2023 ~ https://www.oecd-ilibrary.org/science-and-technology/moving-forward-on-data-free-flow-with-trust_1afab147-en.

¹² "Data Free Flow with Trust," OECD ~ <https://www.oecd.org/en/about/programmes/data-free-flow-with-trust.html>.

¹³ "Championing Privacy in a Digital Age: Collective Action Today for a Trusted Tomorrow," G-7 Data Protection and Privacy Authorities, Communiqué, June 19, 2025, available at <https://www.priv.gc.ca/en/opc-news/speeches-and-statements/2025/communique-g7-250619>.

technologies” as a driver of economic success. The meeting identified the need to evaluate the opportunities and challenges to data protection and privacy presented by emerging technologies such as AI and quantum computing. It concluded by offering support to operationalizing the DFFT concept, a call that was echoed in the G-7 leaders’ statement on AI for prosperity.¹⁴

The EU’s adequacy framework and other tools. The EU’s effort to shape global data governance is largely defined by its use of “adequacy determinations” to ascertain whether a non-EU country provides a level of data privacy protection equivalent to the EU’s General Data Protection Regulation (GDPR), which safeguards the privacy of EU citizens’ personal data.¹⁵ After nearly a decade, however, the EU has reviewed and declared only a small, eclectic group of fifteen jurisdictions as adequate.¹⁶ As per the commission’s 2024 review of eleven of its fifteen existing adequacy decisions, these countries and territories have modernized and strengthened their safeguards and protections for personal data.¹⁷ However, the overall adequacy process and criteria are criticized as opaque and inconsistent, given that some countries are deemed adequate while others are not without clear reasons.¹⁸ Nevertheless, the EU has continued its advocacy for more countries to undergo adequacy assessments, such as Kenya.¹⁹

Other EU-led initiatives to shape the global data governance narrative include its first-ever high-level meeting on safe data flows, which convened the responsible European ministers and the heads of the data protection authorities in the jurisdictions that received adequacy decisions in March 2024.²⁰ The EU supports the OECD initiative on trusted government access to data, known as the “Principles for Government Access to Personal Data Held by Private Sector Entities.” The EU has also negotiated other data-related agreements, such as the U.S.-EU Data Privacy Framework, and is in the

¹⁴ “G7 Leaders’ Statement on AI for Prosperity,” G-7 2025 Kananaskis, June 16, 2025 ~ <https://g7.canada.ca/en/news-and-media/news/g7-leaders-statement-on-ai-for-prosperity>.

¹⁵ “Adequacy Decisions,” European Commission ~ https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

¹⁶ Ibid.

¹⁷ “Commission Staff Working Document—Country Reports on the Functioning of the Adequacy Decisions Adopted under Directive 95/46/EC,” European Commission, January 15, 2024 ~ https://commission.europa.eu/document/f8229eb2-1a36-4cf5-a099-1cd001664bff_en.

¹⁸ “Response to the Consultation of the EU Commission on Transfers of Personal Data to Third Countries and Cooperation between Data Protection Authorities,” ITIF ~ <https://www2.itif.org/2020-gdpr-two-year-review.pdf>.

¹⁹ “Data Protection: Kenya and the EU Launch Very First Adequacy Dialogue on the African Continent,” Delegation of the EU to Kenya, May 7, 2025 ~ https://www.eas.europa.eu/delegations/kenya/data-protection-kenya-and-eu-launch-very-first-adequacy-dialogue-african-continent_en.

²⁰ “Adequacy Decisions.”

process of negotiating an agreement with the United States on cross-border requests for law-enforcement data.²¹ The Data Privacy Framework provides participating businesses with legal certainty and a streamlined, cost-effective pathway for data transfers between the United States and EU without the use of other safeguards, such as standard contractual clauses.

