



GLOBAL DATA ALLIANCE

TRUST ACROSS BORDERS

TABLE OF EXHIBITS

USTR INQUIRY RE *PROMOTING SUPPLY CHAIN RESILIENCE*

- Exhibit 1: GDA, *Hearing Testimony on Supply Chain Resilience*
- Exhibit 2: The White House, *US National Cybersecurity Strategy* (excerpts)
- Exhibit 3: The White House, *US National Security Strategy* (excerpts)
- Exhibit 4: The White House, *US Indo-Pacific Strategy*
- Exhibit 5: US Department of State, *Declaration for the Future of the Internet*
- Exhibit 6: US Department of Commerce, *US-EU Data Privacy Framework*
- Exhibit 7: US Department of Commerce, *Global Cross-Border Privacy Rules Forum Overview*
- Exhibit 8: US Department of Treasury, *Joint Statement on Financial Services Data Connectivity*
- Exhibit 9: US Department of State, *US Cyberspace and Digital Policy Strategy*
- Exhibit 10: GDA, Letter to White House re Indo-Pacific Economic Framework
- Exhibit 11: GDA, Letter to USTR re “Early Harvest” Cross-Border Data Outcomes in IPEF
- Exhibit 12: Global Industry Letter to White House re Indo-Pacific Economic Framework
- Exhibit 13: Global Industry Letter to Commerce and USTR re Indo-Pacific Economic Framework
- Exhibit 14: GDA, Position Paper, *Cross-Border Data Policy Principles*
- Exhibit 15: GDA, Position Paper, *Cross-Border Data Transfers and Data Localization*
- Exhibit 16: GDA, *Cross-Border Data Policy Index*
- Exhibit 17: US Senate, *Bipartisan Letter from 32 Senators re USTR’s Digital Trade Policy Reversal*
- Exhibit 18A: China Ministry of Commerce, *Three-Year Action Plan for Digital Commerce (2024-2026)*
- Exhibit 18B: MarcoPolo, *Much Ado About Data – How America and China Stack Up*
- Exhibit 18C: LawFare, *Assessing US Data Policy Towards China*
- Exhibit 19A: GDA, Memorandum, *Impact of USTR Digital Trade Policy Reversal on USG Priorities*
- Exhibit 19B: GDA, Memorandum, *Impact of USTR Digital Policy Reversal on Other Gov’t Agency Interests*
- Exhibit 19C: GDA, Memorandum, *Impact of USTR Digital Policy Reversal on US Artificial Intelligence Policy*
- Exhibit 19D: GDA, Recommendations to White House on Cross-Border Data
- Exhibit 19E: Hinrich Foundation, “The True Cost of USTR’s U-Turn on WTO E-Commerce Talks”
- Exhibit 20: GDA, *Submission to USTR on Worker-Centered Trade Policy*

- Exhibit 21A: US Chamber of Commerce, *How US Workers and Companies Benefit from Digital Trade*
- Exhibit 21B: Trade Partnership (for Business Roundtable), *Trade & American Jobs*
- Exhibit 22: Deloitte/ Manufacturing Institute, *Manufacturers Support Growth with Active Workforce Strategies*
- Exhibit 23: CSI, *Services and Digital Trade Are Critical to US Competitiveness & Middle-Class Job Creation*
- Exhibit 24: CSI, *Addressing Foreign Services Trade & Investment Barriers Benefits American Workers*
- Exhibit 25: CSI, *Services and Digital Trade Workforce Development Programs*
- Exhibit 26: BSA, *Workforce Development Agenda*
- Exhibit 27: GDA, Supply Chain Resilience Issue Brief, *Cross-Border Data & Cybersecurity*
- Exhibit 28: Swire, et al., *Risks to Cybersecurity from Data Localization*
- Exhibit 29: GDA, Supply Chain Resilience Issue Brief, *Cross-Border Data & Competition*
- Exhibit 30: sifma, *Why Financial Services are Vital to US International Economic Strategy*
- Exhibit 31A: GDA, Supply Chain Resilience Issue Brief, *Cross-Border Data & Regulatory Compliance*
- Exhibit 31B: Transparency International, *Supply Chain Corruption & Customs Transparency*
- Exhibit 32: American Civil Liberties Union, Freedom House, et al., *Letter to USTR, State, and Commerce*
- Exhibit 33: Internet Society, *The US Takes a Dangerous Step Back from Core Internet Principles*
- Exhibit 34: Freedom House, *Reversal of US Trade Policy Threatens the Free and Open Internet*
- Exhibit 35: Freedom House, *The Human Rights Costs of Data Localization Around the World*
- Exhibit 36: Senate Foreign Relations Committee, *The New Big Brother – China & Digital Authoritarianism*
- Exhibit 37: Freedom House, *Freedom on the Net 2022* (excerpts)
- Exhibit 38: GDA, Report, *Cross-Border Data Transfers & Innovation*
- Exhibit 39: GDA, Filing, *Submission to USTR re Special 301 Annual Review of IP Protection & Enforcement*
- Exhibit 40: GDA, Supply Chain Resilience Sector Brief, *Medical Technology*
- Exhibit 41: GDA, Report, *Cross-Border Data & Remote Health Services*
- Exhibit 42: GDA, Report, *Cross-Border Data & Biopharmaceutical R&D*
- Exhibit 43: GDA, Report, *Cross-Border Data & Environmental Sustainability*
- Exhibit 44: GDA, Supply Chain Resilience Issue Brief, *Cross-Border Data & Artificial Intelligence*
- Exhibit 45: GDA, *Submission to USAID re Artificial Intelligence in Global Development*
- Exhibit 46: GDA, Report, *Cross-Border Data & Economic Development*
- Exhibit 47: US Agency for International Development, *Digital Strategy (2020-2024)*
- Exhibit 48: GDA, Supply Chain Resilience Sector Brief, *Cross-Border Data & Small Business*
- Exhibit 49A: Small Business & Entrepreneurship Council, *Letter to House W&M re Support for Small Business*
- Exhibit 49B: Allied for Startups, et al., *Letter to President Biden re Support for Small Business*
- Exhibit 50: US Chamber, *How USTR's Digital Trade Reversal Will Hurt Small Businesses*
- Exhibit 51: ACT, *Why Has the USTR Stopped Supporting Small Business Digital Trade?*
- Exhibit 52: ACT, *Another Blow Meant for Big Tech Lands on the Left Eye of Small Biz*

- Exhibit 53: ACT, *The Importance of Digital Trade for Small Businesses*
- Exhibit 54: Engine, *For Startups' Sake, Congress Needs to Reorient US Trade Agency*
- Exhibit 55: GDA Report, *Cross-Border Data & Supply Chain Management*
- Exhibit 56A: Forum for International Trade Training, *Unpacking the Digital Transformation of Trade*
- Exhibit 56B: Hinrich Foundation, *Leveraging Electronic Documents for Sustainable Ag. Trade*
- Exhibit 57: Global Industry Statement on the WTO Moratorium on Customs Duties on E. Transmissions
- Exhibit 58: US Industry Letter to NSC, NEC, and USTR re *Customs Duties on Electronic Transmissions*
- Exhibit 59: Association CEO Letter to President Biden re *Customs Duties on Electronic Transmissions*
- Exhibit 60: US Industry Letter to NSC re *US Support for Renewal of WTO Moratorium*
- Exhibit 61: Letter to USTR Tai re *Customs Duties on Electronic Transmissions*
- Exhibit 62: GDA, *Statistical Summary of Evidence re Customs Duties on Electronic Transmissions*
- Exhibit 63: GDA, *Recommendations to WTO re Customs Duties on Electronic Transmissions*
- Exhibit 64: BSA, *Customs Duties on Software and Other Digital Exports– A Threat to Growth and Innovation*
- Exhibit 65A: Progressive Policy Institute, *WTO E-Commerce Tariff Moratorium at 25*
- Exhibit 65B: OECD, *Understanding the Scope, Definition and Impact of the WTO E-Commerce Moratorium*
- Exhibit 65C: Trade Experettes, *WTO E-Commerce Moratorium & Women*
- Exhibit 66A: GDA, Report, *Cross-Border Movement of Information – Creating Jobs in Every Sector*
- Exhibit 66B: GDA, Infographic, *Jobs in all Sectors Depend on Cross-Border Data Flows*
- Exhibit 66C: GDA, Infographic, *Cross-Border Data Facts & Figures*
- Exhibit 67: GDA, Supply Chain Sector Brief, *Cross-Border Data & the Automotive Sector*
- Exhibit 68: GDA, Supply Chain Sector Brief, *Cross-Border Data & Agriculture*
- Exhibit 69: GDA, Supply Chain Sector Brief, *Cross-Border Data & Natural Resources*
- Exhibit 70: GDA, Supply Chain Sector Brief, *Cross-Border Data & Finance and Insurance*
- Exhibit 71: GDA, Supply Chain Sector Brief, *Cross-Border Data & Healthcare Delivery*
- Exhibit 72: GDA, Supply Chain Sector Brief, *Cross-Border Data & Health Research*
- Exhibit 73: GDA, Supply Chain Sector Brief, *Cross-Border Data & Media and Publishing*
- Exhibit 71: GDA, Supply Chain Sector Brief, *Cross-Border Data & Media and Publishing*
- Exhibit 74: GDA, Supply Chain Sector Brief, *Cross-Border Data & Supply Chain Logistics*
- Exhibit 75: GDA, Supply Chain Sector Brief, *Cross-Border Data & Telecommunications*
- Exhibit 76: SELECTUSA, *FDI in Advanced Manufacturing*
- Exhibit 77: SELECTUSA, *FDI in Aerospace*
- Exhibit 78: SELECTUSA, *FDI in Agribusiness*
- Exhibit 79: SELECTUSA, *FDI in the Automotive Industry*
- Exhibit 80: SELECTUSA, *FDI in Energy*
- Exhibit 81: SELECTUSA, *FDI in High-Tech*

- Exhibit 82: SELECTUSA, *FDI in Information & Communications Technology*
- Exhibit 83: SELECTUSA, *FDI in Life Sciences*
- Exhibit 84: SELECTUSA, *FDI in Logistics & Supply Chain*
- Exhibit 85: SELECTUSA, *FDI in Manufacturing*
- Exhibit 86: SELECTUSA, *FDI in Professional Services*
- Exhibit 87: The White House, *Presidential Directive for Democratic Renewal*
- Exhibit 88: GDA, Memorandum, *Legal Analysis of USTR Digital Policy Reversal (2024)*
- Exhibit 89: GDA, *Myths v. Facts, Cross-Border Data and Access to Information (2024)*
- Exhibit 90: Compilation of Select Congressional Statements re USTR Digital Trade Policy Reversal
- Exhibit 91: Bipartisan Senate Letter Raising Concerns with USTR Digital Trade Policy Reversal
- Exhibit 92: Bipartisan House Letter Raising Concerns with USTR Digital Trade Policy Reversal
- Exhibit 93: Congressional Letter re Small Business Concerns with USTR Digital Trade Policy Reversal
- Exhibit 94: Congressional Letter re Competition Concerns with USTR Digital Trade Policy Reversal
- Exhibit 95: Congressional Letter re Oversight with USTR Digital Trade Policy Reversal
- Exhibit 96: New Democrat Coalition Letter Raising Concerns with USTR Trade Policy
- Exhibit 97: Congressional Letter re USTR Failure to Address Digital Barriers in NTE Report
- Exhibit 98: Bipartisan House Letter Raising Concerns re USTR Support for WTO E-Commerce Moratorium
- Exhibit 99: Bipartisan House Letter Urging USTR Support for Renewal of WTO E-Commerce Moratorium
- Exhibit 100: Senate Letter Criticizing USTR's Disregard for Congressional Direction on Cross-Border Data
- Exhibit 101: GDA, *Frequently Asked Questions on Cross-Border Data Trade Rules*
- Exhibit 102: Multi-Industry Letter to Senate Finance and House Ways & Means re USTR NTE Report
- Exhibit 103: Multi-Industry Letter to White House re USTR's Failure to Address Digital Barriers in NTE Report
- Exhibit 104: Multi-Industry Letter to White House re USTR's Withdrawal of Support for Digital Trade
- Exhibit 105: Center for Strategic and International Studies, *USTR Upends U.S. Negotiating Position on Cross-Border Data Flows*
- Exhibit 106: Lawfare, *China Gains as US Abandons Digital Policy Negotiations*
- Exhibit 107: Center for New American Security, *Is US Trade Policy Hitting Rock Bottom?*
- Exhibit 108: IBM, *USTR's Disastrous 180 on Digital Trade*
- Exhibit 109: Hinrich Foundation, *Katherine Tai's Struggles Over the US Trade Agenda*
- Exhibit 110: Hinrich Foundation, *Maintaining Robust Digital Trade Monitoring and Enforcement*
- Exhibit 111: Hinrich Foundation, *Why Does the US Hate Digital Trade?*
- Exhibit 112: Coalition to Reduce Cyber Risk, *Unraveling the Impact of USTR's WTO Reversal on Cybersecurity and Global Trade*
- Exhibit 113: US Chamber of Commerce, *How Reversal on Digital Trade Threatens US Workers, Businesses*
- Exhibit 114A: US Chamber of Commerce, *Why Digital Trade Is Critical to the US and Global Economies*
- Exhibit 114B: US Chamber of Commerce, *Documents Show FTC and DOJ Influence Over US Trade Policy*

- Exhibit 115: US Chamber of Commerce, *Bipartisan Concern with US Surrendering on Digital Trade*
- Exhibit 116: US Chamber of Commerce, *Setting the Record Straight on Foreign Trade Barriers*
- Exhibit 117: US Chamber of Commerce, *Why Restoring America's Digital Trade Leadership Is Critical*
- Exhibit 118: US Chamber of Commerce, *How Digital Trade Benefits the American Economy*
- Exhibit 119: US Chamber of Commerce, *Digital Trade Rules Benefit Every Sector of the US Economy*
- Exhibit 120: Centre for International Governance Innovation, *After USTR's Move, Global Governance of Digital Trade Is Fraught with Unknowns*
- Exhibit 121: Inside Trade, *USTR is mirroring China's data stance, undermining U.S. interests*
- Exhibit 122: NetChoice, *Biden's USTR Gave Progressives a Political Win on Digital Trade, American Businesses Lose*
- Exhibit 123: The Hill, *The Biden Administration is Betraying Congress on Digital Trade*
- Exhibit 124: Progressive Policy Institute, *US Internet Policy is Suddenly Uncertain*
- Exhibit 125: CCIA, *Responding to the Myths Holding Back US Action on Digital Trade*
- Exhibit 126: CCIA, *USTR's Revisionist History on Data and Trade Agreements*
- Exhibit 127: Law360, *USTR's Retreat from Digital Trade Talks Confounds Attorneys*
- Exhibit 128: Lawfare, *Trusted Cross-Border Data Flows – A National Security Priority*
- Exhibit 129: Business Roundtable, *Business Roundtable Calls For Reset on Trade*
- Exhibit 130: CTA, *Why is US Trade Representative Working against American Business?*
- Exhibit 131: US Aerospace Industry, *US Jobs and Export Figures*
- Exhibit 132: US Automotive Industry, *US Jobs and Export Figures*
- Exhibit 133: US Financial Industry, *US Jobs and Export Figures*
- Exhibit 134: US Film & Television Industry, *US Jobs and Export Figures*
- Exhibit 135: US Medical Device Industry, *US Jobs and Export Figures*
- Exhibit 136: US Biopharmaceutical Industry, *US Jobs and Export Figures*
- Exhibit 137: US Semiconductor Industry, *US Jobs and Export Figures*
- Exhibit 138: Bureau of Economic Analysis, *US Digital Economy – New & Revised Estimates 2017-22*
- Exhibit 139: Bureau of Economic Analysis, *New and Revised Statistics of the Digital Economy 2005-21*
- Exhibit 140: AAIP, *Digital Trade – The IPEF Keystone*
- Exhibit 141: Wilson Center, *The Indo-Pacific Region Needs a Comprehensive Trade Agenda*
- Exhibit 142: CSIS, *The Indo-Pacific Economic Framework & Digital Trade in Southeast Asia*
- Exhibit 143: CSIS, *Filling in the Indo-Pacific Economic Framework*
- Exhibit 144: Progressive Policy Institute, *Digital Trade 2023*
- Exhibit 145: Brookings, *An American Strategy for the Indo-Pacific in an Age of US-China Competition*
- Exhibit 146: American Leadership Initiative, *A Worker-Centric Digital Trade Agenda*
- Exhibit 147: American Leadership Initiative, *America Must be the Standards Setter in the Digital Sphere*
- Exhibit 148: American Leadership Initiative, *Advancing Digital Governance with the Pacific and Europe*

- Exhibit 149: American Leadership Initiative, *A Global Digital Strategy for America*
- Exhibit 150: American Leadership Initiative, *US Digital Leadership is Vital for Women-Owned Businesses*
- Exhibit 151: East Asia Forum, *The High Stakes Indo-Pacific Economic Framework*
- Exhibit 152: Third Way, *Supply Chains and Value Chains Explained*
- Exhibit 153: Third Way, *Five Things to Know about the IPEF*
- Exhibit 154: Council on Foreign Relations, *Unpacking the IPEF*
- Exhibit 155: Atlantic Council, *Experts React – Biden’s New Indo-Pacific Economic Framework*

EXHIBIT 1



GDA TESTIMONY ON SUPPLY CHAIN RESILIENCE

USTR SOLICITATION OF COMMENTS ON *PROMOTING SUPPLY CHAIN RESILIENCE*

May 3, 2024

GDA Testimony on Promoting Supply Chain Resilience (Docket Number USTR–2024–0002)

The Global Data Alliance (GDA)¹ appreciates the opportunity to testify at today’s hearing organized by the Office of the US Trade Representative (USTR) to discuss supply chain resilience.

The GDA is a cross-industry coalition of companies, headquartered in the United States and allied nations, that are committed to high standards of data responsibility and that rely on the ability to access and transfer information across borders to innovate and create jobs in the United States. GDA member companies are active in many sectors of the economy and support millions of jobs across all 50 US states.

The GDA welcomes USTR’s recognition that the United States must maintain close and productive economic relationships with its trusted allies to achieve supply chain resilience. The GDA focuses its comments on the critical importance of maintaining cross-border access to knowledge, ideas, and information as a core feature of a deliberate US government approach to supply chain resilience.

USTR’s efforts to collaborate with allied partners and to engage in near-shoring and friend-shoring will only succeed if the United States and its allies trust one another and work together. This requires – among other things – a posture of openness and a willingness not to impose cross-border data restrictions on one another for arbitrary, discriminatory, disguised, or unnecessary reasons. To permit trusted US allies to impose such restrictions on the United States would be antithetical to the notion of collaboration on supply chain resilience.

The GDA welcomes a deliberate Administration effort to advance supply chain resilience through collaboration and information exchange with allies. For example, in the Indo-Pacific region, this approach should be aligned with the whole-of-government commitment reflected in: (1) the US Indo-Pacific Strategy goals of a “free and open Indo-Pacific” that include norms to “govern our digital economies and cross-border data flows according to open principles”; (2) the White House IPEF promise to achieve “high-standard rules of the road in the digital economy, including standards on cross-border data flows and data localization”; and (3) the IPEF [Ministerial Statement](#) aim to “enhance access to online information and use of the Internet; facilitate digital trade; address discriminatory practices,” and “work to promote and support... trusted and secure cross-border data flows.”²

This whole-of-government commitment is important because the exchange of knowledge, ideas, and information with our trusted US allies – not only in the Indo-Pacific, but also across the Americas, Europe, Africa, and the Middle – supports the stated goals of the supply chain resilience Federal Register Notice. This includes:

- Improving cybersecurity, data security, and privacy;
- Combatting corruption, money laundering, terrorist financing, and financial fraud;
- Growing economic opportunity and financial and digital inclusion for all Americans
- Supporting human rights and labor rights – while combatting digital authoritarianism;
- Promoting science and innovation;
- Supporting transparency and good regulatory practices;
- Protecting the environment via better carbon tracking and improved climate change mitigation; and
- A wide array of other core US government interests relating to supply chain resilience.³

Conversely, permitting US allies to impose arbitrary, discriminatory, disguised, or unnecessary cross-border data restrictions on the United States would undermine US supply chain resilience for several reasons:

First, cross-border access to data and digital tools supports the resilience of the US workforce and the US supply chain, which increasingly depends on the integration of AI- and other software-based tools necessary to compete globally and support well-paid jobs in advanced manufacturing, precision agriculture, and skilled services. These tools – used in sectors including the automotive, aerospace, clean energy, civil engineering, construction, farming, film production, telecom, transport, and many other sectors – depend upon cross-border access to information used to enhance US-based R&D, market forecasting, manufacturing, sourcing, logistics, sales, and service processes. For example, so-called “Digital Twins” technology, which is particularly cross-border data-dependent, allows US companies to build, simulate, and measure performance in a virtual setting of their US factories, products and services, significantly enhancing the competitive position of these production sites vis-à-vis overseas peers. In this and many other contexts, without reliable access to such data, the US workforce will be a significant competitive disadvantage, frustrating efforts to grow American manufacturing and service jobs.

Second, foreign cross-border data restrictions hurt US workers (and families and communities) that depend upon digitally-enabled or digitally-delivered exports from the United States.⁴ Some 40 million US jobs depend on international trade; 16 million US jobs are in software-related fields; and roughly 4 million new US manufacturing jobs are anticipated in the coming years.⁵ US supply chain resilience is also threatened by trading partner imposition of customs duties on US digital exports. The impacts of such restrictions would be borne not only by American workers in semiconductors, pharmaceuticals, and other integrated supply chains, but also by artists, musicians, performers, writers, photographers, software coders, and many other creators in the graphic arts, film, music, publishing, and software sectors.⁶

Third, such restrictions also undermine efforts to increase diversity in resilient supply chains – harming diverse communities across the United States and beyond. As the United Nations has stated, “regulatory fragmentation in the digital landscape...is most likely to adversely impact ... less well-off individuals, and marginalized communities the world over, as well as worsen structural discrimination against women.”⁷

Fourth, and more broadly, macro- and micro-economic analyses performed by the WTO, World Bank, IMF, OECD, and independent economists show that foreign cross-border data restrictions also harm GDP (minus 0.7-1.7%); investment flows (minus 4%); productivity (4.5% loss); small business (up to 80% higher trade costs); and the US tax base.⁸ As the World Bank has noted, “[r]estrictions on data flows have large negative consequences on the productivity of local companies.”

Fifth, US supply chain resilience – and US national security – depend heavily on agreeing with allies on cross-border data norms. This perspective is articulated clearly and explicitly in the National Security Strategy and the National Cybersecurity Strategy. Failure to agree on such norms with US allies brings risk: If the United States doesn’t set

such rules with its allies, then US adversaries will fill the vacuum. Those governments will be free to replace norms that include the United States, US values, and US law with new agreements that exclude the United States and hurt American interests and citizens.⁹

For the foregoing reasons, it is critical to US supply chain resilience that USTR reengage and negotiate with its allies to – among other things – safeguard US and allied cross-border exchange and mutual access to knowledge, information, and data. Thank you for the opportunity to testify today. I look forward to your questions.

¹ GDA member companies are active in the accounting, agriculture, automotive, aerospace and aviation, biopharmaceutical, consumer goods, energy, film and television, finance, healthcare, hospitality, insurance, manufacturing, medical device, natural resources, publishing, semiconductor, software, supply chain, telecommunications, and transportation sectors. GDA member companies have operations and support millions of jobs across all 50 US states. For more information, see <https://www.globaldataalliance.org>

² See generally, Global Data Alliance, *Cross-Border Exchange of Information with US Allies under the Indo-Pacific Economic Framework*, Submission to White House (Dec. 5, 2023), at: <https://globaldataalliance.org/wp-content/uploads/2023/12/12052023gdawhitehouseipef.pdf>

³ See generally, Global Data Alliance website, *GDA Issue Briefs on Cybersecurity, Data Analytics, Economic Development, Environmental Sustainability, Innovation, Regulatory Compliance, Privacy, and Small Business* (2024), at: <https://globaldataalliance.org/issues/>; See also Global Data Alliance website, *GDA Sector Briefs on Agriculture, Automotive, Biopharmaceutical R&D, Energy, Finance, Healthcare, Media & Publishing, Medical Technology, Supply Chain, and Telecommunications* (2024), at: <https://globaldataalliance.org/issues/>, at: <https://globaldataalliance.org/sectors/>; Global Data Alliance, *Cross-Border Access to Information and Data Transfers Support US Government Priorities* (2023), at: <https://globaldataalliance.org/wp-content/uploads/2023/11/11212023gdaustrback.pdf>

⁴ See generally, Global Data Alliance, *GDA Comments on Worker-Centered Trade Policy* (2023), <https://globaldataalliance.org/wp-content/uploads/2023/09/09252023gdaworktradepolicy.pdf>

⁵ See e.g., Business Roundtable, *Trade Supports over 40 Million American Jobs* (2020), at: <https://www.businessroundtable.org/new-study-trade-supported-over-40-million-american-jobs>; Software.org – The BSA Foundation, *Software – Supporting US Through COVID* (2020), at: <https://software.org/wp-content/uploads/2021SoftwareJobs.pdf>; National Association of Manufacturers, *US Manufacturing Could Need up to 3.8 million workers* (2024), at: <https://nam.org/study-manufacturing-in-u-s-could-need-up-to-3-8-million-workers-30626/>; US Chamber of Commerce, *How US Workers and Companies Benefit from Digital Trade* (2024), at: https://www.uschamber.com/assets/documents/USCC_Digital-Trade-Report.pdf

⁶ See Global Data Alliance, *WTO Moratorium on Customs Duties on Electronic Transmissions – Statistical Summary* (2024), at: <https://globaldataalliance.org/wp-content/uploads/2024/02/02222024gdawtostatsum.pdf>; BSA | The Software Alliance, *Customs Duties on Software and Other US Digital Exports – A Threat to Growth & Innovation* (2019), at: <https://www.bsa.org/files/policy-filings/10182019wtomoratoriumus.pdf>

⁷ See id.

⁸ See generally, Global Data Alliance, *Cross-Border Data Policy Index* (2023), at: <https://globaldataalliance.org/resource/cross-border-data-policy-index/>

⁹ This is no longer a hypothetical concern as reflected in a recent China State Council announcement that capitalizes on the United States' lack of trade policy engagement with US allies on cross-border data policy matters. The State Council announcement is indicative of the cross-border data policy vacuum created by US inaction on digital trade. The announcement calls for the exploration of pilot projects for cross-border data transfers members of the Digital Economy Partnership Agreement (i.e., among Chile, New Zealand, Singapore and South Korea and possibly future DEPA members (e.g., Canada and Costa Rica). The aim is to accelerate the establishment of mechanisms for cooperation regarding cross-border data transfers with the aforementioned economies, and to promote the construction of a multi-level global digital cooperation partnership network with these and other economies. The State Council also calls for the “active promotion of accession to the CPTPP and DEPA”, including the “signing of FTAs with more countries and regions, and expand the network of high-standard free trade areas open to the world.” These initiatives build upon the negotiation of cross-border data policies in the Regional Comprehensive Economic Partnership (RCEP) that broadly support an authoritarian digital governance

model. This RCEP model adopts a self-judging approach to governmental conduct in the digital environment, giving license for Parties to the Agreement to impose arbitrary, discriminatory, disguised, or unnecessary cross-border data restrictions at will. See https://www.gov.cn/zhengce/content/202403/content_6940154.htm

EXHIBIT 2



THE WHITE HOUSE
WASHINGTON

March 1, 2023

Digital technologies today touch nearly every aspect of American life. The openness and connection enabled by access to the Internet are game-changers for communities everywhere, as we have all experienced throughout the COVID-19 pandemic. That's why, thanks to the Bipartisan Infrastructure Law, my Administration is investing \$65 billion to make sure every American has access to reliable, high-speed Internet. And when we pick up our smart phones to keep in touch with loved ones, log on to social media to share our ideas with one another, or connect to the Internet to run a business or take care of any of our basic needs, we need to be able to trust that the underlying digital ecosystem is safe, reliable, and secure. This National Cybersecurity Strategy details the comprehensive approach my Administration is taking to better secure cyberspace and ensure the United States is in the strongest possible position to realize all the benefits and potential of our digital future.

Cybersecurity is essential to the basic functioning of our economy, the operation of our critical infrastructure, the strength of our democracy and democratic institutions, the privacy of our data and communications, and our national defense. From the very beginning of my Administration, we have moved decisively to strengthen cybersecurity. I appointed senior cybersecurity officials at the White House and issued an Executive Order on Improving the Nation's Cybersecurity. Working in close cooperation with the private sector, my Administration has taken steps to protect the American people from hackers, hold bad actors and cybercriminals accountable, and defend against the increasingly malicious cyber campaigns targeting our security and privacy. And we've worked with our allies and partners around the world to improve our capacity to collectively defend against and respond to cyber threats from authoritarian states that go against our national interests.

This strategy recognizes that robust collaboration, particularly between the public and private sectors, is essential to securing cyberspace. It also takes on the systemic challenge that too much of the responsibility for cybersecurity has fallen on individual users and small organizations. By working in partnership with industry; civil society; and State, local, Tribal, and territorial governments, we will rebalance the responsibility for cybersecurity to be more effective and more equitable. We will realign incentives to favor long-term investments in security, resilience, and promising new technologies. We will collaborate with our allies and partners to strengthen norms of responsible state behavior, hold countries accountable for irresponsible behavior in cyberspace, and disrupt the networks of criminals behind dangerous cyberattacks around the globe. And we will work with the Congress to provide the resources and tools necessary to ensure effective cybersecurity practices are implemented across our most critical infrastructure.

As I have often said, our world is at an inflection point. That includes our digital world. The steps we take and choices we make today will determine the direction of our world for decades

to come. This is particularly true as we develop and enforce rules and norms for conduct in cyberspace. We must ensure the Internet remains open, free, global, interoperable, reliable, and secure—anchored in universal values that respect human rights and fundamental freedoms. Digital connectivity should be a tool that uplifts and empowers people everywhere, not one used for repression and coercion. As this strategy details, the United States is prepared to meet this challenge from a position of strength, leading in lockstep with our closest allies and working with partners everywhere who share our vision for a brighter digital future.

A handwritten signature in black ink, appearing to read "J. S. S. S.", written in a cursive style.



TABLE OF CONTENTS

INTRODUCTION	1
PILLAR ONE DEFEND CRITICAL INFRASTRUCTURE	7
PILLAR TWO DISRUPT AND DISMANTLE THREAT ACTORS.....	14
PILLAR THREE SHAPE MARKET FORCES TO DRIVE SECURITY AND RESILIENCE.....	19
PILLAR FOUR INVEST IN A RESILIENT FUTURE.....	23
PILLAR FIVE FORGE INTERNATIONAL PARTNERSHIPS TO PURSUE SHARED GOALS	29
IMPLEMENTATION	34



PILLAR FIVE | FORGE INTERNATIONAL PARTNERSHIPS TO PURSUE SHARED GOALS

The United States seeks a world where responsible state behavior in cyberspace is expected and rewarded and where irresponsible behavior is isolating and costly. To achieve this goal, we will continue to engage with countries working in opposition to our larger agenda on common problems while we build a broad coalition of nations working to maintain an open, free, global, interoperable, reliable, and secure Internet.

For decades, we have worked through international institutions to define and advance responsible state behavior in cyberspace. We have used multilateral processes such as the United Nations (UN) Group of Governmental Experts and Open-Ended Working Group to develop a framework that includes a set of peacetime norms and confidence-building measures, which all UN member states have affirmed in the UN General Assembly. We have supported the expansion of the Budapest Convention on Cybercrime and other global efforts to make cyberspace more secure. We will continue these efforts while recognizing the need to work with partners to thwart the dark vision for the future of the Internet that the PRC and other autocratic governments promote. We will do so by demonstrating to economies and societies the value of openness and jointly imposing consequences for behavior that runs counter to agreed norms of state behavior.

To counter common threats, preserve and reinforce global Internet freedom, protect against transnational digital repression, and build toward a shared digital ecosystem that is more inherently resilient and defensible, the United States will work to scale the emerging model of collaboration by national cybersecurity stakeholders to cooperate with the international community. We will expand coalitions, collaboratively disrupt transnational criminals and other malicious cyber actors, build the capacity of our international allies and partners, reinforce the applicability of existing international law to state behavior in cyberspace, uphold globally accepted and voluntary norms of responsible state behavior in peacetime, and punish those that engage in disruptive, destructive, or destabilizing malicious cyber activity.

STRATEGIC OBJECTIVE 5.1: BUILD COALITIONS TO COUNTER THREATS TO OUR DIGITAL ECOSYSTEM

In April 2022, the United States and 60 countries launched the Declaration for the Future of the Internet (DFI), bringing together a broad, diverse coalition of partners—the largest of its kind—around a common, democratic vision for an open, free, global, interoperable, reliable, and secure digital future. Through the DFI, the Freedom Online Coalition, and other partnerships and mechanisms, the United States is rallying like-minded countries, the international business community, and other stakeholders to advance our vision for the future of the Internet that



promotes secure and trusted data flows, respects privacy, promotes human rights, and enables progress on broader challenges.

Through mechanisms like the Quadrilateral Security Dialogue (“the Quad”) between the United States, India, Japan, and Australia, the United States and its international allies and partners are advancing these shared goals for cyberspace. These include improving information sharing between computer emergency response teams and the development of a digital ecosystem based on shared values. The Indo-Pacific Economic Framework for Prosperity (IPEF) and the Americas Partnership for Economic Prosperity (APEP) create opportunities for the United States and regional governments to collaborate in setting rules of the road for the digital economy, including facilitating the development of technical standards, mechanisms to enable cross-border data flows that protect privacy while avoiding strict data localization requirements, and actions to foster supply chain security and resilience. Through the U.S.-EU Trade and Technology Council (TTC), we are coordinating across the Atlantic to combat shared threats and demonstrate how market approaches to digital trade, technology, and innovation can improve the lives of our citizens and be a force for greater prosperity. The United States is also working closely with Australia and the United Kingdom through the trilateral security and technology pact (“AUKUS”) to secure critical technologies, improve cyber coordination, and share advanced capabilities.

Through these and other partnerships, the United States and international counterparts can advance common cybersecurity interests by sharing cyber threat information, exchanging model cybersecurity practices, comparing sector-specific expertise, driving secure-by-design principles, and coordinating policy and incident response activities. Furthermore, multistakeholder partnerships and coalitions that also include private sector and civil society organizations, such as the Christchurch Call to Action to Eliminate Terrorist and Violent Extremist Content Online, the Freedom Online Coalition, and the Global Partnership for Action on Gender-Based Online Harassment and Abuse, are crucial to tackling systemic issues. We will leverage these partnerships to enable effective operational collaboration to defend our shared digital ecosystem. We will also support and help build, as needed, new and innovative partnerships—as in the case of the international Counter-Ransomware Initiative—that bring together unique collections of stakeholders to address new and emerging cybersecurity challenges.

Because most malicious cyber activity targeting the United States is carried out by actors based in foreign countries or using foreign computing infrastructure, we must strengthen the mechanisms we have to collaborate with our allies and partners so that no adversary can evade the rule of law. The United States will work with its allies and partners to develop new collaborative law enforcement mechanisms for the digital age. For example, the European Cybercrime Centre has played a vital role in modernizing legal frameworks, training law enforcement, improving attribution, collaborating with private sector partners, and responding to malicious cyber activities in Europe. To extend this model, we will support efforts to build effective hubs with partners in other regions.



STRATEGIC OBJECTIVE 5.2: STRENGTHEN INTERNATIONAL PARTNER CAPACITY

As we build a coalition to advance shared cybersecurity priorities and promote a common vision for the digital ecosystem, the United States will strengthen the capacity of like-minded states across the globe to support these goals. We must enable our allies and partners to secure critical infrastructure networks, build effective incident detection and response capabilities, share cyber threat information, pursue diplomatic collaboration, build law enforcement capacity and effectiveness through operational collaboration, and support our shared interests in cyberspace by adhering to international law and reinforcing norms of responsible state behavior.

To accomplish this goal, the United States will marshal expertise across agencies, the public and private sectors, and among advanced regional partners to pursue coordinated and effective international cyber capacity-building and operational collaboration efforts. Within the law enforcement community, DOJ will continue to build a more robust cybercrime cooperation paradigm through bilateral and multilateral engagement and agreements, formal and informal cooperation, and providing international and regional leadership to strengthen cybercrime laws, policies, and operations. DoD will continue to strengthen its military-to-military relationships to leverage allies' and partners' unique skills and perspectives while building their capacity to contribute to our collective cybersecurity posture. The Department of State will continue to coordinate whole-of-government efforts to ensure Federal capacity building priorities are strategically aligned and further U.S., allied, and partner interests.

STRATEGIC OBJECTIVE 5.3: EXPAND U.S. ABILITY TO ASSIST ALLIES AND PARTNERS

As recent cyberattacks against Costa Rica, Albania, and Montenegro have demonstrated, allies and partners who fall victim to a significant cyberattack may seek support from the United States and allied and partner nations to investigate, responding to, and recover from such incidents. Providing this support will not only assist with partner recovery and response, but will also advance U.S. foreign policy and cybersecurity goals. Close cooperation with an affected ally or partner demonstrates solidarity in the face of adversary activity and can accelerate efforts to expose counter-normative state behavior and impose consequences.

The Administration will establish policies for determining when it is in the national interest to provide such support, develop mechanisms for identifying and deploying department and agency resources in such efforts, and, where needed, rapidly seek to remove existing financial and procedural barriers to provide such operational support. As one example, the United States is leading a North Atlantic Treaty Organization (NATO) effort to build a virtual cyber incident



support capability that enables Allies to more effectively and efficiently support each other in response to significant malicious cyber activities.

STRATEGIC OBJECTIVE 5.4: BUILD COALITIONS TO REINFORCE GLOBAL NORMS OF RESPONSIBLE STATE BEHAVIOR

Every member of the United Nations has made a political commitment to endorse peacetime norms of responsible state behavior in cyberspace that includes refraining from cyber operations that would intentionally damage critical infrastructure contrary to their obligations under international law. While our adversaries know that such commitments are not self-enforcing, the growing influence of this framework has led states to call out those who act contrary to it. Increasingly, a community of nations has collaborated to produce coordinated statements of attribution that carry the simultaneous diplomatic condemnation of many governments and strengthening the coalition committed to a stable cyberspace.

The United States, as a core part of its renewed, active diplomacy, will hold irresponsible states accountable when they fail to uphold their commitments. To effectively constrain our adversaries and counter malicious activities below the threshold of armed conflict, we will work with our allies and partners to pair statements of condemnation with the imposition of meaningful consequences. These efforts will require collaborative use of all tools of statecraft, including diplomatic isolation, economic costs, counter-cyber and law enforcement operations, or legal sanctions, among others.

STRATEGIC OBJECTIVE 5.5: SECURE GLOBAL SUPPLY CHAINS FOR INFORMATION, COMMUNICATIONS, AND OPERATIONAL TECHNOLOGY PRODUCTS AND SERVICES

Complex and globally interconnected supply chains produce the information, communications, and operational technology products and services that power the U.S. economy. From raw materials and basic components to finished products and services—both virtual and physical—we depend upon a growing network of foreign suppliers. This dependency on critical foreign products and services from untrusted suppliers introduces multiple sources of systemic risk to our digital ecosystem. Mitigating this risk will require long-term, strategic collaboration between public and private sectors at home and abroad to rebalance global supply chains and make them more transparent, secure, resilient, and trustworthy.

Critical inputs, components, and systems must increasingly be developed at home or in close coordination with allies and partners who share our vision of an open, free, global, interoperable, reliable, and secure Internet. Building on the National Strategy to Secure 5G, we are working with our partners to develop secure, reliable, and trustworthy supply chains for 5G and next-generation



wireless networks including through Open Radio Access Networks (Open RAN) and collaborative initiatives to diversify suppliers. Such efforts include DoD testing of Open RAN implementations across multiple bases, with multi-million dollar smart warehouse and logistics projects, and National Telecommunications and Information Administration’s (NTIA) work to catalyze the development and adoption of open, interoperable, and standards-based networks through the Public Wireless Supply Chain Innovation Fund. Extending this model to other critical technologies will require long-term, strategic collaboration between public and private sectors at home and abroad to rebalance global supply chains and make them more secure, resilient, and trustworthy. The Bipartisan Infrastructure Law mandates “Build America, Buy America” for Federally-funded projects, including for digital infrastructure. Through EO 14017, “America’s Supply Chains,” the CHIPS and Science Act, and the Inflation Reduction Act, the Federal Government has introduced new industrial and innovation strategy tools to help restore production of critical goods to the United States and its close partners while securing our information technology and advanced manufacturing supply chains.

The United States will work with our allies and partners, including through regional partnerships like IPEF, the Quad Critical and Emerging Technology Working Group, and the TTC, to identify and implement best practices in cross-border supply chain risk management and work to shift supply chains to flow through partner countries and trusted vendors. This effort will prioritize opportunities to provide higher levels of assurance that digital technologies will function as expected and to attract countries to support the shared vision of an open, free, global, interoperable, reliable, and secure Internet. The Department of State will further accelerate these efforts through the new International Technology Security and Innovation Fund to support the creation of secure and diverse supply chains for semiconductors and telecommunications. Finally, through implementation of EO 13873, “Securing the Information and Communications Technology and Services Supply Chain,” as well as EO 14034 “Protecting Americans’ Sensitive Data From Foreign Adversaries,” we will work to prevent unacceptable and undue risks to our national security from information and communications technology and services subject to control or influence from adversarial governments.

EXHIBIT 3



THE WHITE HOUSE
WASHINGTON

October 12, 2022

From the earliest days of my Presidency, I have argued that our world is at an inflection point. How we respond to the tremendous challenges and the unprecedented opportunities we face today will determine the direction of our world and impact the security and prosperity of the American people for generations to come. The 2022 National Security Strategy outlines how my Administration will seize this decisive decade to advance America's vital interests, position the United States to outmaneuver our geopolitical competitors, tackle shared challenges, and set our world firmly on a path toward a brighter and more hopeful tomorrow.

Around the world, the need for American leadership is as great as it has ever been. We are in the midst of a strategic competition to shape the future of the international order. Meanwhile, shared challenges that impact people everywhere demand increased global cooperation and nations stepping up to their responsibilities at a moment when this has become more difficult. In response, the United States will lead with our values, and we will work in lockstep with our allies and partners and with all those who share our interests. We will not leave our future vulnerable to the whims of those who do not share our vision for a world that is free, open, prosperous, and secure. As the world continues to navigate the lingering impacts of the pandemic and global economic uncertainty, there is no nation better positioned to lead with strength and purpose than the United States of America.

From the moment I took the oath of office, my Administration has focused on investing in America's core strategic advantages. Our economy has added 10 million jobs and unemployment rates have reached near record lows. Manufacturing jobs have come racing back to the United States. We're rebuilding our economy from the bottom up and the middle out. We've made a generational investment to upgrade our Nation's infrastructure and historic investments in innovation to sharpen our competitive edge for the future. Around the world, nations are seeing once again why it's never a good bet to bet against the United States of America.

We have also reinvigorated America's unmatched network of alliances and partnerships to uphold and strengthen the principles and institutions that have enabled so much stability, prosperity, and growth for the last 75 years. We have deepened our core alliances in Europe and the Indo-Pacific. NATO is stronger and more united than it has ever been, as we look to welcome two capable new allies in Finland and Sweden. We are doing more to connect our partners and strategies across regions through initiatives like our security partnership with Australia and the United Kingdom (AUKUS). And we are forging creative new ways to work in common cause with partners around issues of shared interest, as we are with the European Union, the Indo-Pacific Quad, the Indo-Pacific Economic Framework, and the Americas Partnership for Economic Prosperity.

These partnerships amplify our capacity to respond to shared challenges and take on the issues that directly impact billions of people's lives. If parents cannot feed their children, nothing else matters. When countries are repeatedly ravaged by climate disasters, entire futures are wiped out. And as we have all experienced, when pandemic diseases proliferate and spread, they can worsen inequities and bring the entire world to a standstill. The United States will continue to prioritize leading the international response to these transnational challenges, together with our partners, even as we face down concerted efforts to remake the ways in which nations relate to one another.

In the contest for the future of our world, my Administration is clear-eyed about the scope and seriousness of this challenge. The People's Republic of China harbors the intention and, increasingly, the capacity to reshape the international order in favor of one that tilts the global playing field to its benefit, even as the United States remains committed to managing the competition between our countries responsibly. Russia's brutal and unprovoked war on its neighbor Ukraine has shattered peace in Europe and impacted stability everywhere, and its reckless nuclear threats endanger the global non-proliferation regime. Autocrats are working overtime to undermine democracy and export a model of governance marked by repression at home and coercion abroad.

These competitors mistakenly believe democracy is weaker than autocracy because they fail to understand that a nation's power springs from its people. The United States is strong abroad because we are strong at home. Our economy is dynamic. Our people are resilient and creative. Our military remains unmatched—and we will keep it that way. And it is our democracy that enables us to continually reimagine ourselves and renew our strength.

So, the United States will continue to defend democracy around the world, even as we continue to do the work at home to better live up to the idea of America enshrined in our founding documents. We will continue to invest in boosting American competitiveness globally, drawing dreamers and strivers from around the world. We will partner with any nation that shares our basic belief that the rules-based order must remain the foundation for global peace and prosperity. And we will continue to demonstrate how America's enduring leadership to address the challenges of today and tomorrow, with vision and clarity, is the best way to deliver for the American people.

This is a 360-degree strategy grounded in the world as it is today, laying out the future we seek, and providing a roadmap for how we will achieve it. None of this will be easy or without setbacks. But I am more confident than ever that the United States has everything we need to win the competition for the 21st century. We emerge stronger from every crisis. There is nothing beyond our capacity. We can do this—for our future and for the world.

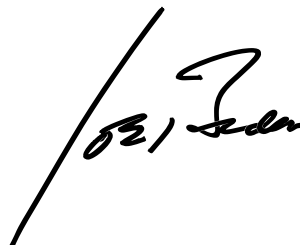
A handwritten signature in black ink, appearing to read "Joe Biden". The signature is written in a cursive style with a large, sweeping initial "J".



Table of Contents

PART I: THE COMPETITION FOR WHAT COMES NEXT	6
Our Enduring Vision	6
Our Enduring Role.....	7
The Nature of the Competition Between Democracies and Autocracies	8
Cooperating to Address Shared Challenges in an Era of Competition.....	9
Overview of Our Strategic Approach	10
PART II: INVESTING IN OUR STRENGTH.....	14
Investing in Our National Power to Maintain a Competitive Edge	14
Implementing a Modern Industrial and Innovation Strategy.....	14
Investing In Our People.....	15
Strengthening Our Democracy	16
Using Diplomacy to Build the Strongest Possible Coalitions.....	16
Transformative Cooperation.....	16
An Inclusive World	18
A Prosperous World	19
Modernizing and Strengthening Our Military.....	20
PART III: OUR GLOBAL PRIORITIES	23
Out-Competing China and Constraining Russia	23
China.....	23
Russia.....	25
Cooperating on Shared Challenges	27
Climate and Energy Security.....	27
Pandemics and Biodefense	28
Food Insecurity	29
Arms Control and Non-Proliferation.....	29
Terrorism	30
Shaping the Rules of the Road	32
Technology	32
Securing Cyberspace	34
Trade and Economics	34
PART IV: OUR STRATEGY BY REGION	37



Promote a Free and Open Indo-Pacific	37
Deepen Our Alliance with Europe	38
Foster Democracy and Shared Prosperity in the Western Hemisphere	40
Support De-Escalation and Integration in the Middle East.....	42
Build 21st Century U.S.-Africa Partnerships	43
Maintain a Peaceful Arctic.....	44
Protect Sea, Air, and Space	45
PART V: CONCLUSION.....	47



PART I: THE COMPETITION FOR WHAT COMES NEXT

“The world is changing. We’re at a significant inflection point in world history. And our country and the world—the United States of America has always been able to chart the future in times of great change. We’ve been able to constantly renew ourselves. And time and again, we’ve proven there’s not a single thing we cannot do as a nation when we do it together—and I mean that—not a single solitary thing.”

PRESIDENT JOSEPH R. BIDEN, JR

United States Coast Guard Academy's 140th Commencement Exercises

Our Enduring Vision

We are now in the early years of a decisive decade for America and the world. The terms of geopolitical competition between the major powers will be set. The window of opportunity to deal with shared threats, like climate change, will narrow drastically. The actions we take now will shape whether this period is known as an age of conflict and discord or the beginning of a more stable and prosperous future.

We face two strategic challenges. The first is that the post-Cold War era is definitively over and a competition is underway between the major powers to shape what comes next. No nation is better positioned to succeed in this competition than the United States, as long as we work in common cause with those who share our vision of a world that is free, open, secure, and prosperous. This means that the foundational principles of self-determination, territorial integrity, and political independence must be respected, international institutions must be strengthened, countries must be free to determine their own foreign policy choices, information must be allowed to flow freely, universal human rights must be upheld, and the global economy must operate on a level playing field and provide opportunity for all.

The second is that while this competition is underway, people all over the world are struggling to cope with the effects of shared challenges that cross borders—whether it is climate change, food insecurity, communicable diseases, terrorism, energy shortages, or inflation. These shared challenges are not marginal issues that are secondary to geopolitics. They are at the very core of national and international security and must be treated as such. By their very nature, these challenges require governments to cooperate if they are to solve them. But we must be clear-eyed that we will have to tackle these challenges within a competitive international environment where heightening geopolitical competition, nationalism and populism render this cooperation even more difficult and will require us to think and act in new ways.



This National Security Strategy lays out our plan to achieve a better future of a free, open, secure, and prosperous world. Our strategy is rooted in our national interests: to protect the security of the American people; to expand economic prosperity and opportunity; and to realize and defend the democratic values at the heart of the American way of life. We can do none of this alone and we do not have to. Most nations around the world define their interests in ways that are compatible with ours. We will build the strongest and broadest possible coalition of nations that seek to cooperate with each other, while competing with those powers that offer a darker vision and thwarting their efforts to threaten our interests.

Our Enduring Role

The need for a strong and purposeful American role in the world has never been greater. The world is becoming more divided and unstable. Global increases in inflation since the COVID-19 pandemic began have made life more difficult for many. The basic laws and principles governing relations among nations, including the United Nations Charter and the protection it affords all states from being invaded by their neighbors or having their borders redrawn by force, are under attack. The risk of conflict between major powers is increasing. Democracies and autocracies are engaged in a contest to show which system of governance can best deliver for their people and the world. Competition to develop and deploy foundational technologies that will transform our security and economy is intensifying. Global cooperation on shared interests has frayed, even as the need for that cooperation takes on existential importance. The scale of these changes grows with each passing year, as do the risks of inaction.

Although the international environment has become more contested, the United States remains the world's leading power. Our economy, our population, our innovation, and our military power continue to grow, often outpacing those of other large countries. Our inherent national strengths—the ingenuity, creativity, resilience, and determination of the American people; our values, diversity, and democratic institutions; our technological leadership and economic dynamism; and our diplomatic corps, development professionals, intelligence community, and our military—remain unparalleled. We are experienced in using and applying our power in combination with our allies and partners who add significantly to our own strengths. We have learned lessons from our failures as well as our successes. The idea that we should compete with major autocratic powers to shape the international order enjoys broad support that is bipartisan at home and deepening abroad.

The United States is a large and diverse democracy, encompassing people from every corner of the world, every walk of life, every system of belief. This means that our politics are not always smooth—in fact, they're often the opposite. We live at a moment of passionate political intensities and ferment that sometimes tears at the fabric of the nation. But we don't shy away from that fact or use it as an excuse to retreat from the wider world. We will continue to reckon openly and humbly with our divisions and we will work through our politics transparently and democratically. We know that for all of the effort that it takes, our democracy is worth it. It is the only way to ensure that people are truly able to live lives of dignity and freedom. This American project will never be complete—democracy is always a work in progress—but that will not stop us from defending our values and continuing to pursue our national security interests in the world. The quality of our democracy at home affects the strength and credibility of our leadership abroad—just as the character of the world we inhabit affects our ability to enjoy security, prosperity, and freedom at home.



Our rivals' challenges are profound and mounting. Their problems, at both home and abroad, are associated with the pathologies inherent in highly personalized autocracies and are less easily remedied than ours. Conversely, the United States has a tradition of transforming both domestic and foreign challenges into opportunities to spur reform and rejuvenation at home. This is one reason that prophecies of American decline have repeatedly been disproven in the past—and why it has never been a good bet to bet against America. We have always succeeded when we embrace an affirmative vision for the world that addresses shared challenges and combine it with the dynamism of our democracy and the determination to out-compete our rivals.

The Nature of the Competition Between Democracies and Autocracies

The range of nations that supports our vision of a free, open, prosperous, and secure world is broad and powerful. It includes our democratic allies in Europe and the Indo-Pacific as well as key democratic partners around the world that share much of our vision for regional and international order even if they do not agree with us on all issues, and countries that do not embrace democratic institutions but nevertheless depend upon and support a rules-based international system.

Americans will support universal human rights and stand in solidarity with those beyond our shores who seek freedom and dignity, just as we continue the critical work of ensuring equity and equal treatment under law at home. We will work to strengthen democracy around the world because democratic governance consistently outperforms authoritarianism in protecting human dignity, leads to more prosperous and resilient societies, creates stronger and more reliable economic and security partners for the United States, and encourages a peaceful world order. In particular, we will take steps to show that democracies deliver—not only by ensuring the United States and its democratic partners lead on the hardest challenges of our time, but by working with other democratic governments and the private sector to help emerging democracies show tangible benefits to their own populations. We do not, however, believe that governments and societies everywhere must be remade in America's image for us to be secure.

The most pressing strategic challenge facing our vision is from powers that layer authoritarian governance with a revisionist foreign policy. It is their behavior that poses a challenge to international peace and stability—especially waging or preparing for wars of aggression, actively undermining the democratic political processes of other countries, leveraging technology and supply chains for coercion and repression, and exporting an illiberal model of international order. Many non-democracies join the world's democracies in forswearing these behaviors. Unfortunately, Russia and the People's Republic of China (PRC) do not.

Russia and the PRC pose different challenges. Russia poses an immediate threat to the free and open international system, recklessly flouting the basic laws of the international order today, as its brutal war of aggression against Ukraine has shown. The PRC, by contrast, is the only competitor with both the intent to reshape the international order and, increasingly, the economic, diplomatic, military, and technological power to advance that objective.

Just as the United States and countries around the world benefited greatly from the post-Cold War international order, so too did the PRC and Russia. The PRC's economy and geopolitical influence grew rapidly. Russia joined the G8 and G20 and recovered economically in the 2000s. And yet, they concluded that the success of a free and open rules-based international order posed a threat to their regimes and stifled their ambitions. In their own ways, they now seek to remake



the international order to create a world conducive to their highly personalized and repressive type of autocracy.

Their pursuit of this vision is complicated by several factors. The PRC's assertive behavior has caused other countries to push back and defend their sovereignty, for their own, legitimate reasons. The PRC also retains common interests with other countries, including the United States, because of various interdependencies on climate, economics, and public health. Russia's strategic limitations have been exposed following its war of aggression against Ukraine. Moscow also has some interest in cooperation with countries that do not share its vision, especially in the global south. As a result, the United States and our allies and partners have an opportunity to shape the PRC and Russia's external environment in a way that influences their behavior even as we compete with them.

Some parts of the world are uneasy with the competition between the United States and the world's largest autocracies. We understand these concerns. We also want to avoid a world in which competition escalates into a world of rigid blocs. We do not seek conflict or a new Cold War. Rather, we are trying to support every country, regardless of size or strength, in exercising the freedom to make choices that serve their interests. This is a critical difference between our vision, which aims to preserve the autonomy and rights of less powerful states, and that of our rivals, which does not.

Cooperating to Address Shared Challenges in an Era of Competition

Heightened competition between democracies and autocracies is just one of two critical trends we face. The other is shared challenges—or what some call transnational challenges—that do not respect borders and affect all nations. These two trends affect each other—geopolitical competition changes, and often complicates, the context in which shared challenges can be addressed while those problems often exacerbate geopolitical competition, as we saw with the early phases of the COVID-19 pandemic when the PRC was unwilling to cooperate with the international community. We cannot succeed in our competition with the major powers who offer a different vision for the world if we do not have a plan to work with other nations to deal with shared challenges and we will not be able to do that unless we understand how a more competitive world affects cooperation and how the need for cooperation affects competition. We need a strategy that not only deals with both but recognizes the relationship between them and adjusts accordingly.