The Global Cross-Border Privacy Rules Forum. Global CBPR is one of the few truly global data transfer frameworks and certification processes currently operating. It offers a principles- and accountability-based data privacy certification, whereby firms agree to an audit by designated accountability agents to demonstrate compliance, thus ensuring they adhere to baseline data protection and privacy requirements.²² Global CBPR does not require member nations to harmonize their data privacy laws. Rather, it provides a robust system for organizations to navigate the complexities of cross-border data flows between different regulatory approaches to data protection and privacy. As such, it fosters trust, supports trade, and drives innovation. The initiative traces its origins to 2022, when the United States and several other members of the Asia-Pacific Economic Cooperation (APEC) organization decided to take the existing regional CBPR framework out of its initial home in APEC to create a global system.²³ While this endeavor was undertaken in part due to China's opposition to the growth and reform of the initiative within APEC, broader reasons also sparked Global CBPR's creation—mainly the perceived need to establish a framework that supports privacy-respecting data flows and a shared sense of trust at the global level.

The Trump administration supports Global CBPR, given that the United States was part of its official launch in June 2025.²⁴ Other current members include Australia, Canada, Japan, Mexico, the Philippines, South Korea, Singapore, and Taiwan (as Chinese Taipei), plus several associate members (such as the United Kingdom). At launch, the system included approximately one hundred certified companies covering over 2,000 entities (subsidiaries included within the parent company's certification). Scale, however, remains a hurdle to overcome. Global CBPR partners must demonstrate the value of certification to encourage new firms and countries to join, as the framework

²¹ Peter Swire, "CLOUD Act Agreements, EU-U.S. E-Evidence Negotiations and Beyond," Cross-Border Data Forum, April 8, 2024 ~ <https://www.crossborderdataforum.org/cloud-act-agreements-eu-us-e-evidence-negotiations-and-beyond>.

²² "Accountability Agents," Global CBPR ~ <https://www.globalcbpr.org/economies/singapore>.

²³ Global CBPR Forum ~ <https://www.globalcbpr.org>.

²⁴ "ITA Announces the Official Launch of International Privacy Certifications," U.S. International Trade Administration, Press Release, June 2, 2025 ~ <https://www.trade.gov/press-release/ita-announces-official-launch-international-privacy-certifications>.

needs to grow and demonstrate network effects to become a truly useful global data transfer tool.

Data governance provisions in trade and digital economy agreements. A growing number of free trade agreements (FTAs) recognize the impact that restrictions on data flows have on trade and now include provisions to protect cross-border data flows, often as part of dedicated digital chapters.²⁵ Some countries, such as Australia and Singapore, have gone further in negotiating fully scoped digital economy agreements, which include foundational protections for data flows among trade partners.

Modern trade agreements increasingly act as a bridge in building interoperability between different countries' data privacy and security systems. The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) was the first significant trade agreement with specific provisions prohibiting restrictions on cross-border data flows and data localization requirements. For these provisions to be meaningful, however, they must be enforced. Yet, CPTPP parties have not so far initiated trade disputes against other members, such as Vietnam, that have enacted data localization requirements.²⁶ The CPTPP also formed the basis for the U.S.-Mexico-Canada Agreement in 2020, which strengthened provisions to protect data flows, including by covering financial data and explicitly citing APEC's CBPR as a valid data transfer mechanism. The Regional Comprehensive Economic Partnership (RCEP), a major regional Asian FTA that includes all ten ASEAN countries at the time of writing as well as Australia, China, Japan, New Zealand, and South Korea, has less stringent provisions on data transfers than the CPTPP. RCEP provisions essentially allow members full authority to determine when they contravene data flow provisions. In addition, the agreement's provisions are not subject to dispute settlement and thus are not legally enforceable.²⁷

China's domestic and international data agenda. China takes a highly restrictive and control-orientated approach to data governance and data flows. It is the world leader in data localization and other digital barriers to trade and data transfers—for example, the “great firewall of China” that restricts

²⁵ Patrick Leblond, “Trade Agreements and Data Governance,” Centre for International Governance Innovation (CIGI), November 12, 2024 ~ <https://www.cigionline.org/articles/trade-agreements-and-data-governance>.

²⁶ Nigel Cory, “How the United States and CPTPP Countries Can Stop Vietnam's Slide toward China-Like Digital Protection and Authoritarianism,” ITIF, September 8, 2023 ~ <https://itif.org/publications/2023/09/08/how-the-united-states-and-cptpp-countries-can-stop-vietnams-slide-toward-china-like-digital-protection-and-authoritarianism>.

²⁷ Leblond, “Trade Agreements and Data Governance.”

Chinese citizens' access to many prominent, popular global applications.²⁸ Chinese trade agreements do not contain meaningful commitments on data flows. Moreover, the country's evolving domestic data laws and frameworks do not place significant constraints on the government and its ability to compel access to organizational and personal data. The United States and other countries are increasingly concerned about the lack of legal protections, safeguards, and transparency around government access to data held by private firms in China. To wit, the European Data Protection Board's report on government access to data in third countries highlighted the extensive powers that Chinese authorities have over data.²⁹

Chinese authorities are slowly making marginal reforms to the domestic data governance regime in an effort to make it easier for businesses, particularly multinationals, operating in the country to transfer data overseas. These efforts implicitly recognize the impact that restrictive data policies have had on trade, foreign direct investment, and Chinese firms' efforts to expand globally. For example, the government has narrowed the impact of restrictions to specific sensitive data categories, such as important data, core data, or national secrets, and to sensitive data processors like "critical information infrastructure operators" and large internet platforms.³⁰

Many of China's recent efforts have also been criticized as merely posturing for geopolitical purposes. In November 2024, the Cyberspace Administration of China announced the Global Cross-Border Data Flow Cooperation Initiative to foster cross-border data flows and portray China as a proponent of nondiscriminatory and cooperative data policies.³¹ However, these reforms have not proved substantive from a legal and commercial perspective (that is, they have not actually made it easier for firms to transfer data out of China) and, in the case of the new initiative, appear to reflect geopolitical posturing (in reacting to U.S. initiatives targeting Chinese tech firms). At the United Nations and elsewhere, China generally advocates for its view of "cyber sovereignty," which is a state-centric approach to international data governance. This is

²⁸ Cory and Dascoli, "How Barriers to Cross-Border Data Flows Are Spreading Globally."

²⁹ "Legal Study on Government Access to Data in Third Countries," European Data Protection Board, November 8, 2021 ~ https://www.edpb.europa.eu/our-work-tools/our-documents/legal-study-external-provider/legal-study-government-access-data-third_en.

³⁰ "China Unveils New Framework to Stimulate Cross-Border Data Flows: Risk or Opportunity for Multinational Companies," Crowell, January 13, 2025 ~ <https://www.crowell.com/en/insights/client-alerts/china-unveils-new-framework-to-stimulate-cross-border-data-flows-risk-or-opportunity-for-multinational-companies>.

³¹ "China to Unveil Global Cross-Border Data Flow Cooperation Initiative, Says Xi," MLex, November 18, 2024 ~ https://content.mlex.com/#/content/1610830/china-to-unveil-global-cross-border-data-flow-cooperation-initiative-says-xi?referrer=search_linkclick.

reflected in proposals such as its Global Initiative on Data Security.³² China's vision for cyber sovereignty emphasizes that governments can essentially take any actions they deem necessary with respect to data, including leveraging it for economic development and national security.³³ At the same time, none of these initiatives changes the fact that China remains at the forefront of data localization requirements. China sees control of data as critical to regime stability; its data governance frameworks and views on cross-border transfers will, therefore, necessarily remain focused on security and strict controls.

THE TRUMP ADMINISTRATION'S DATA POLICY THUS FAR

President Donald Trump re-entered the White House in 2025 with a limited legacy on digital policy upon which to build. His first administration's approach was largely defined by its Clean Network Initiative, a comprehensive effort to address threats to data privacy from authoritarian state actors, and its cybersecurity strategy.³⁴ The 2025 Presidential Transition Project ("Project 2025") did mention the Department of Commerce's "indispensable work ensuring cross-border data flows, particularly with Europe, remain open and relatively unrestricted."³⁵ But at the time of writing, well into the first year of the president's second term, the White House has not announced any major global technology strategy (beyond AI) or data policy. As noted above, it has reversed several Biden administration digital trade policies that undermined U.S. global data policy, including listing data localization policies in the USTR's 2025 National Trade Estimate.³⁶ The administration has, however, made several specific public statements and policy decisions that indicate its general approach to global data policy. In line with the new AI action plan, it

³² Emily de La Bruyère, Doug Strub, and Jonathon Marek, eds., "China's Digital Ambitions: A Global Strategy to Supplant the Liberal Order," National Bureau of Asian Research, NBR Special Report, no. 97, March 1, 2022, 79 ~ https://www.nbr.org/wp-content/uploads/pdfs/publications/sr97_chinas_digital_ambitions_mar2022.pdf.