Of all of the shared problems we face, climate change is the greatest and potentially existential for all nations. Without immediate global action during this crucial decade, global temperatures will cross the critical warming threshold of 1.5 degrees Celsius after which scientists have warned some of the most catastrophic climate impacts will be irreversible. Climate effects and humanitarian emergencies will only worsen in the years ahead—from more powerful wildfires and hurricanes in the United States to flooding in Europe, rising sea levels in Oceania, water scarcity in the Middle East, melting ice in the Arctic, and drought and deadly temperatures in sub-Saharan Africa. Tensions will further intensify as countries compete for resources and energy advantage—increasing humanitarian need, food insecurity and health threats, as well as the potential for instability, conflict, and mass migration. The necessity to protect forests globally, electrify the transportation sector, redirect financial flows and create an energy revolution to head off the climate crisis is reinforced by the geopolitical imperative to reduce our collective dependence on states like Russia that seek to weaponize energy for coercion.



It is not just climate change. COVID-19 has shown that transnational challenges can hit with the destructive force of major wars. COVID-19 has killed millions of people and damaged the livelihoods of hundreds of millions, if not more. It exposed the insufficiency of our global health architecture and supply chains, widened inequality, and wiped out many years of development progress. It also weakened food systems, brought humanitarian need to record levels, and reinforced the need to redouble our efforts to reduce poverty and hunger and expand access to education in order to get back on track to achieve the Sustainable Development Goals by 2030. Meanwhile, communicable diseases like Ebola continue to reemerge and can only be dealt with if we act early and with other nations. The pandemic has made clear the need for international leadership and action to create stronger, more equitable, and more resilient health systems—so that we can prevent or prepare for the next pandemic or health emergency before it starts.

The global economic challenges resulting from the COVID-19 pandemic have been extended and deepened globally as uneven, recovering demand has outpaced suppliers and put strains on supply chains. Consumers and policymakers the world over have also struggled with surging energy prices and mounting food insecurity, which sharpen security challenges like migration and corruption. Moreover, autocratic governments often abuse the global economic order by weaponizing its interconnectivity and its strengths. They can arbitrarily raise costs by withholding the movement of key goods. They leverage access to their markets and control of global digital infrastructure for coercive purposes. They launder and hide their wealth, often the proceeds of foreign corrupt practices, in major economies through shell and front companies. Nefarious actors—some state sponsored, some not—are exploiting the digital economy to raise and move funds to support illicit weapons programs, terrorist attacks, fuel conflict, and to extort everyday citizens targeted by ransomware or cyber-attacks on national health systems, financial institutions and critical infrastructure. These various factors constrain our policy options, and those of our allies and partners, to advance our security interests and meet the basic needs of our citizens.

We have also experienced a global energy crisis driven by Russia’s weaponization of the oil and gas supplies it controls, exacerbated by OPEC’s management of its own supply. This circumstance underscores the need for an accelerated, just, and responsible global energy transition. That’s why — even as we continue to explore all opportunities with our allies and partners to stabilize energy markets and get supplies to those who need it — we are also focused on implementing the most significant piece of climate legislation in our nation’s history, to bring innovative energy technologies to scale as quickly as possible.

We must work with other nations to address shared challenges to improve the lives of the American people and those of people around the world. We recognize that we will undertake such effort within a competitive environment where major powers will be actively working to advance a different vision. We will use the impulses released by an era of competition to create a race to the top and make progress on shared challenges, whether it is by making investments at home or by deepening cooperation with other countries that share our vision.

Overview of Our Strategic Approach

Our goal is clear—we want a free, open, prosperous, and secure international order. We seek an order that is free in that it allows people to enjoy their basic, universal rights and freedoms. It is open in that it provides all nations that sign up to these principles an opportunity to participate in,



and have a role in shaping, the rules. It is prosperous in that it empowers all nations to continually raise the standard of living for their citizens. And secure, in that it is free from aggression, coercion and intimidation.

Achieving this goal requires three lines of effort. We will: 1) invest in the underlying sources and tools of American power and influence; 2) build the strongest possible coalition of nations to enhance our collective influence to shape the global strategic environment and to solve shared challenges; and 3) modernize and strengthen our military so it is equipped for the era of strategic competition with major powers, while maintaining the capability to disrupt the terrorist threat to the homeland. This is covered in Part II of this strategy.

We will use these capabilities to outcompete our strategic competitors, galvanize collective action on global challenges, and shape the rules of the road for technology, cybersecurity, and trade and economics. This is covered in Part III. Our approach encompasses all elements of national power—diplomacy, development cooperation, industrial strategy, economic statecraft, intelligence, and defense—and is built on several key pillars.

First, we have broken down the dividing line between foreign policy and domestic policy. We understand that if the United States is to succeed abroad, we must invest in our innovation and industrial strength, and build our resilience, at home. Likewise, to advance shared prosperity domestically and to uphold the rights of all Americans, we must proactively shape the international order in line with our interests and values. In a competitive world, where other powers engage in coercive or unfair practices to gain an edge over the United States and our allies, this takes on a special importance. We must complement the innovative power of the private sector with a modern industrial strategy that makes strategic public investments in America’s workforce, and in strategic sectors and supply chains, especially critical and emerging technologies, such as microelectronics, advanced computing, biotechnologies, clean energy technologies, and advanced telecommunications.

Second, our alliances and partnerships around the world are our most important strategic asset and an indispensable element contributing to international peace and stability. A strong and unified NATO, our alliances in the Indo-Pacific, and our traditional security partnerships elsewhere do not only deter aggression; they provide a platform for mutually beneficial cooperation that strengthens the international order. We place a premium on growing the connective tissue—on technology, trade and security—between our democratic allies and partners in the Indo-Pacific and Europe because we recognize that they are mutually reinforcing and the fates of the two regions are intertwined. The United States is a global power with global interests. We are stronger in each region because of our affirmative engagement in the others. If one region descends into chaos or is dominated by a hostile power, it will detrimentally impact our interests in the others.

Third, this strategy recognizes that the PRC presents America’s most consequential geopolitical challenge. Although the Indo-Pacific is where its outcomes will be most acutely shaped, there are significant global dimensions to this challenge. Russia poses an immediate and ongoing threat to the regional security order in Europe and it is a source of disruption and instability globally but it lacks the across the spectrum capabilities of the PRC. We also recognize that other smaller autocratic powers are also acting in aggressive and destabilizing ways. Most notably, Iran interferes in the internal affairs of neighbors, proliferates missiles and drones through proxies, is plotting to harm Americans, including former officials, and is advancing a nuclear program



beyond any credible civilian need. The Democratic People’s Republic of Korea (DPRK) continues to expand its illicit nuclear weapons and missile programs.

Fourth, we will avoid the temptation to see the world solely through the prism of strategic competition and will continue to engage countries on their own terms. We will pursue an affirmative agenda to advance peace and security and to promote prosperity in every region. A more integrated Middle East that empowers our allies and partners will advance regional peace and prosperity, while reducing the resource demands the region makes on the United States over the long term. In Africa, the dynamism, innovation, and demographic growth of the region render it central to addressing complex global problems. The Western Hemisphere directly impacts the United States more than any other region so we will continue to revive and deepen our partnerships there to advance economic resilience, democratic stability, and citizen security.

Fifth, we recognize that globalization has delivered immense benefits for the United States and the world but an adjustment is now required to cope with dramatic global changes such as widening inequality within and among countries, the PRC’s emergence as both our most consequential competitor and one of our largest trading partners, and emerging technologies that fall outside the bounds of existing rules and regulations. We have an affirmative agenda for the global economy to seize the full range of economic benefits of the 21st century while advancing the interests of American workers. Recognizing we have to move beyond traditional Free Trade Agreements, we are charting new economic arrangements to deepen economic engagement with our partners, like the Indo-Pacific Economic Framework for Prosperity (IPEF); a global minimum tax that ensures corporations pay their fair share of tax wherever they are based in the world; the Partnership for Global Investment and Infrastructure (PGII) to help low- and middle-income countries secure high-standard investment for critical infrastructure; updated rules of the road for technology, cyberspace, trade, and economics; and ensuring the transition to clean energy unlocks economic opportunities and good jobs around the world.

Finally, the community of nations that shares our vision for the future of international order is broad and includes countries on every continent. We share in common a desire for relations among nations to be governed by the UN Charter; for the universal rights of all individuals—political, civil, economic, social and cultural—to be upheld; for our environment, air, oceans, space, cyberspace and arteries of international commerce to be protected and accessible for all; and for international institutions, including the United Nations, to be modernized and strengthened to better address global challenges and deliver more tangible benefits for our citizens. The order we seek builds on what came before, but addresses serious shortcomings, new realities, and the attempts by some states to advance a much less free and open model. To preserve and increase international cooperation in an age of competition, we will pursue a dual-track approach. On one track, we will cooperate with any country, including our geopolitical rivals, that is willing to work constructively with us to address shared challenges. We will also fully engage with, and work to strengthen, international institutions. On the other track, we will deepen our cooperation with democracies and other like-minded states. From the Indo-Pacific Quad (Australia, India, Japan, United States) to the U.S.-EU Trade and Technology Council, from AUKUS (Australia, United Kingdom, United States) to I2-U2 (India, Israel, UAE, United States), we are creating a latticework of strong, resilient, and mutually reinforcing relationships that prove democracies can deliver for their people and the world.

The world is now at an inflection point. This decade will be decisive, in setting the terms of our competition with the PRC, managing the acute threat posed by Russia, and in our efforts to deal



with shared challenges, particularly climate change, pandemics, and economic turbulence. If we do not act with urgency and creativity, our window of opportunity to shape the future of international order and tackle shared challenges will close. Those actions must begin with developing the means to execute our strategy, by making renewed investments at home and abroad.



Combatting Transnational Organized Crime

Transnational organized crime impacts a growing number of victims while amplifying other consequential global challenges, from migration to cyber-attacks. Transnational criminal organizations (TCOs) are involved in activities such as the trafficking of drugs and other illicit goods, money laundering, theft, human smuggling and trafficking, cybercrime, fraud, corruption, and illegal fishing and mining. These activities feed violence in our communities, endanger public safety and health, and contribute to tens of thousands of drug-overdose deaths in the United States each year. They degrade the security and stability of our neighbors and partners by undermining the rule of law, fostering corruption, acting as proxies for hostile state activities, and exploiting and endangering vulnerable populations. We will accelerate our efforts to curb the threat posed by transnational organized crime, integrating the vital work of law enforcement with diplomatic, financial, intelligence, and other tools, and in coordination with foreign partners. As part of this effort, we will work to reduce the availability of illicit drugs in the United States, especially the growing scourge of fentanyl and methamphetamines, by bringing all the tools of government to bear to interdict drugs and disrupt TCO's supply chains and the financial networks that enable their corrosive activities. Recognizing that this is a problem with global reach we will work closely with our international partners to stop TCOs from getting precursor chemicals and work closely with private industry to increase vigilance and prevent the diversion of chemicals for illicit fentanyl production.

Shaping the Rules of the Road

Since 1945, the United States has led the creation of institutions, norms, and standards to govern international trade and investment, economic policy, and technology. These mechanisms advanced America's economic and geopolitical aims and benefited people around the world by shaping how governments and economies interacted—and did so in ways that aligned with U.S. interests and values. These mechanisms have not kept pace with economic or technological changes, and today risk being irrelevant, or in certain cases, actively harmful to solving the challenges we now face—from insecure supply chains to widening inequality to the abuses of the PRC's nonmarket economic actions. We are endeavoring to strengthen and update the UN system and multilateral institutions generally. Nowhere is this need more acute than in updating the rules of the road for technology, cyberspace, trade, and economics.

By doing so in close coordination with our allies and partners, we will establish fair rules while also sustaining our economic and technological edge and shape a future defined by fair competition—because when American workers and companies compete on a level playing field, they win.

Technology

Technology is central to today's geopolitical competition and to the future of our national security, economy and democracy. U.S. and allied leadership in technology and innovation has long underpinned our economic prosperity and military strength. In the next decade, critical and emerging technologies are poised to retool economies, transform militaries, and reshape the



world. The United States is committed to a future where these technologies increase the security, prosperity, and values of the American people and like-minded democracies. Our technology strategy will enable the United States and like-minded democracies to work together to pioneer new medicines that can cure diseases, increase the production of healthy foods that are sustainably grown, diversify and strengthen our manufacturing supply chains, and secure energy without reliance on fossil fuels, all while delivering new jobs and security for the American people and our allies and partners. With bipartisan support, we have launched a modern industrial strategy and already secured historic investments in clean energy, microelectronics manufacturing, research, and development, and biotechnology, and we will work with Congress to fully fund historic new authorizations for research and development. We also are doubling down on our longstanding and asymmetric strategic advantage: attracting and retaining the world's best talent. Attracting a higher volume of global STEM talent is a priority for our national security and supply chain security, so we will aggressively implement recent visa actions and work with Congress to do more.

These investments will enable the United States to anchor an allied techno-industrial base that will safeguard our shared security, prosperity and values. This means working with allies and partners to harness and scale new technologies, and promote the foundational technologies of the 21st century, especially microelectronics, advanced computing and quantum technologies, artificial intelligence, biotechnology and biomanufacturing, advanced telecommunications, and clean energy technologies. We also will partner with like-minded nations to co-develop and deploy technologies in a way that benefits all, not only the powerful, and build robust and durable supply chains so that countries cannot use economic warfare to coerce others.

We are already rallying like-minded actors to advance an international technology ecosystem that protects the integrity of international standards development and promotes the free flow of data and ideas with trust, while protecting our security, privacy, and human rights, and enhancing our competitiveness. That includes work through the U.S.-EU Trade and Technology Council to foster transatlantic coordination on semiconductor and critical mineral supply chains, trustworthy artificial intelligence, disinformation, the misuse of technology threatening security and human rights, export controls, and investment screening, as well as through the Indo-Pacific Quad on critical and emerging technologies, open, next-generation digital infrastructure, and people-to-people exchanges. Across this work, we seek to bolster U.S. and allied technology leadership, advance inclusive and responsible technology development, close regulatory and legal gaps, strengthen supply chain security, and enhance cooperation on privacy, data sharing, and digital trade.

We must ensure strategic competitors cannot exploit foundational American and allied technologies, know-how, or data to undermine American and allied security. We are therefore modernizing and strengthening our export control and investment screening mechanisms, and also pursuing targeted new approaches, such as screening of outbound investment, to prevent strategic competitors from exploiting investments and expertise in ways that threaten our national security, while also protecting the integrity of allied technological ecosystems and markets. We will also work to counter the exploitation of American's sensitive data and illegitimate use of technology, including commercial spyware and surveillance technology, and we will stand against digital authoritarianism.

To achieve these goals, the digital backbones of the modern economy must be open, trusted, interoperable, reliable, and secure. That requires working with a broad range of partners to



advance network infrastructure resilience in 5G and other advanced communication technologies, including by promoting vendor diversity and securing supply chains. These investments cannot just be made in wealthy countries; we must also focus on providing high-quality digital infrastructure in low- and middle-income countries, bridging digital divides by emphasizing access among marginalized groups. To ensure these investments support positive technological outcomes, we will partner with industry and governments in shaping technological standards that ensure quality, consumer safety, and global interoperability, and to advance the open and transparent standards process that has enabled innovation, growth, and interconnectivity for decades. And in all that we do we will strive to ensure that technology supports, and does not undermine, democracy, and is developed, deployed, and governed in accordance with human rights.

Securing Cyberspace

Our societies, and the critical infrastructure that supports them, from power to pipelines, are increasingly digital and vulnerable to disruption or destruction via cyber attacks. Such attacks have been used by countries, such as Russia, to undermine countries' ability to deliver services to citizens and coerce populations. We are working closely with allies and partners, such as the Quad, to define standards for critical infrastructure to rapidly improve our cyber resilience, and building collective capabilities to rapidly respond to attacks. In the face of disruptive cyber attacks from criminals, we have launched innovative partnerships, to expand law enforcement cooperation, deny sanctuary to cyber criminals and counter illicit use of cryptocurrency to launder the proceeds of cybercrime. As an open society, the United States has a clear interest in strengthening norms that mitigate cyber threats and enhance stability in cyberspace. We aim to deter cyber attacks from state and non state actors and will respond decisively with all appropriate tools of national power to hostile acts in cyberspace, including those that disrupt or degrade vital national functions or critical infrastructure. We will continue to promote adherence to the UN General Assembly-endorsed framework of responsible state behavior in cyberspace, which recognizes that international law applies online, just as it does offline.

Trade and Economics

America's prosperity also relies on a fair and open trade and international economic system. The United States has long benefited from international trade's ability to promote global economic growth, lower consumer prices, and access to foreign markets to promote U.S. exports and jobs. At the same time, the longstanding rules that govern trade and other means of economic exchange have been violated by non-market actors, like the PRC; were designed to privilege corporate mobility over workers and the environment, thereby exacerbating inequality and the climate crisis; and fail to cover the frontiers of the modern economy, including digital trade. The United States must once again rally partners around rules for creating a level playing field that will enable American workers and businesses—and those of partners and allies around the world—to thrive.

As our recent work to create IPEF and the Americas Partnership for Economic Prosperity show, we are working to update the current trading system to promote equitable and resilient growth—encouraging robust trade, countering anticompetitive practices, bringing worker voices to the decision-making table, and ensuring high labor and environmental standards. We will seek new export opportunities that benefit American workers and companies, especially small- and



medium-sized enterprises, push back on abuses by non-market economies, and enforce rules against unfair trade and labor practices, including intellectual property theft, discriminatory regulations, forced labor, the denial of the right to organize, and other forms of labor repression. We will also use trade tools to advance climate priorities, as we are doing with the landmark steel and aluminum agreement with the EU. These arrangements will be accompanied by real adjustment assistance, ensuring all Americans have a dignified place in our shared future. Taken together, these efforts will create growth and innovation that benefits not only Americans, but people around the world.

Beyond trade, we are working to build an international economic system fit for contemporary realities. We will tackle the harms caused to U.S. workers, consumers, and businesses by currency manipulation; counter corruption and illicit finance; and end the race to the bottom for corporate taxation through promotion of the OECD's Global Minimum Tax. We will partner with countries on sustainable development, including by responding to global debt challenges and financing quality infrastructure through PGII. We will explore the merits and responsibly lead development of digital assets, including a digital dollar, with high standards and protections for stability, privacy, and security to benefit a strong and inclusive U.S. financial system and reinforce its global primacy. And we will address growth-stymying legal, structural, and cultural barriers that undermine labor force participation for women and marginalized groups. We will also support efforts by the international financial institutions which will also need to continue to evolve to meet the challenges of our times. Many of the biggest challenges in our world today—such as pandemics and health, climate change, fragility, migration and refugee flows—cross borders and disproportionately affect the poorest, most vulnerable populations. Bolstering these institutions is also critical to tackling serious long-term challenges to the international order, such as those posed by the PRC.

Hostages and Wrongful Detainees

Using human beings as pawns is antithetical to American values and to the global order to which we aspire. Yet, that is what governments, regimes, and non-state actors do when they hold Americans against their will as hostages and wrongful detainees. We are working with our partners to deter and thwart those inhumane tactics. That includes our issuance in July 2022 of an executive order implementing a recent U.S. law called the Levinson Act and unlocking new tools for punishing those who wrongfully kidnap or detain Americans abroad. And it includes working with key international partners to promote and implement the Canadian-launched Declaration Against Arbitrary Detention in State-to-State Relations so as to turn the tide against this inhumane practice and forge international norms against it.



Countering Corruption

Corruption poses a fundamental threat to the rule of law. When government officials abuse public power for private gain, it degrades the business environment, subverts economic opportunity, and exacerbates inequality. Corruption also contributes to reduced public trust in state institutions, which in turn can add to the appeal of illiberal actors who exploit popular grievances for political advantage. In today's globalized world, international financial systems are used to stash illicit wealth abroad and to send bribes across borders. The United States Strategy on Countering Corruption recognizes the unique threat corruption poses to our national security and places a special emphasis on recognizing the ways in which corrupt actors have used the U.S. financial system and other rule-of-law based systems to launder their ill-gotten gains. In response to Russia's continued invasion of Ukraine, the United States ramped up its kleptocracy initiatives aimed at recovering corruption proceeds as well as both identifying and repatriating the laundered proceeds of crime. Finally, the United States will elevate and expand the scale of diplomatic engagement and foreign assistance, including by enhancing partner governments' capacities to fight corruption in cooperation with U.S. law enforcement authorities and bolstering the prevention and oversight capacities of willing governments.



PART V: CONCLUSION

We are confident that the United States, alongside our allies and partners, is positioned to succeed in our pursuit of a free, open, prosperous, and secure global order. With the key elements outlined in this strategy, we will tackle the twin challenges of our time: out-competing our rivals to shape the international order while tackling shared challenges, including climate change, pandemic preparedness, and food security, that will define the next stage of human history. We will strengthen democracy across the world, and multilateral institutions, as we look to the future to chart new and fair rules of the road for emerging technology, cybersecurity, and trade and economics. And we will do all this and more by leveraging our considerable advantages and our unparalleled coalition of allies and partners.

As we implement this strategy, we will continually assess and reassess our approach to ensure we are best serving the American people. We will be guided by the indisputable fact that the strength and quality of the American project at home is inextricably linked with our leadership in the world and our ability to shape the terms of the world order. This National Security Strategy will be evaluated by an overriding metric: whether it makes life better, safer, and fairer for the people of the United States, and whether it lifts up the countries and people around the world who share our vision for the future.

We are motivated by a clear vision of what success looks like at the end of this decisive decade.

By enhancing our industrial capacity, investing in our people, and strengthening our democracy, we will have strengthened the foundation of our economy, bolstered our national resilience, enhanced our credibility on the world stage, and ensured our competitive advantages.

By deepening and expanding our diplomatic relationships not only with our democratic allies but with all states who share our vision for a better future, we will have developed terms of competition with our strategic rivals that are favorable to our interests and values and laid the foundation to increase cooperation on shared challenges.

By modernizing our military, pursuing advanced technologies, and investing in our defense workforce, we will have strengthened deterrence in an era of increasing geopolitical confrontation, and positioned America to defend our homeland, our allies, partners, and interests overseas, and our values across the globe.

By leveraging our national strengths and rallying a broad coalition of allies and partners, we will advance our vision of a free, open, prosperous, and secure world, outmaneuvering our competitors, and making meaningful progress on issues like climate change, global health, and food security to improve the lives not just of Americans but of people around the world.

This is what we must achieve in this decisive decade. As we have done throughout our history, America will seize this moment and rise to the challenge. There is no time to waste.

EXHIBIT 4



TABLE OF CONTENTS

I. THE INDO-PACIFIC'S PROMISE

II. OUR INDO-PACIFIC STRATEGY

ADVANCE A FREE AND OPEN INDO-PACIFIC

BUILD CONNECTIONS WITHIN AND BEYOND THE REGION

DRIVE INDO-PACIFIC PROSPERITY

BOLSTER INDO-PACIFIC SECURITY

BUILD REGIONAL RESILIENCE TO 21ST-CENTURY TRANSNATIONAL THREATS

III. INDO-PACIFIC ACTION PLAN

IV. CONCLUSION



THE INDO-PACIFIC'S PROMISE

The United States is an Indo-Pacific power. The region, stretching from our Pacific coastline to the Indian Ocean, is home to more than half of the world's people, nearly two-thirds of the world's economy, and seven of the world's largest militaries. More members of the U.S. military are based in the region than in any other outside the United States. It supports more than three million American jobs and is the source of nearly \$900 billion in foreign direct investment in the United States. In the years ahead, as the region drives as much as two-thirds of global economic growth, its influence will only grow—as will its importance to the United States.

The United States has long recognized the Indo-Pacific as vital to our security and prosperity. Our ties were forged two centuries ago, when Americans came to the region seeking commercial opportunities, and grew with the arrival of Asian immigrants to the United States. The Second World War reminded the United States that our country could only be secure if Asia was, too. And so in the post-war era, the United States solidified our ties with the region, through ironclad treaty alliances with Australia, Japan, the Republic of Korea (ROK), the Philippines, and Thailand, laying the foundation of security that allowed regional democracies to flourish. Those ties expanded as the United States supported the region's premier organizations, particularly the Association of Southeast Asian Nations (ASEAN); developed close trade and investment relationships; and committed to uphold international law and norms, from human rights to freedom of navigation.

The passage of time has underscored the strategic necessity of the United States' consistent role. At the end of the Cold War, the United States considered but rejected the idea of withdrawing our military presence, understanding that the region held strategic value that would only grow in the 21st century. Since then, administrations of both political parties have shared a commitment to the region. The George W. Bush Administration understood Asia's growing importance and engaged closely with the People's Republic of China (PRC), Japan, and India. The Obama Administration significantly accelerated American prioritization of Asia, investing new diplomatic, economic, and military resources there. And the Trump Administration also recognized the Indo-Pacific as the world's center of gravity.



Under President Biden, the United States is determined to strengthen our long-term position in and commitment to the Indo-Pacific. We will focus on every corner of the region, from Northeast Asia and Southeast Asia, to South Asia and Oceania, including the Pacific Islands. We do so at a time when many of our allies and partners, including in Europe, are increasingly turning their own attention to the region; and when there is broad, bipartisan agreement in the U.S. Congress that the United States must, too. In a quickly changing strategic landscape, we recognize that American interests can only be advanced if we firmly anchor the United States in the Indo-Pacific and strengthen the region itself, alongside our closest allies and partners.

This intensifying American focus is due in part to the fact that the Indo-Pacific faces mounting challenges, particularly from the PRC. The PRC is combining its economic, diplomatic, military, and technological might as it pursues a sphere of influence in the Indo-Pacific and seeks to become the world's most influential power. The PRC's coercion and aggression spans the globe, but it is most acute in the Indo-Pacific. From the economic coercion of Australia to the conflict along the Line of Actual Control with India to the growing pressure on Taiwan and bullying of neighbors in the East and South China Seas, our allies and partners in the region bear much of the cost of the PRC's harmful behavior. In the process, the PRC is also undermining human rights and international law, including freedom of navigation, as well as other principles that have brought stability and prosperity to the Indo-Pacific.

Our collective efforts over the next decade will determine whether the PRC succeeds in transforming the rules and norms that have benefitted the Indo-Pacific and the world. For our part, the United States is investing in the foundations of our strength at home, aligning our approach with those of our allies and partners abroad, and competing with the PRC to defend the interests and vision for the future that we share with others. We will strengthen the international system, keep it grounded in shared values, and update it to meet 21st-century challenges. Our objective is not to change the PRC but to shape the strategic environment in which it operates, building a balance of influence in the world that is maximally favorable to the United States, our allies and partners, and the interests and values we share. We will also seek to manage competition with the PRC responsibly. We will cooperate with our allies and partners while seeking to work with the PRC in areas like climate change and nonproliferation. We believe it is in the interests of the region and the wider world that no country withhold progress on existential transnational issues because of bilateral differences.

THE REGION BY THE NUMBERS



- ◆ **POPULATION:** Over half the world's people, including 58% of youth
- ◆ **ECONOMY:** 60% of global GDP
- ◆ **GROWTH:** 2/3 of global economic growth
- ◆ **GEOGRAPHY:** 65% of the world's oceans and 25% of its land



The Indo-Pacific faces other major challenges. Climate change is growing ever-more severe as South Asia's glaciers melt and the Pacific Islands battle existential rises in sea levels. The COVID-19 pandemic continues to inflict a painful human and economic toll across the region. The Democratic People's Republic of Korea (DPRK) continues to expand its illicit nuclear weapons and missile programs. Indo-Pacific governments grapple with natural disasters, resource scarcity, internal conflict, and governance challenges. Left unchecked, these forces threaten to destabilize the region.

“ **WE WILL FOCUS ON EVERY CORNER OF THE REGION, FROM NORTHEAST ASIA AND SOUTHEAST ASIA, TO SOUTH ASIA AND OCEANIA, INCLUDING THE PACIFIC ISLANDS.**

As we enter a decisive decade that holds considerable promise and historic obstacles for the Indo-Pacific, the American role in the region must be more effective and enduring than ever. To do this, we will modernize our long-standing alliances, strengthen emerging partnerships, and invest in regional organizations—the collective capacity that will empower the Indo-Pacific to adapt to the 21st century's challenges and seize its opportunities. As the PRC, the climate crisis, and a pandemic test us, we must work with our allies and partners toward our positive vision: of a free and open Indo-Pacific that is more connected, prosperous, secure, and resilient. This national strategy outlines that approach and commits the United States to its success.



OUR INDO-PACIFIC STRATEGY

The United States is committed to an Indo-Pacific that is free and open, connected, prosperous, secure, and resilient. To realize that future, the United States will strengthen our own role while reinforcing the region itself. The essential feature of this approach is that it cannot be accomplished alone: changing strategic circumstances and historic challenges require unprecedented cooperation with those who share in this vision.