³³ "China Unveils New Framework to Stimulate Cross-Border Data Flows."

³⁴ The cybersecurity strategy was the closest to a formal strategy for the global internet. It included as a goal to "preserve the long-term openness, interoperability, security, and reliability of the Internet, which supports and is reinforced by America's interests. We will take specific global efforts to promote these objectives, while supporting market growth for infrastructure and emerging technologies and building cyber capacity internationally." "President Trump Unveils America's First Cybersecurity Strategy in 15 Years," U.S. National Security Council, September 20, 2018 ~ <https://trumpwhitehouse.archives.gov/articles/president-trump-unveils-americas-first-cybersecurity-strategy-15-years>.

³⁵ Paul Dans and Steve Groves, eds. *Mandate for Leadership: The Conservative Promise 2025* (Washington, D.C.: Heritage Foundation, 2023).

³⁶ USTR, *2025 National Trade Estimate Report on Foreign Trade Barriers of the President of the United States on the Trade Agreements Program* (Washington, D.C., 2025) ~ <https://ustr.gov/sites/default/files/files/Press/Reports/2025NTE.pdf>.

is clear that the Trump administration prioritizes the deregulation of digital and tech policy and support for innovation rather than the creation of new data privacy and security laws and frameworks.

Specific to trade policy, the Trump administration has re-energized the U.S. posture to support free flows of data and U.S. leadership on digital trade. Until 2023, the government's stance was generally supportive of the free flow of data and provisions to limit data localization in its FTAs and trade negotiations; it also advocated for relevant efforts within multilateral trade forums. In the fall of 2023, however, the Biden administration withdrew support for provisions on cross-border data flows, data localization, and the transfer of source code in the Joint Statement Initiative on E-Commerce at the World Trade Organization. The White House also suspended digital trade talks in the Indo-Pacific Economic Framework for Prosperity.³⁷ In contrast, the Trump administration uses bilateral trade talks to target data localization and other barriers to data flows and digital trade in its negotiations with trading partners. For example, Indonesia agreed to provide certainty to allow firms to move personal data to the United States, among other digital trade commitments.³⁸ With Brazil, the Trump administration is targeting payment service restrictions.³⁹ The Trump administration clearly sees these requirements as nontariff barriers that target U.S. tech firms.⁴⁰ Only time will tell whether countries actually remove these barriers, however, as the enforceability of these agreements is unclear.

To date, the Trump administration has not changed the United States' role in existing global data agreements and initiatives. As detailed, it participated in the launch of Global CBPR, which successive U.S. administrations had worked for years to establish. The Trump administration has also not rescinded the executive order that backs the U.S. commitments made in

³⁷ "Digital Trade and Data Policy: Key Issues Facing Congress," Congressional Research Service, In Focus, IF12347, May 1, 2025 \approx <https://www.congress.gov/crs-product/IF12347>.

³⁸ "The United States and Indonesia Reach Historic Trade Deal," White House, Fact Sheet, July 22, 2025 \approx <https://www.whitehouse.gov/fact-sheets/2025/07/fact-sheet-the-united-states-and-indonesia-reach-historic-trade-deal>.

³⁹ Margaret Spiegelman, "Industry, Civil Society Weigh In on Section 301 Probe of Brazil," Inside U.S. Trade, August 20, 2025 \approx <https://insidetradetrade.com/daily-news/industry-civil-society-weigh-section-301-probe-brazil>.