For centuries, the United States and much of the world have viewed Asia too narrowly—as an arena of geopolitical competition. Today, Indo-Pacific nations are helping to define the very nature of the international order, and U.S. allies and partners around the world have a stake in its outcomes. Our approach, therefore, draws from and aligns with those of our closest friends. Like Japan, we believe that a successful Indo-Pacific vision must advance freedom and openness and offer “autonomy and options.” We support a strong India as a partner in this positive regional vision. Like Australia, we seek to maintain stability and reject coercive exercises of power. Like the ROK, we aim to promote regional security through capacity-building. Like ASEAN, we see Southeast Asia as central to the regional architecture. Like New Zealand and the United Kingdom, we seek to build resilience in the regional rules-based order. Like France, we recognize the strategic value of an increasing regional role for the European Union (EU). Much like the approach the EU has announced in its Strategy for Cooperation in the Indo-Pacific, American strategy will be principled, long-term, and anchored in democratic resilience.

The United States will pursue five objectives in the Indo-Pacific—each in concert with our allies and partners, as well as with regional institutions. We will:

- ADVANCE A FREE AND OPEN INDO-PACIFIC
- BUILD CONNECTIONS WITHIN AND BEYOND THE REGION
- DRIVE REGIONAL PROSPERITY
- BOLSTER INDO-PACIFIC SECURITY
- BUILD REGIONAL RESILIENCE TO TRANSNATIONAL THREATS



1. ADVANCE A FREE AND OPEN INDO-PACIFIC

Our vital interests and those of our closest partners require a free and open Indo-Pacific, where governments can make their own sovereign choices, consistent with their obligations under international law; and where seas, skies, and other shared domains are lawfully governed. Our strategy, therefore, begins with building resilience within countries, as we have done in the United States. In the region, that includes our efforts to support open societies and to ensure Indo-Pacific governments can make independent political choices free from coercion; we will do so through investments in democratic institutions, a free press, and a vibrant civil society. The United States will bolster freedom of information and expression and combat foreign interference by supporting investigative journalism, promoting media literacy and pluralistic and independent media, and increasing collaboration to address threats from information manipulation. Consistent with the first-ever United States Strategy on Countering Corruption, we will also seek to improve fiscal transparency in the Indo-Pacific to expose corruption and drive reform. Through our diplomatic engagement, foreign assistance, and work with regional organizations, the United States will be a partner in strengthening democratic institutions, the rule of law, and accountable democratic governance. And we will work with partners to stand up to economic coercion.

“ INDO-PACIFIC NATIONS ARE HELPING TO DEFINE THE VERY NATURE OF THE INTERNATIONAL ORDER, AND U.S. ALLIES AND PARTNERS AROUND THE WORLD HAVE A STAKE IN ITS OUTCOMES.

Beyond individual countries' borders, the United States will also work closely with like-minded partners to ensure that the region remains open and accessible and that the region's seas and skies are governed and used according to international law. In particular, we will build support for rules-based approaches to the maritime domain, including in the South China Sea and the East China Sea.

We will also work with partners to advance common approaches to critical and emerging technologies, the internet, and cyber space. We will build support for an open, interoperable, reliable, and secure internet; coordinate with partners to maintain the integrity of international standard bodies and promote consensus-based, values-aligned technology standards; facilitate the movement of researchers and open access to scientific data for cutting-edge collaboration; and work to implement the framework of responsible behavior in cyber space and its associated norms.



2. BUILD CONNECTIONS WITHIN AND BEYOND THE REGION

A free and open Indo-Pacific can only be achieved if we build collective capacity for a new age; common action is now a strategic necessity. The alliances, organizations, and rules that the United States and our partners have helped to build must be adapted; where needed, we must update them together. We will pursue this through a latticework of strong and mutually reinforcing coalitions.

Those efforts begin with our closest alliances and partnerships, which we are renewing in innovative ways. We are deepening our five regional treaty alliances—with Australia, Japan, the ROK, the Philippines, and Thailand—and strengthening relationships with leading regional partners, including India, Indonesia, Malaysia, Mongolia, New Zealand, Singapore, Taiwan, Vietnam, and the Pacific Islands. We will also encourage our allies and partners to strengthen their ties with one another, particularly Japan and the ROK. We will support and empower allies and partners as they take on regional leadership roles themselves, and we will work in flexible groupings that pool our collective strength to face up to the defining issues of our time, particularly through the Quad. We will continue to strengthen Quad cooperation on global health, climate change, critical and emerging technology, infrastructure, cyber, education, and clean energy, as we work together and with other partners toward a free and open Indo-Pacific.

“ WE WILL MODERNIZE OUR LONG-STANDING ALLIANCES, STRENGTHEN EMERGING PARTNERSHIPS, AND INVEST IN REGIONAL ORGANIZATIONS—THE COLLECTIVE CAPACITY THAT WILL EMPOWER THE INDO-PACIFIC TO ADAPT TO THE 21ST CENTURY’S CHALLENGES AND SEIZE ITS OPPORTUNITIES.

The United States also welcomes a strong and independent ASEAN that leads in Southeast Asia. We endorse ASEAN centrality and support ASEAN in its efforts to deliver sustainable solutions to the region’s most pressing challenges. To that end, we will deepen long-standing cooperation with ASEAN while launching new high-level engagements on health, climate and environment, energy, transportation, and gender equity and equality. We will work with ASEAN to build its resilience as a leading regional institution and will explore opportunities for the Quad to work with ASEAN. We will also support closer ties between South



Asian partners and ASEAN. Our own work with South Asian partners will prioritize building mechanisms to address humanitarian-assistance and disaster-relief needs, maritime security, water scarcity, and pandemic response. We will seek to be an indispensable partner to Pacific Island nations, in ever-closer coordination with other partners who share that commitment, and will meaningfully expand our diplomatic presence in Southeast Asia and the Pacific Islands. We will also prioritize negotiations on our Compacts of Free Association with the Freely Associated States as the bedrock of the U.S. role in the Pacific.

Allies and partners outside of the region are increasingly committing new attention to the Indo-Pacific, particularly the EU and the North Atlantic Treaty Organization (NATO). We will harness this opportunity to align our approaches and will implement our initiatives in coordination to multiply our effectiveness. We will partner to build regional connectivity with an emphasis on the digital domain, as well as to uphold international law, particularly in the maritime space. Along the way, we will build bridges between the Indo-Pacific and the Euro-Atlantic, and, increasingly, with other regions, by leading on shared agendas that drive collective action. We will also advance our common vision through close coordination at the United Nations.

Our ties do not just connect our governments, but bridge our people. The United States is the leading international provider of education to students from the Indo-Pacific—nearly 68% of international students studying in the United States hail from the region—forging ties that help to fuel next-generation dynamism in both of our countries. We will reinvigorate youth-leadership, educational, and professional exchanges and English-language training programs that have long anchored our bonds, including through the Young Southeast Asian Leaders Initiative (YSEALI). At the same time, we will promote new partnerships for cutting-edge joint research in critical domains of science and technology, including through the new Quad Fellowship, which will support graduate studies of Australian, Japanese, Indian, and American students in STEM fields. Through these and other programs we will continue to invest in the next generation of people-to-people connections.

INDO-PACIFIC STRATEGY ELEMENTS



- ◆ **STRATEGIC ENDS:**
Advance a free and open Indo-Pacific that is more connected, prosperous, secure, and resilient.
- ◆ **STRATEGIC WAYS:**
Strengthen the U.S. role and build collective capacity with allies and partners and with regional institutions.
- ◆ **STRATEGIC MEANS:**
Modernized alliances; flexible partnerships, including an empowered ASEAN, a leading India, a strong and reliable Quad, and an engaged Europe; economic partnership; new U.S. defense, diplomatic, development, and foreign-assistance resources; sustained focus on and commitment to the region at all levels of the U.S. government.



3. DRIVE INDO-PACIFIC PROSPERITY

The prosperity of everyday Americans is linked to the Indo-Pacific. We will put forward an innovative new framework to equip our economies for this moment. Our efforts are built on a strong foundation of close economic integration. Two-way trade between the United States and the region totaled \$1.75 trillion in 2020, and it supports more than five million Indo-Pacific jobs. Foreign direct investment from the United States totaled more than \$969 billion in 2020 and has nearly doubled in the last decade. The United States remains the number-one investment partner in ASEAN member countries—investing more than Southeast Asia’s next three investment partners combined. And the United States is the primary exporter of services to the region, which, in turn, fuels regional growth.

The COVID-19 pandemic has made clear the need for a recovery that promotes broad-based economic growth. That requires investments to encourage innovation, strengthen economic competitiveness, produce good-paying jobs, rebuild supply chains, and expand economic opportunities for middle-class families: 1.5 billion people in the Indo-Pacific will join the global middle class in this decade.

Alongside our partners, the United States will put forward an Indo-Pacific economic framework—a multilateral partnership for the 21st century. This economic framework will help our economies to harness rapid technological transformation, including in the digital economy, and adapt to the coming energy and climate transition. The United States will work with partners to ensure that citizens on both sides of the Pacific reap the benefits of these historic economic changes, while deepening our integration. We will develop new approaches to trade that meet high labor and environmental standards and will govern our digital economies and cross-border data flows according to open principles, including through a new digital-economy framework. We will work with our partners to advance resilient and secure supply chains that are diverse, open, and predictable, while removing barriers and improving transparency and information-sharing. We will make shared investments in decarbonization and clean energy, and work in the Asia-Pacific Economic Cooperation (APEC) to promote free, fair, and open trade and investment, during our host year, in 2023, and beyond.

We will also redouble our commitment to helping Indo-Pacific partners close the region’s infrastructure gap. Through our Build Back Better World initiative with G7 partners, we will equip the emerging economies of



the region with the high-standards infrastructure that will enable them to grow and prosper, while creating good jobs on both sides of the Pacific. As we do, we will promote resilient and secure global telecommunications, focusing on 5G vendor diversification and Open Radio Access Network (O-RAN) technology, and seeking a telecommunications supply market that is well-postured to allow for new, trustworthy entrants. We will also stand shoulder-to-shoulder with regional economic partners who are playing leading roles in setting rules that govern 21st-century economic activity. Together, we will harness rapid economic transformation as a common opportunity for us all.

4. BOLSTER INDO-PACIFIC SECURITY

For 75 years, the United States has maintained a strong and consistent defense presence necessary to support regional peace, security, stability, and prosperity. The United States has been a steadfast regional ally and will remain so in the 21st century. Today, we are extending and modernizing that role: the United States is enhancing our capabilities to defend our interests as well as to deter aggression and to counter coercion against U.S. territory and our allies and partners.

Integrated deterrence will be the cornerstone of our approach. We will more tightly integrate our efforts across warfighting domains and the spectrum of conflict to ensure that the United States, alongside our allies and partners, can dissuade or defeat aggression in any form or domain. We will drive initiatives that reinforce deterrence and counter coercion, such as opposing efforts to alter territorial boundaries or undermine the rights of sovereign nations at sea.

We will renew our focus on innovation to ensure the U.S. military can operate in rapidly evolving threat environments, including space, cyberspace, and critical- and emerging-technology areas. We are developing new concepts of operations, building more resilient command and control, increasing the scope and complexity of our joint exercises and operations, and pursuing diverse force-posture opportunities that will strengthen our ability to operate forward and more flexibly with allies and partners.

Consistent with our broader strategic approach, we will prioritize our single greatest asymmetric strength: our network of security alliances and partnerships. Across the region, the United States will work with allies and partners to deepen our interoperability and develop and deploy advanced warfighting capabilities as we support them in defending their citizens and their sovereign interests. We will continue to modernize our



treaty alliances with Australia, Japan, the ROK, the Philippines, and Thailand; steadily advance our Major Defense Partnership with India and support its role as a net security provider; and build the defense capacity of partners in South and Southeast Asia and the Pacific Islands. We will also work with partners inside and outside of the region to maintain peace and stability in the Taiwan Strait, including by supporting Taiwan's self-defense capabilities, to ensure an environment in which Taiwan's future is determined peacefully in accordance with the wishes and best interests of Taiwan's people. As we do so, our approach remains consistent with our One China policy and our longstanding commitments under the Taiwan Relations Act, the Three Joint Communiqués, and the Six Assurances.

We will foster security ties between our allies and partners in the Indo-Pacific region and beyond, including by finding new opportunities to link our defense industrial bases, integrating our defense supply chains, and co-producing key technologies that will shore up our collective military advantages. As we do, we will bring together our Indo-Pacific and European partners in novel ways, including through the AUKUS partnership.

As the DPRK continues to develop destabilizing nuclear and missile programs, we will continue to seek serious and sustained dialogue, with the goal of complete denuclearization of the Korean Peninsula and addressing its ongoing human-rights violations and improving the lives and livelihoods of the North Korean people. At the same time, we are strengthening extended deterrence and coordination with the ROK and Japan to respond to DPRK provocations, remaining prepared to deter—and, if necessary, defeat—any aggression to the United States and our allies, while bolstering counter-proliferation efforts throughout the region. While reinforcing extended deterrence against nuclear- and ballistic-missile systems and other emerging threats to strategic stability, the United States will seek to work with a wide set of actors, including our rivals, to prevent and manage crises.

We will also innovate to meet civilian security challenges, expanding U.S. Coast Guard presence, training, and advising to bolster our partners' capabilities. We will cooperate to address and prevent terrorism and violent extremism, including by identifying and monitoring foreign fighters traveling to the region, formulating options to mitigate online radicalization, and encouraging counterterrorism cooperation within the Indo-Pacific. And we will strengthen collective regional capabilities to prepare for and respond to environmental and natural disasters; natural, accidental, or deliberate biological threats; and the trafficking of weapons, drugs, and people. We will improve cybersecurity in the region, including the ability of our partners to protect against, recover from, and respond to cybersecurity incidents.



5. BUILD REGIONAL RESILIENCE TO 21ST-CENTURY TRANSNATIONAL THREATS

The Indo-Pacific is the epicenter of the climate crisis, but it is also essential to climate solutions. Achieving the goals of the Paris Agreement will require the major economies in the region to align their targets with the Agreement's temperature goals. This includes urging the PRC to commit to and implement actions in line with the level of ambition required to limit warming to 1.5 degrees Celsius. Our shared responses to the climate crisis are both a political imperative and an economic opportunity in the Indo-Pacific, home to 70% of the world's natural disasters. The United States will work with partners to develop 2030 and 2050 targets, strategies, plans, and policies consistent with limiting the global temperature increase to 1.5 degrees Celsius, and will seek to serve as the preferred partner as the region transitions to a net-zero future. Through initiatives like Clean EDGE, we will incentivize clean-energy technology investment and deployment, seek to drive energy-sector decarbonization, and foster climate-aligned infrastructure investment. The United States will work with partners to reduce their vulnerability to the impacts of climate change and environmental degradation and will support critical-infrastructure resilience and address energy security. We will also work to safeguard the health and sustainable use of the region's vast oceans, including through the legal use of their resources, enhanced research cooperation, and the promotion of beneficial commerce and transportation.

We will partner with the region to help end the COVID-19 pandemic and build resilience against common threats. We will work closely with partners to strengthen their health systems to withstand future shocks, drive investments in global health security, and expand regional platforms to prevent, detect, and respond to emergencies, including biological threats. We will also work through the World Health Organization (WHO), the G7, the G20, and other multilateral fora to strengthen preparedness and response. We will advance our resilience efforts in close coordination with ASEAN, APEC, the Pacific Islands Forum (PIF), and other organizations.



INDO-PACIFIC ACTION PLAN

To implement this strategy, we will pursue ten core lines of effort in the next 12 to 24 months:

DRIVE NEW RESOURCES TO THE INDO-PACIFIC

Building shared capacity requires the United States to make new regional investments. We will open new embassies and consulates, particularly in Southeast Asia and the Pacific Islands, and increase our strength in existing ones, intensifying our climate, health, security, and development work. We will expand U.S. Coast Guard presence and cooperation in Southeast and South Asia and the Pacific Islands, with a focus on advising, training, deployment, and capacity-building. We will refocus security assistance on the Indo-Pacific, including to build maritime capacity and maritime-domain awareness. We will also expand the role of people-to-people exchange, including the Peace Corps. Within the U.S. government, we will ensure we have the necessary capacity and expertise to meet the region's challenges. Throughout, we will work with Congress to ensure that our policy and resourcing have the bipartisan backing necessary to support our strong and steady regional role.

LEAD AN INDO-PACIFIC ECONOMIC FRAMEWORK

We will launch, in early 2022, a new partnership that will promote and facilitate high-standards trade, govern the digital economy, improve supply-chain resiliency and security, catalyze investment in transparent, high-standards infrastructure, and build digital connectivity—doubling down on our economic ties to the region while contributing to broadly shared Indo-Pacific opportunity.

REINFORCE DETERRENCE

The United States will defend our interests, deter military aggression against our own country and our allies and partners—including across the Taiwan Strait—and promote regional security by developing new capabilities, concepts of operation, military activities, defense industrial initiatives, and a more resilient force posture. We will work with Congress to fund the Pacific Deterrence Initiative and the Maritime Security Initiative. Through the AUKUS partnership, we will identify the optimal pathway to deliver nuclear-powered submarines to the Royal Australian Navy at the earliest achievable date; in addition, we will deepen cooperation and enhance interoperability through a concrete program of work on advanced capabilities, including cyber, artificial intelligence, quantum technologies, and undersea capabilities.



STRENGTHEN AN EMPOWERED AND UNIFIED ASEAN

The United States is making new investments in U.S.-ASEAN ties, including by hosting ASEAN leaders for a historic U.S.-ASEAN Special Summit—the first-ever to be held in Washington, D.C. We are committed to the East Asia Summit and ASEAN Regional Forum, and will also seek new ministerial-level engagements with ASEAN. We will implement more than \$100 million in new U.S.-ASEAN initiatives. We will also expand bilateral cooperation across Southeast Asia, prioritizing efforts to strengthen health security, address maritime challenges, increase connectivity, and deepen people-to-people ties.

SUPPORT INDIA'S CONTINUED RISE AND REGIONAL LEADERSHIP

We will continue to build a strategic partnership in which the United States and India work together and through regional groupings to promote stability in South Asia; collaborate in new domains, such as health, space, and cyber space; deepen our economic and technology cooperation; and contribute to a free and open Indo-Pacific. We recognize that India is a like-minded partner and leader in South Asia and the Indian Ocean, active in and connected to Southeast Asia, a driving force of the Quad and other regional fora, and an engine for regional growth and development.

DELIVER ON THE QUAD

We will strengthen the Quad as a premier regional grouping and ensure it delivers on issues that matter to the Indo-Pacific. The Quad will play a leading regional role on COVID-19 response and global health security, delivering on its investment to provide an additional one billion vaccines to the region and to the world. It will advance work on critical and emerging technologies, driving supply-chain cooperation, joint technology deployments, and advancing common technology principles. The Quad will build a green shipping network, and will coordinate the sharing of satellite data to improve maritime domain awareness and climate responses. Its members will cooperate to provide high-standards infrastructure in South and Southeast Asia and the Pacific Islands and will work to improve their cyber capacity. The Quad Fellowship will formally launch in 2022, recruiting its first class of 100 students from all four countries to pursue graduate degrees in STEM fields in the United States beginning in 2023. The Quad will continue to meet regularly at the leader and ministerial levels.



EXPAND U.S.-JAPAN-ROK COOPERATION

Nearly every major Indo-Pacific challenge requires close cooperation among the United States' allies and partners, particularly Japan and the ROK. We will continue to cooperate closely through trilateral channels on the DPRK. Beyond security, we will also work together on regional development and infrastructure, critical technology and supply-chain issues, and women's leadership and empowerment. Increasingly, we will seek to coordinate our regional strategies in a trilateral context.

PARTNER TO BUILD RESILIENCE IN THE PACIFIC ISLANDS

The United States will work with partners to establish a multilateral strategic grouping that supports Pacific Island countries as they build their capacity and resilience as secure, independent actors. Together, we will build climate resilience through the Pacific Region Infrastructure Facility; coordinate to meet the Pacific's infrastructure gaps, especially on information and communications technology; facilitate transportation; and cooperate to improve maritime security to safeguard fisheries, build maritime-domain awareness, and improve training and advising. We will also prioritize finalization of the Compact of Free Association agreements with the Freely Associated States.

SUPPORT GOOD GOVERNANCE AND ACCOUNTABILITY

We will support Indo-Pacific governments' capacity to make independent political choices by helping partners root out corruption, including through foreign-assistance and development policies, leadership at the G7 and G20, and a renewed role in the Open Government Partnership. We are also partnering with governments, civil society, and journalists to ensure they have the capability to expose and mitigate the risks from foreign interference and information manipulation. The United States will continue to stand up for democracy in Burma, working closely with allies and partners to press the Burmese military to provide for a return to democracy, including through credible implementation of the Five Point Consensus.

SUPPORT OPEN, RESILIENT, SECURE, AND TRUSTWORTHY TECHNOLOGIES

We will promote secure and trustworthy digital infrastructure, particularly cloud and telecommunications vendor diversity, including through innovative network architectures such as Open RAN by encouraging at-scale commercial deployments and cooperation on testing, such as through shared access to test beds to enable common standards development. We will also deepen shared resilience in critical government and infrastructure networks, while building new regional initiatives to improve collective cybersecurity and rapidly respond to cyber incidents.



CONCLUSION

We have entered a consequential new period of American foreign policy that will demand more of the United States in the Indo-Pacific than has been asked of us since the Second World War. Our vital interests in the region have become ever-clearer just as they have become more difficult to protect; we will not have the luxury of choosing between power politics and combatting transnational threats; we will rise to our leadership charge on diplomacy, security, economics, climate, pandemic response, and technology.

The Indo-Pacific's future depends on the choices we make now. The decisive decade before us will determine if the region can confront and address climate change, reveal how the world rebuilds from a once-in-a-century pandemic, and decide whether we can sustain the principles of openness, transparency, and inclusivity that have fueled the region's success. If, together with our partners, we can reinforce the region for 21st-century challenges and seize its opportunities, the Indo-Pacific will thrive, bolstering the United States and the world.

“ **AS WE ENTER A DECISIVE DECADE THAT HOLDS CONSIDERABLE PROMISE AND HISTORIC OBSTACLES FOR THE INDO-PACIFIC, THE AMERICAN ROLE IN THE REGION MUST BE MORE EFFECTIVE AND ENDURING THAN EVER.**

Our considerable strategic ambitions derive from the belief that no region will be of more consequence to the world and to everyday Americans than the Indo-Pacific—and that the United States and our allies and partners hold a common vision for it. By pursuing a strategy whose foundational pillars are shared, and by strengthening the region's capacity to realize them, the United States can lead with others toward an Indo-Pacific that is free and open, connected, prosperous, secure, and resilient for generations to come.

EXHIBIT 5

A DECLARATION *for the* FUTURE *of the* INTERNET

We are united by a belief in the potential of digital technologies to promote connectivity, democracy, peace, the rule of law, sustainable development, and the enjoyment of human rights and fundamental freedoms. As we increasingly work, communicate, connect, engage, learn, and enjoy leisure time using digital technologies, our reliance on an open, free, global, interoperable, reliable, and secure Internet will continue to grow. Yet we are also aware of the risks inherent in that reliance and the challenges we face.

We call for a new Declaration for the Future of the Internet that includes all partners who actively support a future for the Internet that is an open, free, global, interoperable, reliable, and secure. We further affirm our commitment to protecting and respecting human rights online and across the digital ecosystem. Partners in this Declaration intend to work toward an environment that reinforces our democratic systems and promotes active participation of every citizen in democratic processes, secures and protects individuals' privacy, maintains secure and reliable connectivity, resists efforts to splinter the global Internet, and promotes a free and competitive global economy. Partners in this Declaration invite other partners who share this vision to join us in working together, with civil society and other stakeholders, to affirm guiding principles for our role in the future of the global Internet.

RECLAIMING THE PROMISE OF THE INTERNET

The immense promise that accompanied the development of the Internet stemmed from its design: it is an open “network of networks”, a single interconnected communications system for all of humanity. The stable and secure operation of the Internet's unique identifier systems have, from the beginning, been governed by a multistakeholder approach to avoid Internet fragmentation, which continues to be an essential part of our vision. For business, entrepreneurs, and the innovation ecosystem as a whole, interconnection promises better access to customers and fairer competition; for artists and creators, new audiences; for everyone, unfettered access to knowledge. With the creation of the Internet came a swell in innovation, vibrant communication, increased cross-border data flows, and market growth—as well as the invention of new digital products and services that now permeate every aspect of our daily lives.

Over the last two decades, however, we have witnessed serious challenges to this vision emerge. Access to the open Internet is limited by some authoritarian governments and online platforms and digital tools are increasingly used to repress freedom of expression and deny other human rights and fundamental freedoms. State-sponsored or condoned malicious behavior is on the rise, including the spread of disinformation and cybercrimes such as ransomware, affecting the security and the resilience of critical infrastructure while holding at risk vital public and private assets. At the same time, countries have erected firewalls and taken other technical measures, such as Internet shutdowns, to restrict access to journalism, information, and services, in ways that are contrary to international human rights commitments and obligations. Concerted or independent actions of some governments and private actors have sought to abuse the openness of Internet governance and related processes to advance a closed vision. Moreover, the once decentralized Internet economy has become highly concentrated and many people have legitimate concerns about their privacy and the quantity and security of personal data collected and stored online. Online platforms have enabled an increase in the spread of illegal or harmful content that can threaten the safety of individuals and contribute to radicalization and violence. Disinformation and foreign malign activity is used to sow division and conflict between individuals or groups in society, undermining respect for and protection of human rights and democratic institutions.

OUR VISION

We believe we should meet these challenges by working towards a shared vision for the future of the Internet that recommits governments and relevant authorities to defending human rights and fostering equitable economic prosperity. We intend to ensure that the use of digital technologies reinforces, not weakens, democracy and respect for human rights; offers opportunities for innovation in the digital ecosystem, including businesses large and small; and, maintains connections between our societies. We intend to work together to protect and fortify the multistakeholder system of Internet governance and to maintain a high level of security, privacy protection, stability and resilience of the technical infrastructure of the Internet.

We affirm our commitment to promote and sustain an Internet that: is an open, free, global, interoperable, reliable, and secure and to ensure that the Internet reinforces democratic principles and human rights and fundamental freedoms; offers opportunities for collaborative research and commerce; is developed, governed, and deployed in an inclusive way so that unserved and underserved communities, particularly those coming online for the first time, can navigate it safely and with personal data privacy and protections in place; and is governed by multistakeholder processes. In short, an Internet that can deliver on the promise of connecting humankind and helping societies and democracies to thrive.

The Internet should operate as a single, decentralized network of networks – with global reach and governed through the multistakeholder approach, whereby governments and relevant authorities partner with academics, civil society, the private sector, technical community and others. Digital technologies reliant on the Internet, will yield the greatest dividends when they operate as an open, free, global, interoperable, reliable, and secure systems. Digital technologies should be produced, used, and governed in ways that enable trustworthy, free, and fair commerce; avoid unfair discrimination between, and ensure effective choice for, individual users; foster fair competition and encourage innovation; promote and protect human rights; and, foster societies where:

- Human rights and fundamental freedoms, and the well-being of all individuals are protected and promoted;
- All can connect to the Internet, no matter where they are located, including through increased access, affordability, and digital skills;
- Individuals and businesses can trust the safety and the confidentiality of the digital technologies they use

and that their privacy is protected;

- Businesses of all sizes can innovate, compete, and thrive on their merits in a fair and competitive ecosystem;
- Infrastructure is designed to be secure, interoperable, reliable, and sustainable;
- Technology is used to promote pluralism and freedom of expression, sustainability, inclusive economic growth, and the fight against global climate change.

PRINCIPLES TO PROMOTE THIS VISION

The partners in this Declaration intend to uphold a range of key principles, set out below, regarding the Internet and digital technologies; to promote these principles within existing multilateral and multistakeholder fora; to translate these principles into concrete policies and actions; and, work together to promote this vision globally, while respecting each other's regulatory autonomy within our own jurisdictions and in accordance with our respective domestic laws and international legal obligations. These principles are not legally binding but should rather be used as a reference for public policy makers, as well as citizens, businesses, and civil society organizations.