⁴⁰ "Defending American Companies and Innovators from Overseas Extortion and Unfair Fines and Penalties," White House, February 26, 2025 \approx <https://www.federalregister.gov/documents/2025/02/26/2025-03188/defending-american-companies-and-innovators-from-overseas-extortion-and-unfair-fines-and-penalties>.

the U.S.-EU Data Privacy Framework, although it fired some key personnel involved in the framework.⁴¹

The first instance of definitive policy action on data and digital trade undertaken by the second Trump administration was the Department of Justice's issuance of implementation and enforcement guidance in April 2025 for its Data Security Program (DSP) protecting bulk sensitive data. The DSP essentially establishes rules for U.S. persons and entities engaging in specific data transactions deemed by the U.S. government as posing an unacceptable risk of giving "countries of concern" or "covered persons" access to government-related data or bulk U.S. sensitive personal data. All the additional requirements, including due diligence, auditing, and reporting related to the DSP are set to become effective on October 6, 2025.⁴² The DSP is being equated by many to "an official export control program for certain sensitive personal data."⁴³

In another, more targeted instance of controlling the movement of U.S. citizens' personal data, the U.S. Food and Drug Administration announced a halt and immediate review of new clinical trials in June 2025.⁴⁴ This includes trials where American patients' cells were sent to China or other "hostile countries" for genetic engineering with the expectation that the cells would be reinfused into U.S. patients.⁴⁵ The announcement apparently came in the face of "mounting evidence" that some researchers had failed to obtain informed consent from trial participants on the international transfer and manipulation of biological material.⁴⁶ Nevertheless, there is continued ambiguity regarding the finer details of the policy, including how it will impact ongoing trials and questions regarding details that will be required to sufficiently obtain informed consent.⁴⁷

⁴¹ Divya Sridhar, "Trump Administration Playing Truth or Dare with EU-U.S. Data Privacy Framework," *Infosecurity Magazine*, May 5, 2025 ~ <https://www.infosecurity-magazine.com/opinions/trump-eu-us-data-privacy-framework>.

⁴² "Ready To Know Your Data? DOJ Issues Implementation and Enforcement Guidance for Data Security Program Protecting Bulk Sensitive Data," Crowell, April 18, 2025 ~ <https://www.crowell.com/en/insights/client-alerts/ready-to-know-your-data-doj-issues-implementation-and-enforcement-guidance-for-data-security-program-protecting-bulk-sensitive-data>.

⁴³ "DOJ Data Security Program Update: Active Enforcement Begins This Week," Crowell, July 7, 2025 ~ <https://www.crowell.com/en/insights/client-alerts/doj-data-security-program-update-active-enforcement-begins-this-week>.

⁴⁴ "FDA Halts New Clinical Trials That Export Americans' Cells to Foreign Labs in Hostile Countries for Genetic Engineering," U.S. Food and Drug Administration, June 18, 2025, Press Release ~ <https://www.fda.gov/news-events/press-announcements/fda-halts-new-clinical-trials-export-americans-cells-foreign-labs-hostile-countries-genetic>.

⁴⁵ *Ibid.*

⁴⁶ *Ibid.*

⁴⁷ "FDA Targets Gene Editing Clinical Trials in China and Other 'Hostile Countries,'" Crowell, June 26, 2025 ~ <https://www.crowell.com/en/insights/client-alerts/fda-targets-gene-editing-clinical-trials-in-china-and-other-hostile-countries>.


HOW THE TRUMP ADMINISTRATION CAN BUILD FAIR AND TRUSTED DATA GOVERNANCE THAT SUPPORTS U.S. TECH LEADERSHIP


The Trump administration should consider developing a data policy to induce partners to treat both U.S. tech firms and U.S. data fairly and to build data flows between trusted partners.

Continue to leverage trade negotiations to remove data-related barriers to digital trade. The Trump administration should prioritize addressing barriers to digital trade in its negotiations with trading partners, such as India, Indonesia, Mexico, and Vietnam. The administration has made several statements that show it recognizes the importance of removing barriers to data flows and digital free trade. This should be a key aim given that U.S. firms are world leaders in digital trade. Through sales abroad, U.S. firms brought in \$626 billion from digitally enabled services exports in 2022, up 5.5% from \$599 billion in 2021.⁴⁸ The surplus for the United States in such services was \$256 billion in 2022.⁴⁹ But absent consistent and concerted action by the administration, more countries will likely enact nontariff barriers related to data in order to disadvantage U.S. firms and their services.⁵⁰

Promote Global CBPR as a vehicle for trusted data flows. The Trump administration should use the recently launched Global CBPR Forum as the vehicle for partners to show that they are committed to working with the United States to build trusted data governance, digital free trade, and AI leadership. Global CBPR is a fair, reasonable, and useful tool that provides an additional certifiable layer of accountability about how data is protected and respected when transferred between trusted members.