PROTECTION OF HUMAN RIGHTS AND FUNDAMENTAL FREEDOMS

- Dedicate ourselves, in conducting and executing our respective domestic authorities, to respect human rights, including as reflected in the Universal Declaration of Human Rights, as well as the principles of the rule of law, legitimate purpose, non-arbitrariness, effective oversight, and transparency, both online and offline, and call upon others to do the same.
- Promote online safety and continue to strengthen our work to combat violence online, including sexual and gender-based violence as well as child sexual exploitation, to make the Internet a safe and secure place for everyone, particularly women, children, and young people.
- Promote safe and equitable use of the Internet for everyone, without discrimination based on sex, race, color, ethnic, national or social origin, genetic features, language, religion or belief, political or any other opinion, membership of an indigenous population, property, birth, disability, age, gender identity or sexual orientation.
- Reaffirm our commitment that actions taken by governments, authorities, and digital services including online platforms to reduce illegal and harmful content and activities online be consistent with international human rights law, including the right to freedom of expression while encouraging diversity of opinion, and pluralism without fear of censorship, harassment, or intimidation.
- Protect and respect human rights and fundamental freedoms across the digital ecosystem, while providing access to meaningful remedies for human rights violations and abuses, consistent with international human rights law.
- Refrain from misusing or abusing the Internet or algorithmic tools or techniques for unlawful surveillance, oppression, and repression that do not align with international human rights principles, including developing social score cards or other mechanisms of domestic social control or pre-crime detention and arrest.

A GLOBAL INTERNET

- Refrain from government-imposed internet shutdowns or degrading domestic Internet access, either entirely or partially.
- Refrain from blocking or degrading access to lawful content, services, and applications on the Internet, consistent with principles of Net Neutrality subject to applicable law, including international human rights law.
- Promote our work to realize the benefits of data free flows with trust based on our shared values as like-minded, democratic, open and outward looking partners.
- Promote cooperation in research and innovation and standard setting, encourage information sharing regarding security threats through relevant international fora, and reaffirm our commitment to the framework of responsible state behavior in cyberspace.

INCLUSIVE AND AFFORDABLE ACCESS TO THE INTERNET

- Promote affordable, inclusive, and reliable access to the Internet for individuals and businesses where they need it and support efforts to close digital divides around the world to ensure all people of the world are able to benefit from the digital transformation.
- Support digital literacy, skills acquisition, and development so that individuals can overcome the digital divide, participate in the Internet safely, and realize the economic and social potential of the digital economy.
- Foster greater exposure to diverse cultural and multilingual content, information, and news online. Exposure to diverse content online should contribute to pluralistic public discourse, foster greater social and digital inclusion within society, bolster resilience to disinformation and misinformation, and increase participation in democratic processes.

TRUST IN THE DIGITAL ECOSYSTEM

- Work together to combat cybercrime, including cyber-enabled crime, and deter malicious cyber activity.
- Ensure that government and relevant authorities' access to personal data is based in law and conducted in accordance with international human rights law.
- Protect individuals' privacy, their personal data, the confidentiality of electronic communications and information on end-users' electronic devices, consistent with the protection of public safety and applicable domestic and international law.
- Promote the protection of consumers, in particular vulnerable consumers, from online scams and other unfair practices online and from dangerous and unsafe products sold online.
- Promote and use trustworthy network infrastructure and services suppliers, relying on risk-based assessments that include technical and non-technical factors for network security.
- Refrain from using the Internet to undermine the electoral infrastructure, elections and political pro-

cesses, including through covert information manipulation campaigns.

- Support a rules-based global digital economy which fosters trade and contestable and fair online markets so that firms and entrepreneurs can compete on their merits.
- Cooperate to maximize the enabling effects of technology for combatting climate change and protecting the environment whilst reducing as much as possible the environmental footprint of the Internet and digital technologies.

MULTISTAKEHOLDER INTERNET GOVERNANCE

- Protect and strengthen the multistakeholder system of Internet governance, including the development, deployment, and management of its main technical protocols and other related standards and protocols.
- Refrain from undermining the technical infrastructure essential to the general availability and integrity of the Internet.

We believe that the principles for the future of the Internet are universal in nature and as such we invite those who share this vision to affirm these principles and join us in the implementation of this vision. This Declaration takes into account, and expects to contribute to, existing processes in the UN system, G7, G20, the Organisation for Economic Cooperation and Development, the World Trade Organization, and other relevant multilateral and multistakeholder fora, the Internet Corporation for Assigned Names and Numbers, Internet Governance Forum, and Freedom Online Coalition. We also welcome partnership with the many civil society organizations essential to promoting an open, free, global, interoperable, reliable, and secure Internet, and defending fundamental freedoms and human rights online. Partners in this Declaration intend to consult and work closely with stakeholders in carrying forward this vision.



EXHIBIT 6

DATA PRIVACY FRAMEWORK (DPF) OVERVIEW

Data Privacy Framework (DPF) Program Overview

The EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. Data Privacy Framework (UK Extension to the EU-U.S. DPF), and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) were developed to facilitate transatlantic commerce by providing U.S. organizations with reliable mechanisms for personal data transfers to the United States from the European Union / European Economic Area, the United Kingdom (and Gibraltar), and Switzerland that are consistent with EU, UK, and Swiss law.

Organizations participating in the EU-U.S. DPF may receive personal data from the European Union / European Economic Area in reliance on the EU-U.S. DPF effective July 10, 2023. July 10, 2023 is the date of entry into force of the [European Commission's adequacy decision](https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en) (https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en) for the EU-U.S. DPF and the effective date of the EU-U.S. DPF Principles, including the Supplemental Principles and Annex I of the Principles. The adequacy decision enables the transfer of EU personal data to participating organizations consistent with EU law.

Organizations participating in the UK Extension to the EU-U.S. DPF may receive personal data from the United Kingdom and Gibraltar in reliance on the UK Extension to the EU-U.S. DPF effective October 12, 2023, which is the date of entry into force of the adequacy regulations implementing the data bridge for the UK Extension to the EU-U.S. DPF. The data bridge for the UK Extension to the EU-U.S. DPF enables the transfer of UK and Gibraltar personal data to participating organizations consistent with UK law.

The effective date of the Swiss-U.S. DPF Principles, including the Supplemental Principles and Annex I of the Principles is July 17, 2023; however, personal data cannot be received from Switzerland in reliance on the Swiss-U.S. DPF until the date of entry into force of Switzerland's recognition of adequacy for the Swiss-U.S. DPF. The recognition of adequacy will enable the transfer of Swiss personal data to participating organizations consistent with Swiss law.

The Data Privacy Framework (DPF) program, which is administered by the International Trade Administration (ITA) within the U.S. Department of Commerce, enables eligible U.S.-based organizations to self-certify their compliance pursuant to the EU-U.S. DPF and, as

applicable, the UK Extension to the EU-U.S. DPF, and/or the Swiss-U.S. DPF. To participate in the DPF program, a U.S.-based organization is required to self-certify to the ITA via the Department's DPF program website (i.e., this website) and publicly commit to comply with the DPF Principles. While the decision by an eligible U.S.-based organization to self-certify its compliance pursuant to and participate in the relevant part(s) of the DPF program is voluntary, effective compliance upon self-certification is compulsory. Once such an organization self-certifies to the ITA and publicly declares its commitment to adhere to the DPF Principles, that commitment is enforceable under U.S. law.

Organizations that only wish to self-certify their compliance pursuant to the EU-U.S. DPF and/or the Swiss-U.S. DPF may do so; however, organizations that wish to participate in the UK Extension to the EU-U.S. DPF must participate in the EU-U.S. DPF. Such organizations' commitment to comply with the DPF Principles must be reflected in their self-certification submissions to the ITA, and at appropriate times in their relevant privacy policies.

Organizations that self-certified their compliance pursuant to the EU-U.S. Privacy Shield that wish to enjoy the benefits of participating in the EU-U.S. DPF must comply with the EU-U.S. DPF Principles; and organizations that self-certified their compliance pursuant to the Swiss-U.S. Privacy Shield that wish to enjoy the benefits of participating in the Swiss-U.S. DPF must comply with the Swiss-U.S. DPF Principles.

To rely on the EU-U.S. DPF and, as applicable, the UK Extension to the EU-U.S. DPF, and/or the Swiss-U.S. DPF, an organization must self-certify its adherence to the DPF Principles to the ITA and be placed and remain on the Data Privacy Framework List. The ITA will update the Data Privacy Framework List on the basis of annual re-certification submissions made by participating organizations and by removing organizations when they voluntarily withdraw, fail to complete the annual re-certification in accordance with the ITA's procedures, or are found to persistently fail to comply. The ITA will also maintain and make available to the public an authoritative record of U.S. organizations that have been removed from the Data Privacy Framework List and will identify the reason each organization was removed. The aforementioned authoritative list and record will remain available to the public on the Department's DPF program website.

Any organization removed from the Data Privacy Framework List must cease making claims that it participates in or complies with the EU-U.S. DPF and, as applicable, the UK Extension to the EU-U.S. DPF, and/or the Swiss-U.S. DPF and that it may receive personal information pursuant to the relevant part(s) of the DPF program. Such an organization must continue to apply the DPF Principles to personal information received while participating in the EU-U.S. DPF and, as applicable, the UK Extension to the EU-U.S. DPF, and/or the Swiss-U.S. DPF for as long as it retains such information.

Resources

All organizations interested in self-certifying their compliance pursuant to the EU-U.S. DPF and, as applicable, the UK Extension to the EU-U.S. DPF, and/or the Swiss-U.S. DPF should review the requirements in their entirety. To assist in that effort, the ITA's DPF team has compiled resources and addressed frequently asked questions below.

[Key Requirements for Participating Organizations \(/key-requirements\)](/key-requirements)

[How to Join the DPF Program \(/program-articles/How-to-Join-the-Data-Privacy-Framework-\(DPF\)-Program-\(part-1\)\)](/program-articles/How-to-Join-the-Data-Privacy-Framework-(DPF)-Program-(part-1))

[How to Re-certify under the DPF Program \(/program-articles/How-to-Re-certify-under-the-Data-Privacy-Framework-\(DPF\)-Program\)](/program-articles/How-to-Re-certify-under-the-Data-Privacy-Framework-(DPF)-Program)

[Frequently Asked Questions \(/program-articles/Frequently-Asked-Questions\)](/program-articles/Frequently-Asked-Questions)

[Self-Certify \(/application\)](/application)

[Data Privacy Framework List \(/list\)](/list)

[Audiences \(/US-Businesses\)](/US-Businesses)

[U.S. Businesses \(/US-Businesses\)](/US-Businesses)

[European Businesses \(/European-Businesses\)](/European-Businesses)

[European Individuals \(/Individuals-in-Europe\)](/Individuals-in-Europe)

[Data Protection Authorities \(/Data-Protection-Authorities\)](/Data-Protection-Authorities)

[About \(/Program-Overview\)](/Program-Overview)

[Program Overview \(/Program-Overview\)](/Program-Overview)

[Framework Text \(/EU-US-Framework\)](/EU-US-Framework)

[Inactive Participants \(/list\)](/list)

[News & Events \(/NewsEvents\)](/NewsEvents)

[Contact \(/assistance\)](/assistance)

EXHIBIT 7

Global Cross-Border Privacy Rules (CBPR) Declaration

April 21, 2022

Canada, Japan, the Republic of Korea, the Philippines, Singapore, Chinese Taipei, and the United States of America, as current economies participating in the APEC CBPR System,

Recognising

that growing Internet connectivity and the digitisation of the global economy have resulted in the rapid increase in the collection, use, and transfer of data across borders, a trend that continues to accelerate;

Conscious

that trusted cross-border data flows are indispensable—not just for big, multinational technology companies, but for companies across all sectors of the economy, and for micro, small- and medium-sized businesses, workers, and consumers as well;

Believing

that cross-border data flows increase living standards, create jobs, connect people in meaningful ways, facilitate vital research and development in support of public health, foster innovation and entrepreneurship, and allow for greater international engagement;

Acknowledging

that regulatory barriers threaten to undermine opportunities created by the digital economy at a time when companies are relying increasingly on digital technologies and innovations to continue business operations and recover economically;

Recognising

the importance of strong and effective data protection and privacy in strengthening consumer and business trust in digital transactions;

Acknowledging

the important contribution made by the Asia-Pacific Economic Cooperation (APEC) in developing the APEC CBPR System to foster cross border data flows and interoperability;

Do hereby declare as follows:

1. The establishment of a Global CBPR Forum to promote interoperability and help bridge different regulatory approaches to data protection and privacy;
2. The objectives of the Global CBPR Forum are to:
 - a. establish an international certification system based on the APEC Cross Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) Systems;
 - b. support the free flow of data and effective data protection and privacy through promotion of the Global CBPR and PRP Systems;
 - c. provide a forum for information exchange and cooperation on matters related to the Global CBPR and PRP Systems;

- d. periodically review data protection and privacy standards of members to ensure Global CBPR and PRP program requirements align with best practices; and
- e. promote interoperability with other data protection and privacy frameworks.

SCOPE OF ACTIVITY

3. The Global CBPR Forum is expected to:
 - a. promote expansion and uptake of the Global CBPR and PRP Systems globally to facilitate data protection and free flow of data;
 - b. disseminate best practices for data protection and privacy and interoperability; and
 - c. pursue interoperability with other data protection and privacy frameworks.

MODE OF OPERATION

4. Cooperation is intended to be based on:
 - a. the principle of mutual benefit and a commitment to open dialogue and consensus-building, with equal respect for the views of all members;
 - b. consultation and exchange of views among representatives of members, drawing upon research, analysis and policy ideas contributed by members and other relevant organisations; and
 - c. active multistakeholder participation in appropriate activities.

PARTICIPATION

5. Participation in the Global CBPR Forum is intended to be open, in principle, to those jurisdictions which accept the objectives and principles of the Global CBPR Forum as embodied in this Declaration.
6. Decisions regarding future participation in the Global CBPR Forum should be made on the basis of a consensus of all members.
7. Non-members may be invited to the meetings of the Global CBPR Forum upon such terms and conditions as may be determined by all members.

ORGANISATION

8. Meetings of Global CBPR Forum members should be held at least biannually to determine the direction and nature of activities within the framework of this Declaration and decide on arrangements for implementation. Meetings can be held in person or remotely.
9. Additional meetings may be convened as decided by all members.

EXHIBIT 8

U.S. DEPARTMENT OF THE TREASURY

United States – Singapore Joint Statement on Financial Services Data Connectivity

February 5, 2020

U.S. Treasury Under Secretary for International Affairs Brent McIntosh and Monetary Authority of Singapore Deputy Managing Director Jacqueline Loh met in Singapore to discuss the importance of data connectivity in financial services. At the conclusion of their meeting, Under Secretary McIntosh and Deputy Managing Director Loh issued the following joint statement:

Singapore – The United States and Singapore recognize that the ability to aggregate, store, process, and transmit data across borders is critical to financial sector development. The expanding use of data in financial services and the increasing use of technology to supply financial services offer a range of benefits, including greater consumer choice, enhanced risk management capabilities, and increased efficiency. These developments also pose new and complex risks for markets and challenges for policymakers and regulators. The United States and Singapore are committed to working together and with other countries to promote an environment in financial services that fosters the development of the global economy.

Consistent with these shared objectives, the United States and Singapore support allowing financial service suppliers to transfer data across borders and oppose generally applicable data localization requirements as long as financial regulators have access to data needed for regulatory and supervisory purposes. Data localization requirements can increase cybersecurity and other operational risks, hinder risk management and compliance, and inhibit financial regulatory and supervisory access to information. Data mobility in financial services supports economic growth and the development of innovative financial services and benefits risk management and compliance programs, including by making it easier to detect cross-border money laundering and terrorist financing patterns, defend against cyberattacks, and manage and assess risk on a global basis.

Based on this shared understanding, the United States and Singapore intend to seek to promote adoption and implementation of policies and rules in our bilateral and multilateral economic relationships to facilitate the following goals:

- Ensuring that financial service suppliers can transfer data, including personal information, across borders by electronic means if this activity is for the conduct of the business of a financial service supplier.
- Opposing measures that restrict where data can be stored and processed for financial service suppliers as long as financial regulators have full and timely access to data needed to fulfill their regulatory and supervisory mandate.
- Ensuring that financial service suppliers have the opportunity to remediate the lack of access to such data before being required to use or locate computing facilities locally.

The United States and Singapore also intend to share information on developments related to these issues and, as appropriate, encourage third countries to adopt policies consistent with this joint statement.

The United States and Singapore issue this joint statement without prejudice to governments' rights and obligations under the World Trade Organization (WTO), and to the exceptions contained in the WTO General Agreement on Trade in Services (GATS), such as the exceptions relating to protection of personal data privacy and confidentiality of individual records and accounts, and in related texts, such as the Annex on Financial Services and the prudential exception therein. In addition, relevant portions of this joint statement would not apply to the use and location of certain categories of financial service computing facilities. For greater certainty, this joint statement does not create binding obligations under domestic or international law.

###

EXHIBIT 9

United States International Cyberspace & Digital Policy Strategy

Towards an Innovative, Secure, and Rights-Respecting Digital Future

TABLE OF CONTENTS

Preface

Introduction

The Digital World: Opportunities and Challenges

- **Cyber Attacks and National Security Threats**
- **Competing Internet Norms**
- **Threats to Internet and Digital Freedom**
- **Challenges of the Digital Economy**
- **The Future of AI Technologies Governance**
- **Working with the Private Sector and Civil Society**

Building Digital Solidarity

ACTION AREA 1: Promote, Build, and Maintain an Open, Inclusive, Secure, and

- **Resilient Digital Ecosystem**

ACTION AREA 2: Align Rights-Respecting Approaches to Digital and Data

- **Governance with International Partners**

ACTION AREA 3: Advance Responsible State Behavior in Cyberspace and Counter Threats to Cyberspace and Critical Infrastructure by Building

- **Coalitions and Engaging Partners**

ACTION AREA 4: Strengthen and Build International Partner Digital Policy and

- **Cyber Capacity**

Conclusion

Preface

We are in a pivotal period of international relations, characterized by acute competition between nations, and shared global challenges like climate change, food and health security, and inclusive economic growth.

Technology will play an increasingly critical role in addressing these challenges. That is why at the State Department we have prioritized building capacity and expertise in cyber, digital, and emerging technology issues as part of our broader efforts to modernize diplomacy and ensure U.S. foreign policy delivers on the issues that matter most to the lives and livelihoods of the American people. As a key milestone in this work, I am pleased to share here the Department's International Cyberspace and Digital Policy Strategy.

Central to our strategy is the effort to build digital solidarity – working together to offer mutual assistance to the victims of malicious cyber activity and other digital harms; assist partners – especially emerging economies – in deploying safe, secure, resilient, and sustainable technologies to advance their development goals; and builds strong and inclusive innovation economies that can shape our economic and technological future. We are rallying coalitions of governments, businesses, and civil society to shape the digital revolution at every level of the technology “stack” – from building subsea cables and telecommunication networks, to deploying cloud services and trustworthy artificial intelligence, to promoting rights-respecting data governance and norms of responsible state behavior.

The United States will work with any country or actor that is committed to developing and deploying technology that is open, safe, and secure, that promotes inclusive growth, that fosters resilient and democratic societies, and that empowers all people.

Antony J. Blinken
Secretary of State

Introduction

The United States seeks to work with allies, partners, and stakeholders across the globe to shape the design, development, governance, and use of cyberspace and digital technologies to advance economic prosperity and inclusion; enhance security and combat cybercrime; promote and protect the exercise of human rights, democracy, and the rule of the law; and address transnational challenges. The United States believes in the critical role that the responsible uses of digital technologies and interconnected networks play in empowering people, and that an open, interoperable, secure, and reliable Internet enables new solutions to global challenges. Autocratic states and other actors, however, have used cyber and digital tools to threaten international peace and stability, harm others, exert malign influence, and undermine the exercise of human rights. An innovative, rights-respecting international cyberspace and digital technology policy strategy is foundational to U.S. strategic, security, economic, and foreign policy interests.

Leadership in cyberspace, the digital economy, and emerging digital technologies is central to advancing the U.S. vision set forth in the October 2022 National Security Strategy (NSS) of a “free, open, secure, and prosperous world.” As the lead foreign policy agency for the United States, the Department of State is advancing the 2023 National Cybersecurity Strategy (NCS) and its objectives of forging international partnerships to build an open, resilient, defensible, and rights-respecting digital ecosystem. It is also strengthening the Strategy’s dual approach of 1) rebalancing responsibility for defending cyberspace onto the government and private sector organizations that are the most capable and best positioned to reduce risks and of 2) realigning incentives to favor long term investment in cybersecurity through diplomacy, partnerships, and information-sharing. This strategy will be complemented by the U.S. Agency for International Development’s (USAID) forthcoming Digital Policy.

To advance the NSS and NCS, the Department of State, working with other federal agencies, has developed an international cyberspace and digital policy strategy focused on building broad digital solidarity through three guiding principles and four areas of action to be prioritized over the next three to five years.

Digital solidarity is a willingness to work together on shared goals, to help partners build capacity, and to provide mutual support.^[1] Digital solidarity recognizes that all who use digital technologies in a rights-respecting manner are more secure, resilient, self-determining, and prosperous when we work together to shape the international environment and innovate at the technological edge. Central to the tenets of digital solidarity are efforts to support allies and partners, especially emerging economies, to fully seize the opportunities presented by new technologies and sustainably pursue their economic and development goals. Digital solidarity aligns U.S. national interests with those of our international partners through compatible approaches to technology governance, sustains strong partnerships with civil society and the private sector, and embraces cybersecurity resilience built on a diversity of products and services made by trusted technology vendors. It highlights the mutual support that the United States and its partners offer one another to counter and respond to malicious cyber operations, cybercrime, and other digital harms, and promotes cooperative efforts among states and civic actors to defend and advance human rights. In addition, the concept of digital solidarity rests on efforts to build digital and cyber capacity so that partners are not only better able to build a defensible and resilient digital ecosystem over the long term but are also able to respond and recover quickly when incidents that threaten security, safety, and rights happen. The actions and efforts of this strategy are intended to demonstrate and build digital solidarity with partners across the globe.

The Department of State, with interagency partners, will build digital solidarity through four areas of action, fundamentally supported by three principles:

First, the Department of State will pursue an affirmative vision for cyberspace and digital technologies focused on delivering the benefits of technology and grounded in international commitments and international law, including international human rights law. The United States is committed to working with allies and partners toward a future in which people around the world use digital technologies safely to seek, receive, and impart information and ideas online as they participate in free, open, and informed societies; access educational

and economic opportunities in order to drive inclusive economic growth; and reliably receive critical services and information from their governments.

Second, the Department of State will integrate cybersecurity, sustainable development, and technological innovation throughout our approach. Cybersecurity, data security, and cyber-resilience are prerequisites for and enablers of economic growth and healthy civic spaces where citizens can exercise their rights; countries cannot build and support an innovative digital ecosystem that benefits everyone without first securing it.

in **Third**, the Department of State will implement a comprehensive policy approach that uses the appropriate tools of diplomacy and international statecraft across the entire digital ecosystem. This ecosystem includes but is not limited to hardware, software, protocols, technical standards, providers, operators, users, and supply chains spanning telecommunication networks, undersea cables, cloud computing, data centers, and satellite network infrastructure, operational technologies, applications, web platforms, and consumer technologies as well as Internet of Things (IoT), artificial intelligence (AI) and other critical and emerging technologies. [2]

In line with these three principles, the Department of State will build digital solidarity through four areas of action, which flow from creating and governing digital ecosystems to defending against malicious actions and delivering assistance and building resilience:

1. Promote, build, and maintain an open, inclusive, secure, and resilient digital ecosystem;
2. Align rights-respecting approaches to digital and data governance with international partners;
3. Advance responsible state behavior in cyberspace, and counter threats to cyberspace and critical infrastructure by building coalitions and engaging partners;
4. Strengthen and build international partner digital and cyber capacity.

The Department of State will reinforce efforts to forge digital solidarity by its proactive participation in international, multilateral, and multistakeholder bodies where obligations, norms, standards, and principles are developed that impact cyberspace, digital, Internet, and technology issues. While progress in these venues can be slow and incremental – frequently as a function of their objectives—but a lack of U.S. leadership in international fora may allow adversaries to fill the void and shape the future of technology to the detriment of U.S. interests and values.

Nearly all foreign policy issues – from international security to democracy and human rights to global health and climate change – will be shaped by today’s investments in cyberspace and digital technology diplomacy. The Department of State will lead the interagency process to set, coordinate, and integrate cyber and digital technology diplomacy efforts to advance U.S. national interests and values over the next decade and beyond. The efficacy of U.S. efforts and related messaging, however, depends in part on consistency and action at home, both in policy and on execution. For example, U.S. technology companies are the leaders in the first wave of digitalization and are now pushing the innovative edge on AI systems. The United States, therefore, should be a leader in promoting accountability for technology platforms. We need to help lead the responsible design, development, governance, and use of the next wave of technologies in line with democratic values and respect for human rights.

The United States has great strengths that serve us in shaping the future of digital technologies: strong alliances and partnerships; the world’s most innovative technology companies; a transparent, inclusive, and enabling policy environment; and robust and engaged civil society and technical communities. The United States is mobilizing these resources to implement this affirmative and proactive international cyberspace and digital strategy.

The Digital World: Opportunities and Challenges

Figure 1. Abstract representation of a digital, connected world. (Adobe Stock photo.)

Digital technologies have revolutionized how we live, work, and learn. They, along with expanded connectivity, not only power economic growth but also facilitate the exercise of human rights and improve access to education, financial, and social services. Digital technologies have created new markets and opportunities and have enabled businesses to reach a vast customer base beyond their country's borders. New digital tools have energized civic and political engagement, democratized information and knowledge, been used to hold governments and companies accountable, and increased the transparency, efficiency, and responsiveness of public services.

Looking ahead, these technologies can unlock unparalleled opportunities to address some of the most pressing global challenges, including climate change, economic and social inequality, and health crises. By harnessing the power of data analytics, AI, and real-time connectivity, we can create smarter, more sustainable cities, improve agricultural yields using fewer resources, and make healthcare accessible to even the most remote communities. These technologies enable the development of green energy solutions, fostering a transition towards cleaner and less expensive energy. Advances in data collection, modeling, simulation, and analysis will allow scientists to accelerate research and discovery and identify patterns invisible to humans alone, catalyzing rapid and unexpected breakthroughs. By connecting people and information like never before, digital technologies can foster a more inclusive, equitable world where opportunities for prosperity and well-being are abundant for all.

At the same time, significant harms have accompanied the rapid expansion and evolution of digital technologies. The geopolitics of cyberspace are competitive and complex. Malicious state and non-state actors have developed the capabilities and demonstrated the intent to place critical infrastructure, national critical functions, and even individual citizens at risk. Authoritarian states are promoting competing forms of technology governance that use mass surveillance, privacy-invasive data collection practices, and online censorship tools that threaten the open, interoperable, secure, and reliable Internet. Technology provides new vectors and tools for crime, and the dramatic spread of personal information online has expanded the threat environment. The proliferation and misuse of commercial spyware is a threat to national security, targeting U.S. officials abroad; commercial spyware has also been used to, target and intimidate perceived opponents, facilitate efforts to curb dissent, and thus undermine democratic values. Journalists, activists, educators, researchers, women and girls, and marginalized groups are often the victims of unlawful surveillance, online harassment, and abuse. Countries and technology platforms each have a role to play in mitigating algorithmic bias

and information manipulation, as well as violent extremist messaging, child sexual abuse material (CSAM), technology-facilitated gender-based violence, and other harmful content.

These challenges are pressing and high stakes. Innovation, partnerships, collaboration, coalition building, information sharing, mutual support, assistance, and the other tools of diplomacy are essential to ensuring that digital technologies defend and advance individual freedom and promote economic prosperity.

Cyber Attacks and National Security Threats

Adversarial cyber campaigns can cumulatively produce strategic loss for the United States and its allies, and they increasingly put the development goals of emerging economies at risk. Cyber threats continue to intensify in both frequency and severity, with increased risks of escalatory or uncontrolled cyber activity. State actor and non-state actors, including criminals, terrorists, and violent extremists, have tremendous incentives to invest in and exploit digital technologies to threaten our and other's national interests.

The People's Republic of China (PRC) presents the broadest, most active, and most persistent cyber threat to government and private sector networks in the United States. Beijing has mounted cyber espionage operations against government, commercial, and civil society actors and has increased its ability to carry out destructive and disruptive cyberattacks. The PRC is capable of launching cyberattacks that could disrupt oil and gas pipelines, rail systems, and other critical infrastructure services within the United States or its allies and partners. Attempts to compromise critical infrastructure by PRC actors are designed in part to pre-position themselves to be able to disrupt or destroy critical infrastructure in the event of a conflict—either to either prevent the United States from being able to project power into Asia, or to affect our decision-making during a crisis by instigating societal chaos inside the United States. Both state-sponsored activity and that of PRC-linked actors are part of the PRC cyber approach.