While there are currently only thirteen jurisdictions participating in Global CBPR, they include both major U.S. trading partners, such as Japan, Canada, and Australia, and partners critical to global technological collaboration and innovation, such as Singapore and Taiwan. Integrating Global CBPR into broader U.S. tech policy and trade negotiations would be a way to encourage partners to demonstrate their commitment to fairness,

⁴⁸ Amir Nasr, “New Data Showcase the Strength of Digital Services Exports to Overall U.S. Economy (Disruptive Competition Project),” Korea International Trade Association, July 26, 2023  https://www.kita.net/board/tradeNews/tradeNewsDetail.do;SESSIONID_KITA=B66B3F799B6BD7E886C7D8CCC9BA481A.Hyper?no=1835932.

⁴⁹ Amir Nasr, “The Trade Barriers Carrying the Greatest Threat to U.S. Digital Export Strength in 2023,” Disruptive Competition Project, October 27, 2023  <https://project-disco.org/21st-century-trade/trade-barriers-carrying-the-greatest-threat-to-u-s-digital-export-strength-in-2023>.

⁵⁰ “A Global View of Barriers to Cross-Border Data Flows,” ITIF, July 19, 2021  <https://itif.org/publications/2021/07/19/global-view-barriers-cross-border-data-flows>.

equity, and trust in data flows and digital free trade. Such a move would likely help the framework attract more members. The White House could also leverage Global CBPR as part of the international pillar of its recently launched AI action plan. Likewise, as detailed below, the administration could launch a parallel discussion alongside Global CBPR on trusted government access to data.

It remains early for Global CBPR to emerge as an enduring, viable system, considering that it was only officially launched in June 2025. Increased global participation from partner countries—and the visibility, credibility, and network effects that would come with significant expansion—is the critical pathway that must be traversed. This is where the Trump administration can play a valuable role. The UK is considering membership; similarly, the system has been considered in talks between the United States and India in both government and private-sector channels. If the White House could convince both states to join, along with a rising middle power like Indonesia, for example, it could help achieve a critical mass to make the framework a truly valuable global mechanism for data transfers.

Target China and other untrustworthy countries and support efforts for trusted government access to data. The Chinese government's broad, arbitrary, and opaque ability to access data held by private entities (for potential economic, national security, or military purposes) underpins growing concerns about government access in the United States, the EU, and elsewhere.⁵¹ The Trump administration should create a trusted government access initiative to work with allies and partners to address the data privacy and security issues raised by China's approach.

Congress and successive U.S. administrations have expressed legitimate concerns about whether Chinese tech firms can resist the demands for their data from the Chinese government. The Biden and Trump administrations' DSP, informally known as the bulk data sharing rule, reflects these concerns. U.S. policymakers frequently highlight broad and ambiguous provisions in China's national security, data security, intelligence, and cybersecurity laws to argue that Chinese citizens and firms are subject to direct orders from the government, including its intelligence agencies. Legal analysis suggests that it

⁵¹ For example, in the EU, see Ellen O'Regan, "Ireland Launches Second Probe into TikTok Data Flows to China," *Politico*, July 10, 2025 ~ <https://www.politico.eu/article/ireland-launches-second-probe-into-tiktok-data-flows-to-china>.

would be challenging (to say the least) for any Chinese citizen or company to resist a direct request from Chinese security or law-enforcement agencies.⁵²

The United States has the principles, partners, and forum—the ongoing OECD-led initiative on trusted government access to data held by private entities—to develop a coordinated approach to concerns about overly broad government access to data.⁵³ This multilateral initiative is unique and valuable as it involves security, intelligence, law enforcement, privacy, trade, and other officials from OECD member countries. The declaration on trusted government access to data is the most substantive demonstration so far of how countries can overcome the sensitive nature of the issue and agree on common principles such as the following, which is a clear differentiator from China’s opaque model:

We reject any approach to government access to personal data held by private sector entities that, regardless of the context, is inconsistent with democratic values and the rule of law, and is unconstrained, unreasonable, arbitrary or disproportionate. Such approaches violate privacy and other human rights and freedoms, breach international obligations, undermine trust and create a serious impediment to data flows to the detriment of the global economy. By contrast, our countries’ approach to government access is in accordance with democratic values; safeguards for privacy and other human rights and freedoms; and the rule of law including an independent judiciary. These protections also contribute to promoting trust by private sector entities in meeting their responsibilities in this context.⁵⁴

The Trump administration should work with trusted partners to develop new tools to define trusted government access to data and to prevent sensitive data from going to untrustworthy jurisdictions. Most jurisdictions do not have a clear legal mechanism, process, or framework to do this. The U.S. government’s experience with trying to bring the bulk data initiative to life would be instructive to other countries. The United States should start dialogues on the national security issues of data with trusted partners, such as Australia, the EU, Japan, and the UK, to develop common tools and frameworks to specifically address national security in data flows to China and other problematic jurisdictions, such as Russia.

⁵² Jeremy Daum, “What China’s National Intelligence Law Says, and Why It Doesn’t Matter,” China Law Translate, February 22, 2024 ~ <https://www.chinalawtranslate.com/en/what-the-national-intelligence-law-says-and-why-it-doesnt-matter>.

⁵³ “Declaration on Government Access to Personal Data Held by Private Sector Entities,” OECD, OECD Legal Instruments, December 14, 2022 ~ <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487>.

⁵⁴ Ibid.

The United States and key partners could also create a forum on trusted government access to data to run in parallel to the Global CBPR Forum. The latter addresses commercial data privacy issues, while the new forum could address corresponding privacy issues related to government access to data. Such a dialogue could be attractive to the many non-OECD countries that are likewise grappling with the best approach to address both commercial and government privacy concerns.

Develop a trusted cloud. The United States should establish a trusted cloud initiative with key allies and trading partners—such as the Five Eyes intelligence partners, Japan, and the EU, among others—to develop a common, flexible, and risk-based approach to issues pertaining to cloud trustworthiness, national security, and sensitive data.⁵⁵ This initiative would represent a major coordinated effort to address shared concerns about China and other governments’ access to sensitive data.⁵⁶ Given the role of cloud technology in managing ever-growing amounts of data in today’s digital economy, it merits special attention.

The threat of governments compelling cloud service providers to surrender customer data is a long-standing issue. The United States has made legal and administrative reforms—including in the USA Freedom Act, the Judicial Redress Act, and the Clarifying Lawful Overseas Use of Data (CLOUD) Act—and negotiated international agreements with the EU to address such concerns.⁵⁷ While the EU has thus far taken a blinkered approach by only focusing on the United States, European policymakers seem to have recently awakened to the issue of EU citizens’ data going to China. The Irish Data Protection Commission’s enquiry into TikTok transferring users’ personal data to China is an example of greater EU scrutiny of its citizens’ data outflows.⁵⁸ Australia, Japan, and other countries have taken steps, both small and large, to address national security concerns about data exports to China.

The United States with partners should develop a toolkit of technical, legal, and administrative policies to help define trusted cloud service in a

⁵⁵ Nigel Cory, “Technical and Legal Criteria for Assessing Cloud Trustworthiness,” ITIF, April 22, 2024 ~ <https://itif.org/publications/2024/04/22/technical-legal-criteria-for-assessing-cloud-trustworthiness>.

⁵⁶ Ibid.

⁵⁷ For example, see Peter Swire, “U.S. Surveillance Law, Safe Harbor, and Reforms since 2013,” Georgia Tech Scheller College of Business, Research Paper, no. 36, December 18, 2015 ~ <http://dx.doi.org/10.2139/ssrn.2709619>.