A persistent cyber threat, the Russian government is refining its cyber espionage, cyberattack, influence, and information manipulation capabilities to threaten other states and to weaken U.S. alliances and partnerships. Russia continues to provide safe haven to transnational cybercriminal actors, such as disruptive ransomware gangs. Russia's cyberattacks in support of its 2022 unprovoked invasion of Ukraine were intended to destabilize the Ukrainian state and

military and have resulted in spillover effects onto civilian critical infrastructure in other European countries. As the war continues, Russian government and Russian government-aligned cyber actors have targeted Ukraine with cyber operations against the public and private sectors, information manipulation and online influence operations, and attempts to divert and censor Ukrainians' access to the Internet. Russia appears particularly focused on improving its ability to target critical infrastructure in the United States to demonstrate its ability to damage infrastructure during a crisis.

The governments of the Democratic People's Republic of North Korea (DPRK) and Iran have both increased the scale of their malicious cyber activities. Facing multiple rounds of international sanctions, the DPRK evades controls through cybercrime and the theft of cryptocurrencies. DPRK hackers continue to gather intelligence on military technology targets as well as academia and think tanks. In addition, the DPRK dispatches thousands of skilled IT workers around the world to generate fraudulent revenue that ultimately contributes to its weapons of mass destruction and ballistic missile programs despite U.S. and UN sanctions.

Iran's growing expertise and willingness to conduct cyber operations threaten the security of networks and data globally. Iran's opportunistic approach to cyberattacks makes critical infrastructure owners in the United States susceptible to being targeted by Iranian actors, particularly when Tehran believes that it must demonstrate it can push back against the United States in other domains. Iranian actors have engaged in a wide range of intelligence-gathering operations around the world, and—in the wake of Hamas' atrocities on October 7, 2023, and Israel's military operations in Gaza—have conducted wiper, website takedown, hack and leak operations, espionage, and online information manipulations campaigns. Iranian actors have also conducted malicious activity against operational technology devices used in the water sector and other industries.

Cyber criminals and criminal syndicates operating in cyberspace now represent a specific threat to the economic and national security of countries around the world. Cybercrime and online fraud cause significant harm to economic development, with small- to medium-sized enterprises and financial service providers especially at risk. According to one estimate, the global cost of cybercrime is estimated to top \$23 trillion in 2027. **[3]**

Ransomware incidents have disrupted critical functions, services, and businesses, from energy pipelines and food companies to schools and hospitals. Ransomware attacks against the healthcare industry can undercut the level of care provided to patients and others under care.

Total economic losses from ransomware attacks worldwide continue to climb, reaching into the billions of U.S. dollars annually. Ransomware groups often operate out of safe haven jurisdictions whose governments, often adversaries like Russia, do not cooperate with law enforcement and sometimes encourage, direct, sanction, or tolerate their activities.

Terrorists' and violent extremists' use of digital technologies also represents a threat to the national security of the United States and its allies and partners. Malign activities include the use of information and communications technologies (ICT) to spread violent propaganda; encourage radicalization and mobilization to commit violent acts; recruit individuals to terrorist organizations; to train, plan, and coordinate attacks; and finance terrorist acts.

Competing Internet Norms

Russia, the PRC, and other authoritarian states have promoted a vision of global Internet governance that centers on domestic control and top-down, state-centric mechanisms over the existing bottom-up multistakeholder processes. Russia and the PRC attempt to use multilateral fora like the UN to exert their influence on and appeal to developing countries, with the aim of reshaping the global cyber and technology policy landscape to advance an authoritarian agenda while hampering the United States and its allies. Russia, the PRC, and others seek to reshape norms governing cyberspace, undermine the technical underpinnings of the Internet, and dilute accountability for authoritarian countries' malicious use of cyberspace capabilities.

Authoritarian governments are working to weaken global commitment to universal human rights enshrined in the Universal Declaration of Human Rights and international legal instruments, such as the UN Charter and the International Covenant on Civil and Political Rights. Authoritarian governments, most notably the PRC, are actively working to co-opt and redefine well-established terminology related to "democracy" and "human rights" in the context of international technology policy development, including through their input into the UN Pact for the Future process and its Global Digital Compact.

Threats to Internet and Digital Freedom

Authoritarian and illiberal states are seeking to restrict human rights online and offline through the misuse of the Internet and digital technologies. Governments are closing and siloing the Internet: suppressing dissent through Internet and telecommunications shutdowns, virtual blackouts, restricted networks, and blocked websites.

The PRC has developed a massive system of surveillance, and its firms are now exporting their regulatory approach and technical capabilities to facilitate other governments' monitoring and repression. Beijing has also used cyber means to target people beyond its borders, including journalists, dissidents, and individuals it views as threats to Chinese Communist Party narratives, policies, and actions. In the wake of its full-scale invasion of Ukraine in 2022, the Russian government blocked access to foreign websites and increased censorship and surveillance of domestic users. The Iranian government continues to rely on Internet restrictions, filtering, and surveillance to repress opposition to the regime.

A growing number of governments, including backsliding democracies, are misusing digital tools in ways that violate or abuse the individual's right to be free from arbitrary or unlawful interference with one's privacy, and restricting and threatening individuals' rights to freedoms of expression, association and peaceful assembly. Commercial spyware, AI-enabled facial recognition software, and other surveillance technologies are misused against journalists, human rights defenders and other activists, women, and members of marginalized groups, including beyond countries' borders. Technology-facilitated gender-based violence (TFGBV) chills speech, impedes privacy and freedom of expression, and undermines the ability of women, girls, and LGBTQI+ individuals to participate in democracy, governance, and civic life.

The proliferation of online manipulation, in combination with threats posed by foreign adversaries seeking to interfere with information integrity, pose fundamental threats to democracy, undermining trust in institutions, threatening electoral processes, and sowing discord within and between countries. PRC actors have increased their capabilities to conduct covert influence operations and disseminate disinformation. Even if Beijing sets limits on these activities, individuals not under its direct supervision may attempt election influence activities they perceive are in line with the PRC's goals. The Russian government remains a serious foreign influence threat because of its wide-ranging efforts to try to divide Western alliances and undermine U.S. global standing. Recently, Russian influence actors have adapted their efforts to better hide their hand.

Challenges of the Digital Economy

Some 2.6 billion people still do not have access to the Internet, leaving a third of the world unconnected. This situation presents an economic development challenge for many countries and a strategic challenge for the United States and its allies and partners. Left unaddressed, the digital divide not only imperils efforts to build a strong digital ecosystem, but also threatens to increase income inequality and instability in emerging economies. The digital divide disproportionately affects women and other marginalized groups. For example, 80 percent of women in low-income countries do not use the Internet. [4]

As the world has increasingly digitalized, countries around the world are grappling with how to approach the digital economy in a way that takes advantages of its benefits, addresses its risks, and expands its reach to more people. Governments are developing differing regulatory approaches to a range of policy issues, such as protecting children's safety, health, and privacy, tackling TFGBV, addressing anti-competitive behavior, guaranteeing equitable access to connectivity and technology, building trusted digital infrastructure, and promoting trusted cross-border data flows.

A growing number of countries are promoting digital public infrastructure (DPI) as critical to achieving economic growth, good governance, and the UN sustainable development goals (SDGs). The definition of DPI is evolving, but generally encompasses networked open technology standards designed for the public interest, an enabling regulatory environment, and a community of market players driving innovation. While some of the most prominent models have included digital identification, digital payments, and data platforms for sharing and storing data, there is no one-size-fits-all solution. DPI models need to be grounded in safeguards, including human rights protections, and such models should be interoperable.

U.S. government and private sector actors seek to leverage data and the digital economy for positive economic and social benefits: preserving openness while protecting privacy, promoting safety, and mitigating harms. The Department of State, working with other agencies, looks to shape markets and safeguard innovation from regulatory excesses. Although there is an increasing willingness by some countries to embrace narratives of digital sovereignty and protectionism by blocking access to their markets, unduly preventing cross-border data flows,

and preferencing domestic manufacturers and service providers, we continue international engagement to enhance interoperability, security, and market access.

Many states are promoting digital technologies for economic growth while trying to maintain autonomy and neutrality. They are looking to build digital infrastructure quickly and cheaply and seeking assistance to combat cybercrime and develop cybersecurity capacities. Yet the PRC government distorts markets to advantage PRC-based hardware, software, and services suppliers that compromise the security of the customer. By contrast, the United States seeks to provide the emerging and developing world with financially sound alternatives to unsustainable initiatives. The Department of State is committed to working with allies and partners to offer and deploy secure technologies that allow countries and civic actors around the world to build digital infrastructure and improve cybersecurity across sectors, offering direct benefits to governments while helping to ensure the protection of the human rights and privacy of their citizens that will enable an inclusive digital economy.

The Future of AI Technologies Governance

The uncertainty and complexity that characterizes the geopolitical competition over these digital technologies is compounded by the fact that we sit at the cusp of another technological revolution. The revolution in AI systems may occur at an even faster pace than the development and adoption of the Internet. AI technologies could be powerful tools for expanding knowledge, increasing prosperity and productivity, and addressing global challenges, and AI tools may help advance the seventeen UN SDGs. AI applications have the further potential to improve many aspects of citizens' lives including food security, health applications, good governance and democratic consolidation, and natural disaster preparedness and prevention.

The rapid growth of AI technology, however, comes with the significant risk that its use may exacerbate inequality and economic instability, stifle competition, cause consumer harm, aggravate discrimination and bias, invade privacy, enhance malicious cyber activity, and improve authoritarian capabilities for surveillance and repression. AI will challenge how we compensate for the uses of intellectual property as well as authenticate, label, or detect synthetic content. AI may also require workforce adaptations across economies; the rising energy demands of high-end AI chips and data centers could become a significant barrier to developing local capabilities.

Further, state and non-state actors have been observed using generative AI systems for malicious purposes, including to manipulate and disseminate disinformation at speed and scale. Many AI technologies are also dual use, lending themselves to new military and national security capabilities that may lack appropriate human rights and civil liberty protections and other safeguards. AI can advantage both the attacker and defender in cyberspace, and the systems themselves are subject to data poisoning and other types of malicious activities.

The question of how to balance risk and rewards looms large for governments and civil society around the world. The United States is working with allies and partners to move quickly to address the ways in which artificial intelligence can potentially destabilize societies while preserving its benefits—and, crucially, staying true to democratic values and protecting human rights. A critical part of this work is not only safeguarding an open and independent research environment but also partnering with emerging economies in the development and deployment of AI technologies. Helping to provide unrestricted access to an open, interoperable, reliable, and secure Internet while demonstrating how AI can serve a shared agenda across the globe can help reduce the risk that the AI revolution will contribute to global instability and diminish our ability to address global challenges.

Working with the Private Sector and Civil Society

Competition, consumer choice, vibrant private sector investment, and a robust civil society are the hallmarks of an open, inclusive, and secure digital ecosystem. The Department of State cannot accomplish its objectives without strong partnerships with the private sector, civil society, academic, and technical communities. New innovations spring from the private sector, and the decisions tech companies make on how their systems are developed and deployed have profound implications for how U.S. values and interests are realized—including protecting users' safety and privacy. U.S. officials rely on a range of private sector, academic, and civic actors for insights into technology developments, and private sector and trade association stakeholders often provide early warning of discriminatory regulations that explicitly target American companies. Trusted technology suppliers, including small- and medium-sized enterprises, are essential partners in efforts to expand connectivity through open, secure, and resilient networks across the globe.

Civil society groups are working to ensure that individuals can access and pursue opportunities online free from unlawful surveillance and privacy-invasive data collection practices and are working to counter harmful propaganda and disinformation in digital spaces. Civil society and the technical community are often the first to recognize, warn of, and seek solutions to threats to human rights online and offline. As Internet freedom continues to decline in parts of the world, civil society activists, human rights defenders, and the journalists covering their activism are often leading the push back in digitally repressive societies, often at great personal risk. Additionally, civil society, the academic and technical community, and private sector actors play a crucial role in upholding the multistakeholder model of Internet governance, which is increasingly under threat.

The private sector, civil society, and the technical community are essential in helping defend against malicious cyber activities. In 2022, the private sector aided Albania in the wake of Iranian cyberattacks and, during Russia's full-scale invasion of Ukraine, technology firms and cybersecurity companies provided services, tools, and threat intelligence to help Ukraine defend government and critical infrastructure networks. They migrated data storage and cloud hosting services to counteract Russian efforts to erase critical data and provided Internet and telecommunication services that helped keep government agencies and businesses operating. Non-governmental organizations and academic research groups have exposed the threat posed by the proliferation and misuse of commercial spyware against journalists, activists, and marginalized groups.

Public-private partnerships are essential to cyber and digital diplomacy, and they need to be flexible and adaptable. Cyber defense may require new ways to scale, supply, and license cyber defense services and products in a crisis and may be difficult to launch and sustain in a different regional context. Repressive governments are developing new methods to control digital technologies and to manipulate and interfere with information flows. To address these and other evolving challenges, the Department of State will continue to expand contact with and solicit input from a wide range of civil society and private sector actors. In addition, the United States will continue to work with allies and partners to advance a multistakeholder approach to digital and data governance.

Building Digital Solidarity

The United States believes digital technologies can and should be used to put people on a path to prosperity, solve global challenges, and build a better future for all. The Department of State will work with allies, partners, and stakeholders to promote an affirmative vision for cyber and digital technologies: one in which people around the world use cyberspace and digital technologies to advance economic prosperity and inclusion; enhance security and combat cybercrime; promote and protect human rights, gender equity and equality, democracy, and the rule of the law; and address transnational challenges. As part of this approach, the United States, allies, and partners will demonstrate the advantages of an open, interoperable, secure, and reliable Internet; serve as the partner of choice in the research, design, development, and deployment of digital and emerging technologies; and jointly impose consequences for behavior that runs counter to internationally accepted norms of state behavior. The Department of State will also work with and support emerging economies' efforts to improve cybersecurity and increase their cyber-resilience.

Each of the Strategy's four action areas—promote, build, and maintain an open, inclusive, secure, and resilient digital ecosystem; align rights-respecting approaches to digital governance; advance responsible state behavior, counter malicious activity, and offer mutual support; and strengthen digital and cyber capacity building assistance—reflects aspects of the Department of State's vision of digital solidarity. Moving forward, the Department of State will work to bring a wide range of partners across the globe into the process of building and extending digital solidarity. We welcome all those who seek to develop and deploy technologies that are open and secure, promote inclusive growth, foster resilient and democratic societies, and empower all, including the most vulnerable.

Figure 2. Secretary Blinken and Deputy Secretary Sherman Visit the new Cyberspace and Digital Policy Bureau at the U.S. Department of State in Washington, D.C., on April 4, 2022. (U.S. Department of State photo.)

ACTION AREA 1: Promote, Build, and Maintain an Open, Inclusive, Secure, and Resilient Digital Ecosystem

Digital solidarity rests on and is reinforced by innovation across an open, inclusive, secure, and resilient digital ecosystem. Though the United States is a major power in digital, critical, and emerging technologies, we are not able to—nor should we—go it alone. Rather, the United States, allies, and partners are all made more prosperous, self-determining, and resilient when we work together to catalyze, support, and sustain rapid technological development on a range of critical technologies.

In close coordination with allies, partners, the private sector, and civil society, the Department of State continues to campaign for open, interoperable, secure, trusted, and reliable telecommunication networks, especially on fifth-generation wireless networks (5G). The White

House, Department of State, USAID, Department of Commerce, and the Federal Communications Commission (FCC) are engaged in discussions with allies and partners about deploying 5G mobile networks using trusted vendors and the future of 6G. Digital technologies are not limited to wireless technologies, and the Department of State and other agencies are coordinating with allies and partners on the development, deployment, and security of cloud infrastructure and data centers, undersea cables, and satellite communications. In addition, at all UN bodies the United States aims to promote—at a high level—the development, deployment, and use of rights-respecting digital technologies.

Line of Effort 1: Promote Development and Adoption of Open, Inclusive, Secure, and Resilient Telecommunication Networks

5G applications are rapidly evolving—expanding digital connectivity in new ways and creating new cybersecurity vulnerabilities. Telecommunication networks should be built using products from trusted suppliers that operate, and have supply chain partners that operate, primarily in countries that respect rights through consistent application of the law through an independent judiciary, in accordance with the principles reflected in the Organisation for Economic Co-operation and Development (OECD) Declaration on Government Access to Personal Data Held by Private Sector Entities. Telecommunications networks should not be built using products from suppliers subject to the control or influence of an authoritarian regime, and without meaningful, independent checks and balances or judicial recourse against government demands. International 5G-related principles, such as the Prague Proposals on 5G Security and Prague Proposals on Telecommunications Supplier Diversity, support market competitiveness and the diversity of trusted 5G equipment vendors.

These efforts also extend to the Partnership for Global Infrastructure and Investment's Digital Infrastructure pillar. Recognizing that cost is often the primary driving factor in ICT procurements, the United States is supporting governments, middle-mile internet infrastructure providers, and Internet service providers to develop greater competition and diversity in telecommunications supply chains, particularly through the Digital Connectivity and Cybersecurity Partnership (DCCP). DCCP is a whole-of-government effort, led by the Department of State, to provide capacity building, technical assistance, and project design and financing in support of an open Internet and enhanced cybersecurity.

In addition, the CHIPS and Science Act allocated \$500 million to the International Technology Security and Innovation (ITSI) Fund for the Department of State to support the development and adoption of secure semiconductor supply chains and telecommunications networks. The United States will use this funding to continue to work with partners to put in place policy and regulatory frameworks for secure ICT ecosystems and to level the playing field for secure and trustworthy vendors.

Along with helping build secure networks, digital solidarity is also expressed through efforts to build digital infrastructure that promotes competition, advances consumer choice, and puts communities and individuals in charge of their digital lives and resources. Recognizing the need to attract capital and de-risk potential digital infrastructure investment, USAID—with funding from DCCP—launched a blended finance program called Digital Invest that partners with fund managers and project developers to expand access to Internet connectivity and digital financial services in emerging markets worldwide. To date, Digital Invest's 13 partners have leveraged an initial \$8.45 million in Department of State and USAID funding to raise over \$300 million in investment capital for digital finance and Internet service providers in emerging markets that use secure network equipment, catalyzing an additional \$1.15 billion in follow-on funding from third-party investors.

U.S. foreign assistance programs will also increase competition in the market and promote telecommunications supplier diversity by advancing the development of open and interoperable interfaces and protocols, such as Open Radio Access Networks (Open RAN). This open network architecture eases the ability for new suppliers to enter the market, lowers costs for deployment, and speeds innovation. Open RAN presents opportunities for emerging economies to participate directly in the supply chain, such as through local assembly and software development. Just as important, Open RAN offers alternatives for the reliance on technology from untrusted vendors. As a result, the Department of State will continue to support efforts such as funding commercial trials, feasibility studies, reverse trade missions, and workforce education and awareness activities that promote Open RAN. The United States will continue collaborating with the governments of Australia, Canada, Japan, and the United Kingdom on telecommunications supply chain diversification and related issues through the Global Coalition on Telecommunications, launched in October 2023.

Working with other governments and the private sector, the United States is also preparing for a new wave of innovation. Within the next decade, 6G will within the next decade bring even

higher speeds, larger capacity, and lower latency to wireless communication. Building open and interoperable network architectures such as Open RAN into 6G development from the beginning will help ensure supplier diversity and supply chain resilience. In February 2024, the United States—with Australia, Canada, the Czech Republic, Finland, France, Japan, the Republic of Korea, Sweden, and the United Kingdom—endorsed shared principles for the research and development of 6G wireless communication systems.

Line of Effort 2: Further Common Understandings and Shared Principles for the Secure Use and Trustworthiness of Cloud Services, Data Centers, and Related Infrastructure Technologies

Cloud computing has become an essential enabler of the digital transformation of economies and businesses. By providing on-demand access to scalable computing resources in a reliable and cost-effective manner, cloud services allow governments and businesses to deliver more secure and resilient services to their citizens and customers. Moreover, cloud services were proven to be a strategic asset as Russian forces physically destroyed Ukrainian facilities holding critical data. Migration of government information technology infrastructure to the cloud improved resilience and preserved information essential to the operation of the economy and government.

U.S. cloud computing and data center firms compete globally and offer services to a broad international customer base while, in parallel, the United States government actively partners with foreign governments to promote the fair and safe use of cloud computing resources. At the same time, providers from authoritarian states are globalizing, and they are often more responsive to short-term local economic development goals, providing packages that include financial subsidies, local cloud infrastructure, and workforce training. Cloud services and data centers are also a source of tension with close trade partners. Some have threatened to exclude U.S. cloud providers from their markets in part because of concerns about access to and control of data, despite the U.S. Clarifying Lawful Overseas Use of Data (CLOUD) Act providing for agreements to allow for consistent protections based on the rule of law. The Department of State is committed to reaching a common understanding with our international partners on the fair and safe use of cloud computing resources.

In addition, the Department of State will work with international partners and the private sector to address the costs and increase support for building secure cloud infrastructure in emerging economies. DCCP is reinforcing these efforts through the support of feasibility studies, reverse trade missions, financing, and training programs, such as training grants in the Philippines to support the provision of cloud computing capabilities.

Figure 3. Global Submarine Cable Map 2024. (Illustration by TeleGeography)

Line of Effort 3: Enhance Security and Resilience of Undersea Cables

Undersea cables carry more than 95 percent of the world's digital traffic. As data continues to proliferate and increase exponentially, so too does demand for cables and other transmission systems. Disruption or destruction of the cables as a result of accidents, natural disasters, or malicious actions could isolate a county, threaten national security, and result in billions of dollars of damage to the economy. Choices made about which vendors to rely on for undersea

cable infrastructure, maintenance, and repair operations can either drive development and innovation or lead to new forms of dependency and insecurity. As a result, the Department of State, in coordination with other agencies, will prioritize enhancing the security and resilience of undersea cables.

U.S. firms and other trusted suppliers are leading producers of many network components, embedded technologies, and related services for undersea cables, and they are investing in and financing new undersea cables connecting all regions of the world. The U.S. government will continue to support U.S. and other trusted suppliers in the installation, operation, maintenance, and repair of secure infrastructure as well as to promote a regulatory environment that enables continued investments.

Since 2021, the Department of State has implemented the CABLES program throughout the East Asia Pacific region, responsibly informing essential telecommunications and cables infrastructure stakeholders of the perils of choosing untrusted suppliers. The United States provided capacity building to support five countries using U.S. technology for the South-East Asia-Middle East-Western Europe 6 cable (SMW6), and separately it provided over \$22 million in partnership with Australia and Japan to help fund the East Micronesia Cable being built by a Japanese firm. In October 2023, the United States announced that, working with Congress, it would provide, along with Australia, investments totaling \$65 million to fund future undersea cable connectivity for Pacific Island countries in order to facilitate access to global markets and the realization of regional connectivity goals. In support of these policy objectives, the United States will continue engaging with the G7 and other multilateral groups to strengthen trusted, multi-layered global connectivity that provides data route diversity, resiliency, and redundancies.

Line of Effort 4: Pursue Shared Interests in the Development, Use, Resilience, and Security of Satellite Communication Networks

Satellite communications remain a vital capability for connecting the world and delivering global access to information. Geostationary orbit (GEO) satellites have served this mission for decades and will continue to do so for decades to come. Newly deployed satellite technologies, including low-earth orbit (LEO) satellites, are increasingly important to the United States, its allies, and partners as we work to connect the unconnected. The distributed nature of proliferated satellite

constellations offers resilience, and LEO satellite communication services can increasingly be deployed rapidly to cover disaster or conflict zones. Moreover, the ability of LEO satellite services to bring broadband communications to almost every inch of the planet raises the possibility of expanding Internet access in a rights-respecting manner, closing the digital divide, and advancing UN Sustainable Development Goals.

U.S. firms lead in the development and deployment of GEO and LEO satellite communication services, but other countries, including our strategic competitors, are investing in new technology capacities. The PRC is planning a constellation of about 13,000 satellites, with a clear government mandate and significant financial subsidies. Some states, concerned that LEO satellite capabilities will undermine their ability to control information flows, are raising market access barriers, such as setting stringent domestic equipment requirements or forbidding foreign ownership. Some governments and non-government stakeholders have also raised concerns in multilateral bodies about increased space debris, interference with astronomy, increased cases of radio frequency interference among LEO satellites or from LEO to GEO satellites, and other potential negative impacts of LEO satellite networks. Some countries, although they are interested in the connectivity benefits LEO satellite systems could bring, are unfamiliar with the systems and lack effective regimes to support market entry and licensing. In addition, space systems and assets introduce vulnerabilities to U.S. and allies' critical infrastructure that our adversaries are willing to exploit.

The Department of State will cooperate with partners and allies to pursue shared interests in the development, use, resilience, and security of LEO satellite systems. The Department of State will work to expand global access to secure services through the International Telecommunication Union (ITU), remove barriers to LEO satellite system providers, and increase multilateral assistance for satellite services for underserved areas. The Department of State, along with other agencies, will also facilitate international cooperation on research and development in LEO satellites. The United States will also promote norms, guidelines, and best practices, including the development of licensing and regulatory regimes, for the secure, safe, and sustainable use of LEO satellites, as well as work with allies and partners on enhancing space cybersecurity and critical infrastructure resilience and security.

Line of Effort 5: Enhance the International Telecommunication Union's Effectiveness, Transparency, and Accountability

Responsible, forward-looking, inclusive, and transparent leadership by the ITU on telecommunications standards, telecommunications and ICT development, closing digital divides, and radio frequency spectrum is vital to U.S. development, defense, and economic priorities. The United States has long supported the work of the ITU in its core competencies, including global radiofrequency spectrum harmonization and advancing the development of the world's telecommunications networks by enhancing connectivity and interoperability. Since Secretary-General Doreen Bogdan-Martin's 2022 election, the United States has been working with other member states and partners to help her deliver on her vision to expand digital connectivity and inclusion; strengthen partnerships and stakeholder collaboration; empower and engage youth; and enhance the ITU's organizational effectiveness, transparency, and accountability to achieve its overall goals.

ACTION AREA 2: Align Rights-Respecting Approaches to Digital and Data Governance with International Partners

Digital solidarity recognizes the necessity of the domestic governance of digital and emerging technologies but seeks to develop shared mechanisms that will help maintain an open, interoperable, secure, and reliable Internet as well as trusted cross-border data flows. It works to foster democratic values-based and rights-respecting policies.

To advance the NSS and the NCS effectively, promoting, building, and maintaining a secure digital ecosystem must be accompanied by efforts to make digital and data governance compatible across allies and partners through greater alignment, mutual recognition, and reciprocity of policies. The Department of State, along with other federal agencies, is building and reinforcing digital solidarity through support for the trusted flow of data; advocacy for multistakeholder, risk-based approaches to digital and data governance; and the promotion of shared values and governance principles for critical and emerging technologies. The Department of State, in collaboration with the Department of Commerce and other agencies, is expanding its

capacity to engage in international standards development organizations and to coordinate with industry and civil society to ensure robust participation by U.S. stakeholders in standards setting processes and other international fora. The United States is also working with allies and partners to advance a common, rights-respecting vision for the digital future; negotiate a rights-respecting cybercrime treaty; and defend information integrity.

Line of Effort 1: Support the Trusted Flow of Data and Advocate for Multistakeholder, Risk-Based Approaches to Digital and Data Governance

Digital solidarity is further built and reinforced through the joint development, harmonization, and mutual recognition of rights-respecting approaches to data governance and digital trade. This work is currently ongoing through mechanisms such as Indo-Pacific Economic Framework for Prosperity (IPEF), Digital Transformation with Africa initiative (DTA), the Americas Partnership for Economic Prosperity (APEP), the G7, OECD, TTC, and the Quad.

The United States supports the trusted free flow of data and an open Internet with strong and effective protections for individuals' human rights and privacy and measures to preserve governments' abilities to enforce laws and advance policies in the public interest. Legitimate concerns about data privacy can be addressed through protective mechanisms that follow the data while at the same time facilitate cross-border data flows and strengthen global cooperation among enforcement authorities. The United States will continue championing trusted cross-border data flows by promoting data transfer mechanisms that improve interoperability between different data privacy regimes. Working alongside our interagency partners, the Department of State supported the negotiation and implementation of the EU- U.S. Data Privacy Framework; the development of the OECD Declaration on Trusted Government Access to Data Held by the Private Sector, which identifies commonalities in the privacy safeguards democratic governments follow when accessing data for legitimate law enforcement and national security purposes; as well as initiatives on Data Free Flow with Trust at both the G7 and the OECD. The Department of State works with the Department of Justice to clarify application of the U.S. Clarifying Lawful Overseas Use of Data (CLOUD) Act and to negotiate bilateral agreements under the act.

Along with Australia, Canada, Japan, the Republic of Korea, Mexico, the Philippines, Singapore, and Taiwan, the United States launched the Global Cross-Border Privacy Rules (CBPR) Forum in

April 2022, building on the previously established Asia Pacific Economic Cooperation (APEC) CBPR system. The CBPR provides a data privacy certification backed by relevant authorities that facilitates data flows by promoting interoperable, enforceable data protection standards. Officials from the Departments of State and Commerce will continue efforts to bring new countries into the agreement, building on efforts such as workshops held in Kenya, Mexico, Chile, Brazil, UK, Israel, Jordan, Panama, Colombia, Fiji, and Barbados as well as ASEAN countries.

While the United States and its likeminded trade partners share many of the same values, we often have differing approaches to how to regulate the digital economy. The U.S. government advocates for multistakeholder, risk-based approaches that target the challenges we face while providing the flexibility to realize the benefits of new and emerging technologies. Unilateral approaches in digital taxation and the imposition of network usage fees often do not address the core issues of accessibility and fairness expressed by their proponents. Additionally, the rise of a growing digital sovereignty narrative that has been embraced by some of our close partners and allies has the potential to undermine key digital economy and cybersecurity objectives. The Department of State, working with other agencies, will continue to argue against data localization, network usage fees, digital services taxes as well as other market access barriers that contribute to the perception of increased control, but in reality often can undermine growth and security objectives.

Line of Effort 2: Promote Common Understandings of Trust, Interoperable Standards, and Shared Values and Governance Principles for Critical and Emerging Technologies

One of the most pressing challenges for digital solidarity is developing common approaches to governing critical and emerging technologies such as AI. The speed of innovation, the scale of the competition, and the stakes for our values, security, and prosperity demand concerted action. With AI technologies, we will not have the luxury of time or of pursuing narrow interests that have often slowed our ability to develop shared principles and interoperable regulatory approaches in other parts of the digital economy.

Shaping shared values and governance principles on the development, deployment, and use of AI is increasingly central to American digital diplomacy. The United States is engaging allies,

partners, the private sector, civil society, the technical community, and other stakeholders in discussions at the G7, Global Partnership on Artificial Intelligence, the Council of Europe, OECD, UN, UNESCO, and other fora to manage the risks of AI and ensure its benefits are widely distributed. In addition, we will need to work together to invest in the science research and infrastructure necessary to measure, evaluate, and verify advanced AI technology systems.

In July 2023, President Biden announced voluntary commitments from seven leading AI companies to advance the safe, secure, and transparent development of AI technology. Eight more companies (including one foreign-based company) signed on to the commitments in September. The United States internationalized and expanded on the voluntary commitments through the G7 Hiroshima AI process led by Japan to tackle generative AI, with leaders releasing an International Code of Conduct for Organizations Developing Advanced AI systems in October 2023. We continue to work on broadening acceptance of the Code of Conduct by more countries and companies beyond G7 member countries.

The United States joined twenty-seven other countries at the UK AI Safety Summit and signed the Bletchley Declaration, which encourages transparency and accountability from actors developing frontier AI technology. The United States and the United Kingdom have also signed a memorandum of understanding between their respective AI Safety Institutes advancing the science of measuring, evaluating, and addressing AI risks as a first step toward a global consensus on the scientific underpinnings of AI safety. These efforts outline a role for national governments, promote international cooperation, and encourage innovation by providing technically rigorous guidelines for introducing safe, secure, and trustworthy AI technology. At the same time, USAID and several other international development donors entered into a partnership to promote safe, secure, and trustworthy AI development in low- and middle-income countries in Africa and other parts of the world.

Hiroshima Principles for Generative AI

Take appropriate measures throughout the development of advanced AI systems, including prior to and throughout their deployment and placement on the market, to identify, evaluate, and

Develop and deploy reliable content authentication and provenance mechanisms, where technically feasible, such as watermarking or other

mitigate risks across the AI lifecycle.

Identify and mitigate vulnerabilities, and, where appropriate, incidents and patterns of misuse, after deployment including placement on the market.

Publicly report advanced AI systems' capabilities, limitations and domains of appropriate and inappropriate use, to support ensuring sufficient transparency, thereby contributing to increase accountability.

Work towards responsible information sharing and reporting of incidents among organizations developing advanced AI systems including with industry, governments, civil society, and academia.

Develop, implement, and disclose AI governance and risk management policies, grounded in a risk-based approach – including privacy policies, and mitigation measures, in particular for organizations developing advanced AI systems.

Invest in and implement robust security controls, including physical security, cybersecurity and insider threat safeguards across the AI lifecycle.

techniques to enable users to identify AI-generated content.

Prioritize research to mitigate societal, safety and security risks and prioritize investment in effective mitigation measures.

Prioritize the development of advanced AI systems to address the world's greatest challenges, notably but not limited to the climate crisis, global health and education.

Advance the development of and, where appropriate, adoption of international technical standards.

Implement appropriate data input measures and protections for personal data and intellectual property.

In October 2023, President Biden issued an Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. This Order establishes a process to

develop new standards for AI safety and security and seeks to protect citizens' privacy, promote innovation and competition, and advance equity and human rights. The Order tasked the Department of State with strengthening U.S. leadership abroad on AI issues. The Department of State and USAID, in collaboration with the Department of Commerce, are leading an effort to establish an AI in Global Development Playbook to harness AI's benefits and manage its risks. Relatedly, the Department of State plans to lead an interagency task force on detecting, authenticating, and labeling synthetic content, which aims to facilitate information sharing and mobilize global commitments to both label authentic government-produced content and detect synthetic content. In addition, working with the Department of Homeland Security (DHS), the Department of State is engaging international partners to help prevent, respond to, and recover from potential critical infrastructure disruptions resulting from the incorporation of AI into critical infrastructure systems or the malicious use of AI against those systems. The Department of State and USAID are also working with interagency partners, including the National Institute of Standards and Technology (NIST), National Science Foundation (NSF), and Department of Energy, to develop a human rights risk management framework for AI and a global AI research agenda.

The Department of State is also building broad-based support for the Political Declaration on Responsible Military Use of AI and Autonomy. While there are important discussions ongoing in Geneva under the framework of the Convention on Certain Conventional Weapons (CCW) – which the United States will continue to support – the scope of those discussions only covers one possible military use of AI, namely autonomous weapon systems. The Political Declaration is the first effort to articulate principles and best practices covering all military applications of AI technologies.

Line of Effort 3: Ensure International Standards Processes are Transparent, Open, Inclusive, and Impartial

International technology standards facilitate technology advancement, trade, global economic growth, and market access, particularly for startups and small- and medium-sized enterprises. They are also an area of strategic and economic competition, with the PRC in particular pushing top-down approaches to standards development process and using its economic influence to compel support for its standard proposals. In May 2023, the Biden-Harris White House published the first ever U.S. Government National Standards Strategy for Critical and Emerging

Technology (USG NSSCET). As outlined in the USG NSSCET, the United States will work with allies, partners, the private sector, and civil society to ensure that international standards development embraces transparency, openness, impartiality and consensus, effectiveness and relevance, coherence, and broad multistakeholder participation. The Department of State, in cooperation with the Department of Commerce and other agencies, is building enhanced capacity to engage directly in international standards development organizations and to coordinate with industry and civil society to ensure robust participation by U.S. stakeholders in standards making processes.

Working with the FCC, NIST, National Telecommunications and Information Administration (NTIA), and other federal agencies, the Department of State supports standards development processes for a wide range of critical and emerging technologies and platforms, including IoT, energy grids, smart cities, and connected vehicles. The United States will continue to promote and leverage cybersecurity and privacy standards and guidelines developed by NIST through open processes with a strong connection to international standards.

This approach reinforces the U.S. policy for standards: a private-sector led, industry-driven approach with government participation that emphasizes the use of international standards developed in open, transparent, and consensus-based processes. This alignment helps stakeholders reduce the burden of international regulatory and legal regimes, leading to a reduced cost of operation and a greater understanding of international policies. It also highlights the value of a bottom-up approach for other governments as they develop their cybersecurity priorities.

The U.S. government has developed formal and informal methods of information sharing and standards development monitoring through regular engagement with partners and allies. Quad partners and members of the TTC, for example, have signed memoranda of cooperation to enable increased information sharing, coordination, and influence in international standards development. The Department of State has also supported increasing participation in standards development organizations from historically underrepresented nations.

Line of Effort 4: Expand and Diversify Civil Society Participation in Multistakeholder Processes

The United States and its partners remain committed to the multistakeholder model of Internet and digital governance. Active and meaningful participation of all stakeholders, including governments, civil society, the private sector, academia, and the technical community, is essential to informing our discussions and policymaking, promoting transparency and accountability, and strengthening implementation and sustainable development. Through foreign assistance programs, the Department of State is advancing policy and advocacy initiatives through which civil society stakeholders engage with national governments, regional governance bodies, and international standard-setting entities to encourage Internet and digital governance policies consistent with democratic values and international human rights. The Department of State will continue its efforts to expand and diversify the groups who are working to promote interoperable, rights-respecting, and secure digital technologies. It will also continue to prevent and defend against efforts by repressive governments to exclude civil society and other stakeholders from participation in relevant fora.

The United States strongly supports the Internet Governance Forum (IGF) as the preeminent global body bringing together all stakeholders through a bottom-up process to discuss rights-respecting solutions to Internet public policy issues. It will continue to work with allies and partners to sustain and bolster the IGF's relevance.

Line of Effort 5: Advance a Common, Rights-Respecting Vision for the Digital Future

Digital solidarity is built on a shared commitment to human-rights based technology governance. The Advancing Digital Democracy (ADD) initiative, launched by USAID at the Summit for Democracy in 2021, fosters an open, secure, and inclusive digital ecosystem through programs such as partnerships with governments, private sector and civil society to strengthen legal and regulatory frameworks for data and digital technologies, and increased support for software engineers, tech companies, and researchers working to embed respect for human rights and democratic values across the tech lifecycle. In April 2022, the United States and 60 countries launched the Declaration for the Future of the Internet (DFI), bringing together a broad, diverse coalition of partners around a common, rights-respecting vision for an open, interoperable, reliable, and secure digital future. As chair of the Freedom Online Coalition in 2023, the United States prioritized protecting fundamental freedoms online; countering and

building resilience to the misuse of digital technologies; advancing norms, principles, and safeguards regarding the development and use of artificial intelligence; and strengthening digital inclusion. Similarly, the United States, working with 13 other countries, launched the Global Partnership for Action on Gender-Based Online Harassment and Abuse. This partnership, which emerged from the first Summit for Democracy, is a response to the need to address technology-facilitated gender-based violence as part of a shared global agenda to promote peace, security, and stability.

The United States will continue working with allies and partners to ensure digital technologies are used in a responsible and rights-respecting manner. Along with 45 partners, the United States endorsed in March 2023 Guiding Principles on Government Use of Surveillance Technologies, which are intended to prevent the misuse of surveillance technologies by governments. In addition, the Department of State will continue to advance programs that enable at-risk, vulnerable, and marginalized populations, or those who protect them, to prepare for, prevent, identify, investigate, and obtain remedy for digital abuses or other types of digital repression.

The United States supports several multistakeholder efforts working to address a range of online challenges while respecting freedoms of opinion and expression, including the Christchurch Call to Action in 2019, the French-led Child Online Protection Laboratory, Freedom Online Coalition, and the Global Partnership for Action on Gender-Based Online Harassment and Abuse. The United States will continue to advocate for a rights-respecting approach consistent with protecting freedoms of opinion and expression and promoting gender equity and equality as governments around the world propose increased regulation of online platforms.

Further strengthening domestic policy will enable deeper coordination with international partners on a range of digital issues. The Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, for example, has reinforced the position of the United States in international discussions on the governance of AI. The National Cybersecurity Strategy supports legislative efforts to impose robust, clear limits on the ability to collect, use, transfer, and maintain personal data and provide strong protections for sensitive data like geolocation and health information. The NCS specifically calls for this legislation to mitigate privacy risks arising from data processing and set national requirements to secure personal data.

Line of Effort 6: Negotiate a Rights-Respecting Cybercrime Treaty

The United States, its allies, and partners as well as civil society groups have long supported the Council of Europe Convention on Cybercrime (commonly known as the Budapest Convention) as the most effective tool for providing global standards for criminalizing malicious cyber activities, obtaining electronic evidence, and fostering international cooperation on computer-related crimes. The Convention was drafted to be global and open to all regions. Seventy-two countries, including the United States, are currently parties to the Convention, and 21 additional countries have been invited to accede.

While supporting accession to the Budapest Convention, the United States and its partners are also actively working to ensure that negotiations in the UN Ad Hoc Committee to elaborate a convention against cybercrime reach a positive outcome: a rights-respecting cybercrime treaty that would enable all UN member states to cooperate better in the fight against cybercrime. The United States and its partners will continue to oppose overly broad definitions of cybercrime that could be used to stifle freedom of expression, infringe on privacy, and or endanger individuals and communities. The United States will also continue to advocate for necessary and sufficient safeguards commensurate to the scope of the domestic powers and international cooperation provided for in the convention. Maintaining an open, inclusive, and transparent process will best allow states to negotiate a binding agreement with the participation of interested stakeholders.

Line of Effort 7: Defend Information Integrity

Information integrity challenges are not new, but determined foreign state adversaries and rapid technological advances, especially AI-enabled human-machine interactions, create complex dynamics that compound information risks by enabling rapid, large-scale, and targeted dissemination of AI-enabled synthetic content. Building a resilient information environment—one in which there is open, free public debate and consistent access to diverse sources of fact-based information—is an ongoing priority for the United States and its allies and partners. These features are essential for citizens to inform their opinions and exercise their human rights,

including freedom of expression, freedom of peaceful assembly and association, and the right to vote. Information manipulation is destabilizing and can harm national security, democratic processes, economic welfare, the environment, crisis response, human rights, and public health. While foreign actors seeking to interfere with or manipulate the information environment pose significant risks, there are additional challenges open societies face around the quality of information online and deteriorating trust.

With allies and partners, the Department of State will continue to work to build civic information resilience, counter foreign state and non-state extremist propaganda online, and mitigate risks of AI to information integrity while protecting freedom of expression. The U.S. Government will work to protect the integrity of elections and other democratic processes across the globe. At the TTC, OECD, and G7, the United States develops shared approaches to building healthy and resilient information ecosystems. The United States and France are co-chairing the DIS/MIS Information Resource Hub, the OECD's leading information integrity initiative. At the Hub, the Department of State is focused on increasing cooperation around sharing of best practices and strengthening information resilience, both among OECD and non-OECD countries, and developing a framework to guide whole-of-society efforts in this area. Through the Promoting Information Integrity and Resilience Initiative (Pro-Info), USAID aims to bolster healthy information ecosystems and help address information manipulation through multi-stakeholder engagement, donor coordination, and capacity building efforts.

At the third Summit for Democracy in 2024, the United States launched a democratic roadmap for building civic resilience to global digital manipulation that highlights the importance of the digital information manipulation challenge as a threat to the functionality and vitality of society; recognizes that building information integrity can be consistent with freedom of opinion and expression; reinforces private sector digital platforms' ability to strengthen civic resilience; and prioritizes efforts to address generative AI (GAI)—particularly in the context of global 2024 elections. The United States has also endorsed the Global Declaration on Information Integrity Online, launched by Canada and the Netherlands. The Declaration, grounded in international human rights law, establishes high-level international commitments by participating states to protect and promote information integrity online.

In addition, the Department of State has announced a Framework to Counter Foreign State Information Manipulation. This Framework seeks to develop a common understanding of the threat and establish a common set of action areas from which the United States, with its allies

and partners, can develop coordinated responses to foreign information manipulation and protect free and open societies.

ACTION AREA 3: Advance Responsible State Behavior in Cyberspace and Counter Threats to Cyberspace and Critical Infrastructure by Building Coalitions and Engaging Partners

At the UN and regional security bodies, the United States, along with its allies and partners, is working to advance responsible state behavior in cyberspace based on a UN General Assembly-endorsed framework, underpinned by the applicability of existing international law, adherence to globally accepted and voluntary norms of state behavior in peacetime, development and implementation of confidence-building measures to reduce the risk of conflict in cyberspace, and a commitment to building states' capacities to implement the elements of the framework.

Despite a global consensus on the framework for responsible behavior in cyberspace, the norms are not self-enforcing. Some states act in ways contrary to it. When a state engages in significant destructive, disruptive, or otherwise destabilizing malicious cyber activity contrary to the framework, responsible states must cooperate to hold that irresponsible state accountable.

Digital solidarity in this context is demonstrated by sustained mutual support and coordinated campaigns. The United States and its partners share cyber threat information to help build resilience to and disrupt malicious activities; show solidarity to victims by helping respond to significant incidents, thereby signaling to adversaries they cannot isolate a target country through malicious operations; and ensure accountability for destructive, disruptive, and otherwise destabilizing cyber activities in concert with likeminded countries. The United States and some allies also have affirmed the application to cyberspace of their respective mutual defense treaty obligations. In addition, the Department of State and other federal agencies are working with allies and partners to disrupt ransomware and other criminal networks and safeguard democratic processes and institutions. Looking forward, the United States will continue efforts like these to advance responsible behavior in cyberspace, and counter threats to cyberspace and our critical infrastructure by building coalitions and engaging partners.

Line of Effort 1: Pursue Action-Oriented Discussions Focused on Norm Implementation at the UN

Sustained engagement over almost two and a half decades and across four previous administrations has yielded a framework of responsible state behavior in cyberspace repeatedly supported by all members of the UN General Assembly, which affirms the applicability of international law to states' use of information and communication technologies, endorses adherence to voluntary norms of responsible state behavior in peacetime, and proposes practical confidence-building measures to help reduce the risk of conflict stemming from cyber incidents. The framework is the core of our vision for a cyberspace in which states behave appropriately, manage the risk of unwanted escalation, hold bad actors accountable for irresponsible activities, and work together to respond to and recover from significant cyber incidents. Implementation of these norms, however, is critical to their effectiveness.

We will pursue more action-oriented discussions at the UN focused on how member states and institutions can work together to implement the framework's essential elements and build all states' capacity to manage cyber-related threats. To accommodate this evolving conversation, the United States and its partners have proposed a more action-oriented forum, a Program of Action (POA), as a future permanent mechanism for dialogue on cyber issues related to international security at the UN. Designed to be flexible enough to address future threats, with member states setting its direction over time, the POA will also incorporate the views of civil society, the private sector, and other non-state stakeholders.

As part of advancing responsible state behavior in cyberspace, the United States and our partners will also continue to work together in regional security and other fora, such as the Organization for Security and Cooperation, Organization of American States, and the ASEAN Regional Forum, to develop and implement cyber confidence building measures.

UN Framework of Responsible State Behavior

Figure 4. Four components that make up the UN framework of responsible state behavior in cyberspace. (Australian Strategic Policy Institute/United Nations General Assembly illustration.)

Line of Effort 2: Disrupt and Build Resilience to Malicious State Activity

Given the interconnected nature of cyberspace, international cooperation is crucial to deny, disrupt, and counter adversary activities in and through cyberspace.

The Department of State leads efforts, including facilitating international outreach, to address the rising threat of disruptive or destructive cyberattacks on the critical infrastructure of the United States and its allies and partners. This includes sharing through diplomatic channels joint cybersecurity advisories with the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and National Security Agency (NSA), and allies and partners on threats; capacity building and information sharing with new and existing partners to mitigate cyber threats and ensure the resilience of their critical infrastructure; and using bilateral, multilateral, and other fora to clarify and communicate expectations about adherence to international law and the framework for responsible behavior in cyberspace. In addition, members of the Quad have developed joint principles for the cybersecurity of critical infrastructure and NATO members have committed to ensuring the resilience of critical infrastructure, enhanced protection of critical infrastructure through training and exercises, and shared intelligence on threats.

As part of its counter adversary cyber activity, the Department of State provides foreign policy guidance and uses diplomatic engagements to support the Department of Defense (DoD)'s efforts to campaign in and through cyberspace below the level of armed conflict to reinforce deterrence and frustrate adversaries. As laid out in the 2023 DoD Cyber Strategy, U.S. Cyber Command continues to defend forward to discover, expose, and protect against the sources of malicious cyber activities and to reinforce responsible state behavior by encouraging adherence to international law and internationally recognized cyberspace norms. The DoD Cyber Strategy also notes that cyber operations are most effective when used in concert with other instruments of national power, including diplomatic engagement and cyber capacity building.

The Department of State, in close coordination with interagency and international partners, will continue to organize and execute sustained diplomatic pressure campaigns to raise international and public awareness of significant cyber threats and to increase the costs and risks to malicious cyber actors. For example, the United States has worked with allies, partners, and the private sector to disrupt DPRK revenue-generation efforts through cybercrime, crypto theft, and IT workers. U.S. Cyber Command, NSA, DHS, DOJ, and the FBI have exposed North Korean malware, seized malicious cyber infrastructure, seized cryptocurrency and fiat currency, and shared actionable threat intelligence with the private sector. The Department of State coordinates action with the Republic of Korea through a bilateral DPRK Cyber Working Group, including information sharing and policy coordination. Also, the United States, Japan, and the Republic of Korea coordinate efforts to counter DPRK cyber threats through a trilateral working

group announced during the Camp David Summit in August 2023. The Department of State has also briefed officials around the world on threats posed by DPRK IT workers and cyber actors and deployed foreign assistance funds to build capacity to detect and defend against DPRK cyber and crypto threats.

Line of Effort 3: Support Allies and Partners Amid Malicious Activity

A core element of digital solidarity is standing with partners when they are impacted by significant disruptive or destabilizing cyber incidents. The Department of State will continue to work with allies and partners – through our embassies on the ground and our cyber experts in Washington – to coordinate appropriate support during the investigation, mitigation, and recovery from such cyber incidents. This support can include, as appropriate, the provision of advice by embassy cyber experts; facilitation of remote or on-the-ground investigative, hunt, and malware analysis activities; foreign assistance projects; or coordination of cyber assistance efforts with partner countries. The Department of State views such activities as critical to strengthen collective cyber defense and resilience and to help countries resist cyberattacks aimed at coercing them or otherwise interfering with their sovereignty.

Line of Effort 4: Hold Irresponsible States Accountable

To constrain our adversaries effectively and counter malicious activities below the threshold of armed conflict, we will continue to work with our allies and partners to condemn this activity and impose meaningful consequences. These efforts use all the tools of statecraft, including diplomatic isolation, law enforcement, counter-cyber operations, and economic sanctions. In September 2019, 27 countries publicly pledged in a U.S.-led Joint Statement on Advancing Responsible State Behavior in Cyberspace to collaborate voluntarily to hold states accountable when they act contrary to the framework. The number of states willing to publicly hold states accountable reached 39 in July 2021 when NATO, the EU, Australia, Canada, New Zealand, the United Kingdom, and Japan all publicly condemned the PRC's involvement in the Microsoft Exchange server data breach incident and other malicious cyber activities. More recently, likeminded coalitions attributed Russia's cyberattack on Viasat's KA-SAT satellite communications network on the eve of its invasion of Ukraine and stood in solidarity with Albania in the wake of

Iran's disruptive cyber operations. The United States will continue to work to expand the coalition of those willing to hold states accountable for disruptive and destabilizing cyber activity and to utilize appropriate multilateral groupings to support each other and to assist the victims of such behavior.

Line of Effort 5: Affirm Application of Mutual Defense Treaties with Certain Allies to the Cyber Domain

In line with the long-standing U.S. recognition that existing international law applies in cyberspace, obligations under treaties and other international agreements may apply in cyberspace. Over the past several years, the United States and certain allies have made public statements affirming the application in cyberspace of obligations in their respective mutual defense treaties, including the 1951 Security Treaty between Australia, New Zealand and the United States (ANZUS) (2011); the North Atlantic Treaty (2014); the Treaty of Mutual Cooperation and Security between the United States and Japan (2019); and the Mutual Defense Treaty between the United States and the Republic of Korea (2023). The Departments of State and Defense will continue to work together with allies to engage in pre-contingency planning and to raise awareness further with alliance partners that existing mutual defense treaties may apply in cyberspace and that cyberattacks rising to the level of an armed attack may trigger mutual defense obligations under such treaties.

Figure 5. The Second International Counter Ransomware Initiative Summit November 2022; Vice President Kamala Harris center left and Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger center right with leaders from Australia, Austria, Belgium, Brazil, Bulgaria, Canada, Croatia, Czech Republic, Dominican Republic, Estonia, France, Germany, India, Ireland, Israel, Italy, Japan, Kenya, Lithuania, Mexico, the Netherlands, New Zealand, Nigeria, Norway, Poland, Republic of Korea, Romania, Singapore, South Africa, Spain, Sweden, Switzerland, United Arab Emirates, United Kingdom, United States, and Ukraine, and the European Union. (U.S. Department of State photo.)

Line of Effort 6: Counter Criminal and Ransomware Actors

For many countries, the greatest risk to their digital security and economies is online scams, criminal hacking, and other financial crimes. Ransomware in particular has emerged in recent years as a clear threat to national security, public safety, and economic prosperity. Operating from safe havens like the PRC, DPRK, Iran, Russia, and certain other countries, ransomware operators have disrupted government services, hospitals, schools, pipeline operations, and civil society entities. With some states using ransomware actors as proxies or turning a blind eye to their activities and the significant impact of their cyberattacks on critical infrastructure, it is increasingly clear that ransomware activity can threaten international peace and security. Digital

solidarity is clearly expressed through the Department of State's efforts to leverage its diplomatic capabilities to support the whole-of-government fight against ransomware and other forms of cybercrime, including by building partner capacity; developing coalitions to prevent, disrupt, and punish criminal behavior; and fostering cooperation with the private sector.

The Departments of State, Homeland Security, and Justice will continue to participate in the U.S. Joint Ransomware Task Force and to partner with private industry and international allies to disrupt online criminal infrastructure and resources, take down botnets, and seize cryptocurrency garnered from ransomware campaigns. For example, the U.S. Transnational and High-Tech Crime Global Law Enforcement Network (GLEN) program—a long-standing partnership between the Departments of State and Justice—is a global law enforcement capacity-building network of DOJ International Computer Hacking and Intellectual Property (ICHIP) regional advisors, computer forensic analysts, and federal law enforcement agents. Twelve ICHIP attorney advisors are located around the world. The ICHIP advisor based in The Hague facilitated cooperation among the United States, France, Germany, the Netherlands, the United Kingdom, Romania, and Latvia in the largest ever takedown of the botnet and malware known as Qakbot in August 2023. The network also delivers training and technical assistance to foreign law enforcement partners, prosecutors, and judicial authorities to combat intellectual property theft and cybercrime activity, as well as to assist in the collection and use of electronic evidence to combat all types of crime. The program improves U.S. security by reducing the use of foreign computing infrastructure for malicious activities targeting U.S. networks and by showing that no malicious actor can evade the rule of law.

The GLEN has stood up five regional cryptocurrency working groups around the globe, which are dedicated to information sharing and capacity building to address criminal misuse of cryptocurrency, including in ransomware. Additional priorities for capacity building include Internet fraud and combating the growing scourge of online child sexual exploitation and abuse.

The Department of State will continue to use its diplomatic engagements and capacity building to broaden and strengthen participation in the International Counter Ransomware Initiative (CRI). The CRI is a unique and geographically diverse coalition of nearly 60 countries, plus multilateral institutions such as the European Union, Interpol, and Organization of American States, committed to building collective resilience to ransomware, cooperating to disrupt ransomware and pursue the actors responsible, countering the illicit finance that underpins the ransomware ecosystem, and working with the private sector to defend against ransomware

attacks. As a complement to the CRI, the Department of State, in coordination with the U.S. Joint Ransomware Task Force, will continue to develop bilateral and multilateral efforts designed to discourage states from sponsoring ransomware or permitting their territories to be used as safe havens by cyber criminals.

The work of the CRI supports the implementation of the framework for responsible state behavior in cyberspace, including the voluntary norm that “states should respond to appropriate requests for assistance by another state whose critical infrastructures are subject to malicious ICT acts,” in addition to “appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty.” [5]

Line of Effort 7: Safeguard Democratic Processes and Institutions

With more than 70 countries and nearly half the world’s population experiencing elections in 2024, their vulnerability to cyber-enabled interference—including potential cyberattacks that disrupt electoral processes; espionage, surveillance, and intimidation of politicians, activists, and journalists; and cyber-enabled malign influence activities that seek to impact election outcomes and undermine public confidence in elections—is particularly acute. The United States has highlighted publicly and in international engagements that it considers election infrastructure to be part of critical infrastructure. It has also noted some states’ efforts to use cyber means to destabilize democratic processes. The United States, allies, and partners will continue to expose and defend against malicious operations designed to destabilize democratic processes and societies, including by sharing threat information and strengthening the resilience of election commissions and other key institutions. The United States, for example, joined a United Kingdom-led effort in 2023 to call out Russia-backed online influence actors and hackers for operations targeting UK politicians and democratic processes. This diplomatic effort was accompanied by the Department of Justice concurrently announcing criminal charges against two of the responsible actors.