⁵⁸ “Irish Data Protection Commission Fines TikTok €530 Million and Orders Corrective Measures Following Inquiry into Transfers of EEA User Data to China,” Data Protection Commission (Ireland), May 2, 2025 ~ <https://www.dataprotection.ie/en/news-media/latest-news/irish-data-protection-commission-fines-tiktok-eu530-million-and-orders-corrective-measures-following>.

pragmatic way.⁵⁹ They should map and work to align the technical controls and standards, audits, and certifications they each use to identify trusted and secure cloud service providers. For example, policymakers should develop a common catalog of technical controls, which are the specific requirements for incident response, configuration management, and the privacy and cybersecurity measures that together are used by technical standards and cloud certification regimes. Ideally, policymakers from like-minded countries would designate an institution or mechanism (either existing or new) to help coordinate a common approach to the measures that would define trusted versus untrusted cloud service.

Detailed and clear criteria for cloud trustworthiness—endorsed by the United States and U.S. partners—would represent a clear point of differentiation with Chinese cloud firms. It would obviously be beneficial from a data protection and security perspective. It would also take on broader commercial and strategic significance in terms of geopolitical competition over technology market share in third-country markets. If the Trump administration wants to support the U.S. AI tech stack in markets around the world, it will need to do more to define cloud trustworthiness, considering that trust is a key factor in public-sector and commercial decisions in selecting cloud providers. A trusted cloud initiative would be one way to operationalize administration interest in allowing allies to buy and use U.S. AI on approved U.S. cloud services, but it could be broadened to trusted cloud providers from allies.⁶⁰

While U.S. cloud firms still lead many global markets due to their ability to provide best-in-class services and global operations, Chinese firms are increasingly global and innovative, in addition to being price competitive. Chinese firms excel in using low prices to seize market share in emerging markets, and at the moment policymakers in many third-country markets focus mainly on the price of cloud projects. While they often recognize the importance of privacy, security, and trust-related services and features, it is not easy for them to identify and value what this means in practice when comparing cloud service providers. If the United States and others created a trusted cloud initiative, it would make it far easier for their cloud firms to clearly demonstrate cloud trustworthiness alongside other factors like price.

⁵⁹ Cory, “Technical and Legal Criteria for Assessing Cloud Trustworthiness.”

⁶⁰ Hawkins, “U.S. Plans AI Chip Curbs on Malaysia, Thailand over China Concerns.”

CONCLUSION

The world is becoming more complicated for U.S. firms trying to move data across borders, especially as more countries create their own data laws. This impacts U.S. leadership of new and emerging technologies. In this shifting environment, the United States is at a crossroads—no longer the uncontested leader but still uniquely positioned to shape the technology rules of the road.

As we have seen, there are now three main global approaches to data: China's strict control, the EU's prescriptive push for regulatory harmonization of its laws, and a few newer, more flexible initiatives that emphasize trusted data flows and governance. In the latter category, the Global CBPR Forum is a standout given that it is a clear and broadly applicable framework for building trusted data flows and already has supporting institutional arrangements for expansion. The DFFT Initiative also has the potential to support trusted data flows among the United States and its partners but needs more pragmatic projects to make it real and meaningful.

Against this backdrop, the United States should stop simply reacting to others and instead set out a clear, forward-thinking strategy for global data policy. This strategy should reflect American democratic values and economic, trade, and technology interests while also acknowledging today's geopolitical realities. The United States needs to re-engage in digital trade diplomacy, not just through conducting bilateral talks but by leading broader efforts to create shared rules and practical solutions for trusted data flows.

The United States cannot do this alone. It should lead a coalition of like-minded partners—particularly across the Indo-Pacific, Latin America, and Africa—that want an open, innovative, and rights-respecting digital world. This means listening to partners as well as leading, sharing expertise, and supporting them through technical and policy cooperation.

The stakes are high. Data is increasingly central to global commerce, innovation, and diplomacy. If differing and conflicting data rules fragment the global digital economy, U.S. and allied countries' leadership in technology—and the open internet itself—could suffer. But if the United States creates a clear data strategy at home and works closely with its allies and partners abroad, it can help steer global data rules toward openness, trust, and innovation. This is a critical effort that the United States—and the Trump administration—should lead. ♦