Line of Effort 8: Combat the Proliferation and Misuse of Commercial Spyware

The proliferation and misuse of commercial spyware poses a significant threat to both U.S. national security—including counterintelligence interests—and to democratic values and human rights around the globe by enabling the surveillance, repression, and targeting of journalists, human rights defenders, anti-corruption activists, and other civil society members. In March 2023, President Biden signed an executive order limiting U.S. government operational use of commercial spyware that poses significant counterintelligence or security risks to the United States, or significant risks of improper use, including committing human rights abuses, by a foreign government or foreign person. At the same time, the Department of State launched a Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware with 10 other countries committed to undertaking concrete efforts to counter the misuse and proliferation of commercial spyware, which an additional 6 countries joined in March 2024.

Moving forward, the U.S. government will continue to work to disincentivize misuse and positively reshape the commercial spyware market by driving out or encouraging reform by businesses associated with the misuse of these tools. The Department of State will continue to engage diplomatically to urge the countries that have already joined the Joint Statement to take concrete steps to counter the misuse and proliferation of commercial spyware, induce additional countries to join, and persuade countries that misuse or enable the misuse of spyware to implement safeguards to deviate less from U.S. policy. The Department of State will continue to partner with the Departments of Commerce and Treasury to promote accountability for those who misuse—or enable or benefit from the misuse—of commercial spyware through tools like sanctions, visa restrictions, and export controls. In addition, the Department of State will continue to elevate this issue in multilateral and public forums as well as engage closely with civil society, journalists, tech platforms, and the investment community.

ACTION AREA 4: Strengthen and Build International Partner Digital Policy and Cyber Capacity

Digital and cyber capacity building activities are powerful signs of digital solidarity in action. They assist partners build secure, diverse, and resilient ICT infrastructure and grow global markets for interoperable, secure ICT goods and services. They are also critical for emerging economies to achieve the SDGs.

Adversaries, and the PRC in particular, understand this and look to out-match the United States and like-minded partners by offering holistic support for ICT development from full package training programs to higher-level education and scholarships. The Department of State, working with other federal agencies, international allies and partners, and the private sector, seeks to mobilize technology as well as processes and people in support of our partners' economic and development goals. This assistance often has a catalytic effect, encouraging partner countries to prioritize and invest further in cybersecurity and resilience. It also increases understanding of the benefits of the cybersecurity and digital policy approaches advocated by the United States.

In an effort to increase digital solidarity in the realm of foreign assistance, USAID launched the Donor Principles for Human Rights in the Digital Age in partnership with Canada's International Development Research Centre (IDRC), and in collaboration with the Department of State. These principles – endorsed by 38 partner governments – offer a unified framework and set of benchmarks to promote an inclusive, rights-respecting approach to foreign assistance on digital issues.

To achieve our goals, we must work to ensure we can act quickly and effectively in supporting foreign partners' needs for incident response, trusted infrastructure development, and capacity building.

Line of Effort 1: Support and Expand Digital Policy, Legal, and Regulatory Capacity Building Efforts

For digital infrastructure to reach and effectively serve the public, countries need to have the appropriate legal and regulatory frameworks. It is not enough to promote secure, resilient technology infrastructure; an effective regulatory framework that is transparent, flexible, and technology neutral must be in place to ensure meaningful connectivity. Thus, U.S. foreign assistance focuses on developing and strengthening relevant legislative and regulatory frameworks as well as building local technical capacity and addressing workforce issues.

The Department of State will continue to provide partners the expertise and training they need to develop and govern secure, rights-respecting digital ecosystems. Through technical assistance, ICT and telecom policy capacity building, and training grants, DCCP has facilitated pro-competitive legal and regulatory reforms. For example, Promoting American Approaches to ICT Policy and Regulation (ProICT), another DCCP activity led by the Department of State and USAID, has helped clear the way for new entrants into 5G markets and provided technical advisory support for a 5G spectrum auction.

The Department of State, USAID, NTIA, and FCC, working with industry and the private sector, will continue to provide training programs and technical assistance to developing country officials involved in managing spectrum, deploying wireless and satellite technologies, and acquiring cloud services.

Line of Effort 2: Augment Partner Cyber Capacity Building Efforts



Figure 6. A global map of the Digital Connectivity & Cybersecurity Partnership activities (2018-2024). (U.S. Department of State, CDP)

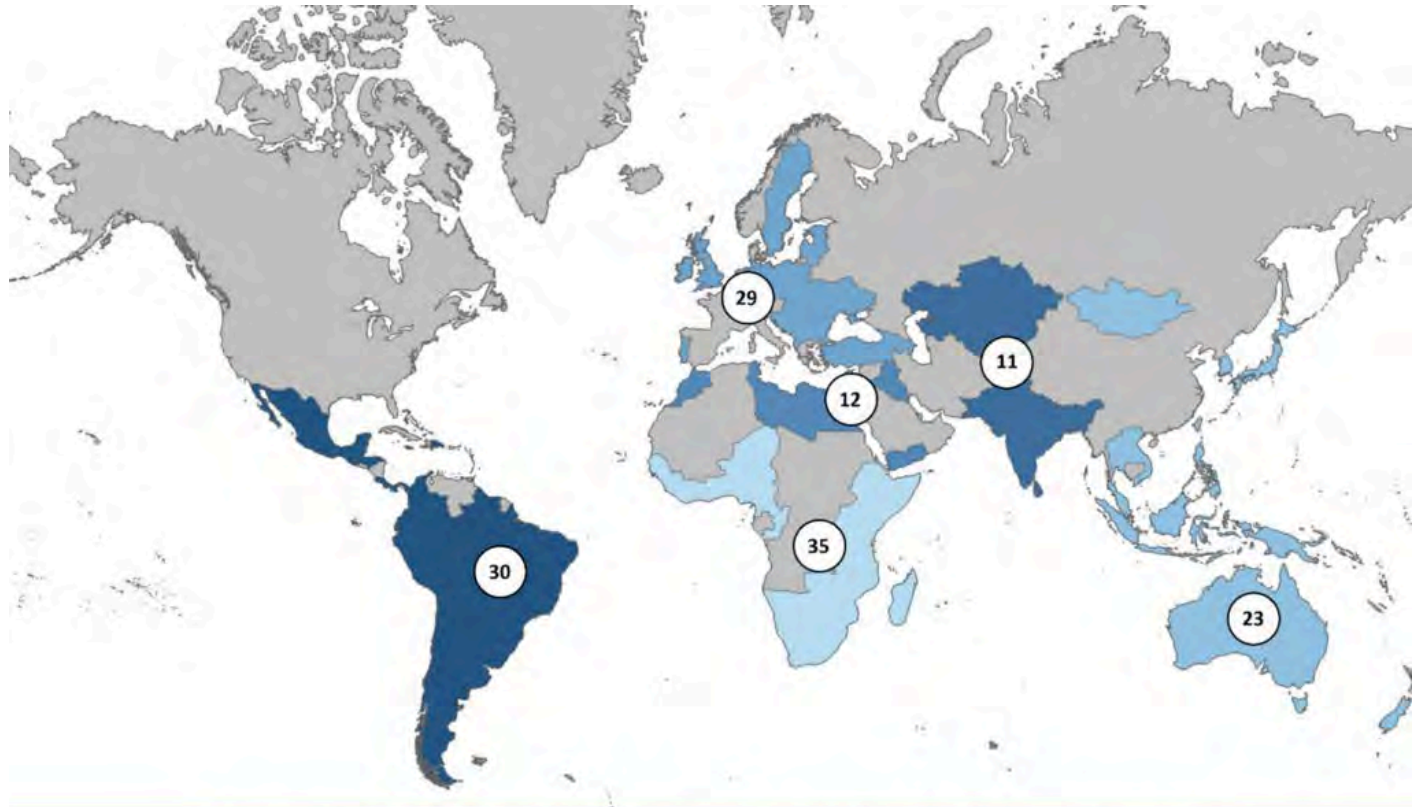
Cyber capacity building efforts—which usually focus on strengthening a nation’s ability to adopt and develop cyber policies and strategies or improving their technical ability to detect, respond to, and recover from cyber incidents—have a direct and positive impact on international cyber stability and the security of U.S. citizens. Assistance directed at policy- and strategy-making increases states’ credibility and engagement in international discussions. It provides them with the national-level capabilities needed to implement the norms developed under the framework

for responsible state behavior in cyberspace, to conform with the standards of the Budapest Cybercrime Convention, to hold irresponsible actors accountable in cyberspace, and to develop a national-level approach to counter persistent cyber threats and build long-term resilience. Improving partner operational capabilities makes it more likely they will be able to combat transnational cybercrime threats, share useful cyber threat and incident information with the United States, and successfully partner with the United States in operations to disrupt malicious cyber activity.

Over the last two decades, the Department of State has collaborated with other agencies, international partners, regional organizations, and the private sector to build cyber capacity abroad. Officials and private sector professionals from around the world participate in workshops on industrial control systems held with CISA. The United States assists efforts by the Organization of American States in areas such as cyber incident response, national cybersecurity strategy development and implementation, cybersecurity awareness, and cyber workforce development. The United States is a leading donor to Council of Europe programs designed to expand adoption of the Budapest Cybercrime Convention. The Global Forum on Cyber Expertise (GFCE), of which the United States is a founding and active member, provides a global platform to connect cyber policymakers, practitioners, and experts and to match assistance programs with recipients.

Multiple agencies have supported international partners in using and adapting the NIST Cybersecurity Framework, and the Department of State has supported international participation in the development of version 2.0 of the framework. The NICE Workforce Framework for Cybersecurity (NICE Framework) has been leveraged to support talent development and management. The Department of Commerce, NIST, USAID, and the Department of State will engage international partners to promote the development of critical and emerging technology standards in areas such as best practices regarding data capture, processing, privacy, handling, and analysis; trustworthiness, verification, and assurance of AI systems and AI risk management; and content authentication and provenance, synthetic content detection, and content labeling. In addition, NIST has selected four algorithms designed to withstand cyberattacks by quantum computers and is developing standards for U.S. Government use. The Department of State will work with NIST to internationalize – including through ongoing engagements in international standards bodies – these post quantum cryptography standards so that organizations around the world can integrate them into their encryption infrastructure. They will also continue engaging international partners in developing

and implementing cybersecurity best practices in areas such as Zero Trust, IoT cybersecurity, digital identity, operational technology, software security, and supply chain risk management.



140 countries benefitting from Cyber and Digital Training Programs Since 2018

Figure 7. A global map of the Digital Connectivity & Cybersecurity Partnership countries benefitting from Cyber & Digital Training (2018-2024). (U.S. Department of State, CDP)

The Department of State will continue coordinating closely with DoD, DOJ, DHS, CISA, NIST, NTIA, USAID, Department of Treasury, Department of Energy, Department of Commerce, and other federal agencies to help ensure that multiple streams of capacity building feed into and support strategic interests.

Figure 8. (Left) Nathaniel C. Fick U.S. Ambassador at Large for Cyberspace and Digital Policy, (center) Rodrigo Chaves Robles President of Costa Rica, (right) Anne Neuberger Deputy National Security Advisor for Cyber and Emerging Technology at a Center for Strategic and International Studies (CSIS) event on August 30, 2023. (CSIS photo.)

Line of Effort 3: Develop New Tools to Deliver Digital and Cyber Assistance Quickly and Efficiently

The demand for cybersecurity and cybercrime assistance, in particular cyber defense, incident response, and skills to combat criminal misuse of cryptocurrency, is growing in scale. After cyberattacks against Ukraine, Costa Rica, and Albania, the United States and its allies shared threat intelligence; facilitated operational collaboration; enabled access to commercial cybersecurity companies' services, including hardware, software, and embedded technical support; and funded longer term capacity building.

From these and other cases, the State Department has learned the importance of regular and close coordination across the U.S. government and with international partners, as well as the importance of mobilizing private-sector technology and expertise. Modernizing authorities and

mechanisms to provide technology-related foreign assistance at the speed and scale necessary is crucial. We must adapt our foreign assistance resources and authorities to support long-term U.S. leadership and foster digital solidarity.

Recognizing the urgent and growing need for additional tools to advance U.S. cyber and digital foreign policy, Congress created, through the Department of State Authorization Act of 2023 and funded, through the Department of State, Foreign Operations, and Related Program Appropriations Act, 2024, the Cyberspace, Digital Connectivity, and Related Technologies Fund. This fund will provide the Department of State with authorities and dedicated funding to support strategically important cyber, digital, and technology-related foreign assistance programs. This is a significant step in advancing U.S. foreign policy. The Department will work to operationalize and implement these new authorities.

Ukraine

The United States, allies, and partners have invested in Ukrainian cyber capacity building for years, providing a foundation for more immediate assistance in mitigating and recovering from attacks. Before Russia's full-scale invasion of Ukraine, U.S. agencies, including the Federal Bureau of Investigation, U.S. Cyber Command, and the Cybersecurity and Infrastructure Security Agency, shared cyber intelligence with Ukrainian partners. Since the invasion, the United States, United Kingdom, and EU Governments have delivered more than \$100 million in cyber foreign assistance and enabled Ukrainian agencies to access the services of commercial cybersecurity companies. In 2023, the U.S. and nine close partners established the Tallinn Mechanism, a donor coordination group that aims to deliver assistance quickly and efficiently in support of Ukraine's most urgent cybersecurity needs.

Costa Rica

Following a year of repeated ransomware attacks on Costa Rica's government networks that impacted critical services such as health care, tax collection, and customs, and resulted in a national emergency, the United States announced an \$25 million assistance package to address immediate critical cyber vulnerabilities, including hardware, software, licenses, and embedded technical support. Working with the Costa Rican Ministry of Science, Innovation, Technology, and Telecommunications, the United States helped establish and equip a centralized security operations center to monitor, prevent, detect, investigate, and respond to cyber threats. The United States is also supporting medium- and longer-term technical projects and workforce development to help Costa Rica develop a secure, resilient, and locally sustainable cyber ecosystem.

Albania

In the case of Albania, after a request from the prime minister in July 2022, the U.S. rapidly deployed technical teams in response to a destructive cyberattack, which featured ransomware and wiper malware against public sector networks, including some Albania had designated as critical infrastructure. The U.S. government and the private sector attributed the attack to Iran, and the State Department coordinated a diplomatic campaign that included U.S. sanctions and NATO and EU statements of condemnation. After these more immediate responses, the State Department turned to longer-term capacity building, including implementing over \$50 million in U.S. assistance to civilian and military agencies to harden their networks. International partners such as the UK and EU have

also provided cybersecurity assistance. U.S. agencies, including the Department of State, Federal Bureau of Investigation, U.S. Cyber Command, and the Cybersecurity and Infrastructure Security Agency continue to collaborate with Albanian cyber authorities following subsequent smaller scale cyberattacks in 2023 and 2024.

Conclusion

As the NSS and NCS note, the 2020s are a decisive decade, and actions taken now will shape the contours of cyberspace, digital technologies, and the digital economy for the future. As it implements this strategy, the Department of State will work with Congress and interagency partners to evaluate current cyber authorities and to amend or create authorities as needed for the Department to keep pace with evolving cyber and digital technologies.

Building innovative, secure, and rights-respecting digital ecosystems is a process that will extend beyond the timespan of this strategy, and likely to be characterized by progress, pauses, and reversals. There will be, however, some early signposts that will indicate the United States, allies, and partners are moving forward.

First, the United States, allies, and partners, along with the private sector and civil society, will build on the early successes of the G7-Hiroshima Code of Conduct, the Biden-Harris Executive Order on AI, and the UK AI Safety Summit. We will reach consensus on guiding principles that foster innovation and the development of responsible AI as well as make significant investments to build the knowledge and infrastructure necessary to measure, evaluate, and verify advanced AI systems, including through the launch of the U.S. AI Safety Institute. We will advance global norms on the responsible and rights-respecting use of AI-enabled technologies.

Second, the United States allies, and partners, along with the private sector, will develop common understandings and shared principles for security and trustworthiness in subsea cable, cloud services, and data centers and will increase support for extending access to cloud services to emerging economies.

Third, the United States, allies, and partners will succeed in pushing forward more action-oriented discussions at the UN on international security issues in cyberspace. These discussions

will focus on how member states can work together to implement critical elements of the framework for responsible state behavior and on building all states' capacity to manage cyber-related threats.

Fourth, the Department of State will draw on the Cyberspace, Digital Connectivity, and Related Technologies Fund to provide rapid incident response and cyber aid quickly and effectively, as well as longer-term capacity and resilience building. These strategic investments will not only strengthen the role of the United States as a digital partner, but also generate larger, self-sustaining investments by host countries in their own cybersecurity and digital transformation.

Moving forward, the United States will strive for a future in which cyberspace and digital technologies are used to advance economic prosperity and inclusion, enhance security, promote and protect human rights and democracy, and address transnational challenges. The Department of State will build and extend digital solidarity to partners across the globe. The United States recognizes the need to work together to align approaches to data and digital governance and to promote the research, development, and deployment of critical and emerging technologies. The United States seeks to be the partner of choice in improving cybersecurity, building resilience, responding to, and recovering from malicious cyber activity. Digital solidarity aims to connect people and information like never before, fostering a more inclusive, secure, prosperous, rights-respecting, safe, and equitable world.

. . .

Notes

[1] The idea of digital solidarity was first promoted by Pablo Chavez, "Toward Digital Solidarity," Lawfare, June 28, 2022, <https://www.lawfaremedia.org/article/toward-digital-solidarity>

[back to 1]

[2] Fast Track Action Subcommittee on Critical and Emerging Technologies, Critical and Emerging Technologies Update, National Science and Technology Council, February 2024,

<https://www.whitehouse.gov/wp-content/uploads/2024/02/Critical-and-Emerging-Technologies-List-2024-Update.pdf>

[back to 2]

[3] Anna Fleck, "Cybercrime Expected To Skyrocket in Coming Years," Statista, February 22, 2024, <https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/>

[\[back to 3\]](#)

[4] ITU, The Gender Digital Divide,

<https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-the-gender-digital-divide/>

[\[back to 4\]](#)

[5] UN, Secretary General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, July 2015,

<https://digitallibrary.un.org/record/799853?ln=en&v=pdf> [\[back to 5\]](#)

TAGS

[Bureau of Cyberspace and Digital Policy](#)

[Cyber Issues](#)

[Cyber Security](#)

White House

USA.gov

Office of the Inspector General

Archives

Contact Us

EXHIBIT 10



December 5, 2023

The White House
Eisenhower Executive Office Building
639 17th St NW
Washington DC, 20500

Cross-Border Exchange of Information with US Allies under the Indo-Pacific Economic Framework

The Global Data Alliance ([GDA](#)) respectfully offers the following recommendations in relation to your oversight and planning of overall US strategic foreign and economic policy under the Indo-Pacific Economic Framework (IPEF) in the coming months. This is the first in a series of submissions that we are preparing for your review. Later submissions will address other aspects of cross-border information exchange with US allies under the IPEF.

The GDA is a cross-industry coalition of companies, headquartered in the United States and allied nations, that are committed to high standards of data responsibility and that rely on the ability to access and transfer information across borders to innovate and create jobs. GDA member companies are active in many sectors of the economy and support millions of jobs across all 50 US states. A full list of member companies can be found on our [website](#).¹

The GDA supports the Administration's IPEF strategy of advancing common goals in four domains through collaboration and information exchange with allies. We applaud the substantial conclusion of negotiations relating to the [Supply Chain](#) (Pillar II), [Clean Economy](#) (Pillar III) and the [Fair Economy](#) (Pillar IV).

As regards Pillar I, we call for a renewed commitment to: (1) the [US Indo-Pacific Strategy](#) goals of a "free and open Indo-Pacific" that include norms to "govern our digital economies and cross-border data flows according to open principles"; (2) the [White House](#) IPEF commitment to "high-standard rules of the road in the digital economy, including standards on cross-border data flows and data localization"; and (3) the IPEF [Ministerial Statement](#) aim to "enhance access to online information and use of the Internet; facilitate digital trade; address discriminatory practices," and "work to promote and support... trusted and secure cross-border data flows."

The exchange of knowledge, ideas, and information within the IPEF supports: (1) strategic and economic alignment among Indo-Pacific allies; (2) the success of other IPEF pillars and other government policy goals, (3) national security; and (4) economic opportunity.

First, the IPEF will only succeed if IPEF partners trust one another and work together. This requires – among other things – a posture of openness and a willingness not to impose cross-border data restrictions on one another for arbitrary, discriminatory, disguised, or unnecessary reasons. To permit IPEF Parties to impose such restrictions on one another is antithetical to the very notion of an international agreement among allies.

Second, to fulfill the promise of Pillars II – IV, it is important that all IPEF partners make baseline commitments not to unreasonably restrict each other's access to information necessary to address [supply chain](#), [climate](#), [anti-corruption](#), [labor](#), and [mutual legal assistance](#) goals. More broadly, such cross-border data restrictions also undermine other policies, since such restrictions will hurt [developing countries](#) and [small businesses](#); impede [financial equity and inclusion](#); undermine [national security](#) and [cybersecurity](#); threaten [human rights](#); slow [science and innovation](#); and impair various [health and safety](#), [environmental](#), and other [regulatory compliance](#) priorities.

Third, it is in the US national security interest to agree with Indo-Pacific allies on cross-border data norms. (*See* [National Security Strategy](#); [National Cybersecurity Strategy](#)). Failure to agree brings significant risk: If the United

States doesn't set such rules with its allies, then US adversaries will fill the vacuum. Those governments will be free to replace norms that reflect US interests, US values, and US law with new norms that don't.

Finally, permitting IPEF partners to impose arbitrary, discriminatory, disguised, or unnecessary cross-border data restrictions on one another jeopardizes jobs and economic opportunity in the United States and among its allies. Such restrictions harm GDP ([minus 0.7-1.7%](#)); investment flows ([minus 4%](#)); productivity ([4.5% loss](#)); and small business ([up to 80% higher trade costs](#)). As the [World Bank](#) has noted, “[r]estrictions on data flows have large negative consequences on the productivity of local companies.” As the [United Nations](#) has stated, “regulatory fragmentation in the digital landscape...is most likely to adversely impact low-income countries, less well-off individuals, and marginalized communities the world over, as well as worsen structural discrimination against women. A future of exclusionary digital development must be avoided at all costs.”

To avoid such a future, it is instructive to review the dozen digital economy frameworks already agreed by some 40 US allies.² These existing frameworks support more predictable information sharing among allies, and they all contain safeguards to promote democratic norms of due process and governmental accountability.

In contrast, an unsuitable model for the IPEF would be the China-led Regional Comprehensive Economic Partnership (RCEP). The [RCEP](#) adopts a self-judging, “[anything goes](#)” approach to governmental conduct in the digital environment. More specifically, the RCEP effectively gives license for Parties to the Agreement to impose arbitrary, discriminatory, disguised, or unnecessary cross-border data restrictions on other Parties. To adopt similar positions – whether in the name of “[policy space](#)” or for other reasons – would create an appearance of [alignment](#) with the digital authoritarian policies that the IPEF was intended to counter.

We urge you to advance an IPEF that is built on trust amongst allies and on “[the rule of law and accountable democratic governance](#).” To that end, we urge you to fulfill the [shared promises](#) that the United States and other IPEF partners made to their populations to “enhance access to online information and use of the Internet; facilitate digital trade; address discriminatory practices,” and “work to promote and support... trusted and secure cross-border data flows.” These outcomes are central to the success of the IPEF and the promotion of an Indo-Pacific that is ‘[open, connected, prosperous, resilient, and secure](#).’

¹ GDA member companies are active in the accounting, agriculture, automotive, aerospace and aviation, biopharmaceutical, consumer goods, energy, film and television, finance, healthcare, hospitality, insurance, manufacturing, medical device, natural resources, publishing, semiconductor, software, supply chain, telecommunications, and transportation sectors. GDA member companies have operations and support millions of jobs across all 50 US states. For more information, see <https://www.globaldataalliance.org>

² These include the cross-border data and localization provisions found in principles of governmental accountability and good governance are reflected in provisions found in the [Digital Economy Partnership Agreement](#) (DEPA), [Australia-Singapore Digital Economy Agreement](#) (DEA), [Australia-UK Free Trade Agreement](#) (FTA), [Japan-EU Economic Partnership Agreement](#) (EPA), [Japan-UK EPA](#), [Japan-US Digital Trade Agreement](#) (DTA), [Korea-Singapore DPA](#), [UK-NZ FTA](#), [UK-Singapore DEA](#), the [UK-Ukraine DTA](#), as well as the [USMCA](#), [CPTPP](#), and the GDA's [model digital trade provisions](#). While all of these agreements are useful model frameworks, we note that some should be updated in key respects (e.g., the cross-border data and localization obligations in the CPTPP and DEPA should be extended to financial services).

EXHIBIT 11



September 13, 2022

The Honorable Sarah Bianchi
Deputy US Trade Representative
Office of the US Trade Representative
600 17th Street, NW
Washington DC, 20508

Dear Ambassador Bianchi,

The Global Data Alliance¹ (GDA) congratulates the United States on the conclusion of the Indo-Pacific Economic Framework (IPEF) Ministerial Meeting held on September 8-9, 2022. We introduce through this submission the GDA and our priorities for the IPEF.

I. Introduction

The GDA 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.² GDA member companies, which have headquarters and operations around the world, employ tens of millions of workers across the Indo-Pacific region, including in IPEF economies. GDA member companies are active in a broad array of sectors, including aerospace, agriculture, automotive, energy, electronics, finance, health, logistics, and telecommunications, among others. Data transfers and digital networks lie at the heart of the IPEF economy: They support jobs in every country, across every sector, and at every stage of the value chain in billions of transactions every day.

The GDA applauds IPEF economies for agreeing in the September 9 Ministerial Statement to “advancing inclusive digital trade by building an environment of trust and confidence in the digital economy; enhancing access to online information and use of the Internet; facilitating digital trade; addressing discriminatory practices; and advancing resilient and secure digital infrastructure and platforms.” The GDA also welcomes IPEF economies’ commitment to “work to promote and support, inter alia: (1) trusted and secure cross-border data flows; (2) inclusive, sustainable growth of the digital economy; and (3) the responsible development and use of emerging technologies.”

The GDA also respectfully encourages IPEF economies to specifically include “trusted and secure cross-border data flows” (noted above) as part of “early harvest” negotiating outcomes – thus addressing the cross-border digital interests of all IPEF economies, their industries, and their workers, including in the automotive,³ clean energy,⁴ finance,⁵ healthcare,⁶ logistics,⁷ medical technology, pharmaceutical, software, semiconductor, and telecommunications sectors.⁸

II. Discussion

The GDA urges IPEF economies participating in the digital trade negotiations (*hereinafter* “IPEF digital trade negotiators”) to agree on an “early harvest” of cross-border data commitments.

A. Proposed Cross-Border Data Commitments in IPEF

Consistent with prior agreements among IPEF economies,⁹ this “early harvest” should cover:

- Cross-Border Transfer of Information by Electronic Means: Across all sectors, Parties shall not prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of a business.
- Location of Computing Facilities: Across all sectors, Parties shall not impose requirements to use or locate computing facilities in their own territory as a condition for conducting business.
- Custom Duties: Parties shall not impose customs duties on electronic transmissions.

These commitments focus on the impact that data regulations may have on trade among IPEF economies, and do not prevent governments from enacting rules to promote data privacy, data security, or other policy goals. These commitments are also designed, as framed in the September 9 IPEF Ministerial Statement, to accommodate “the rapidly evolving nature of digital technology” as well as “flexibilities to achieve public policy objectives, including protecting the rights and interests of our diverse communities.” This is because the commitments focus on the cross-border impacts of data regulations – rather than their substantive privacy, security, or other legal aspects.

To address the cross-border impacts of any data regulations that involve incidental restrictions on data transfers,¹⁰ we urge IPEF digital trade negotiators to clarify that such data regulations:

- Be necessary to achieve a legitimate public policy objective;¹¹
- Not be applied in a manner that would result in arbitrary or unjustifiable discrimination or a disguised restriction on trade;¹²
- Not impose restrictions on transfers that are greater than necessary;¹³
- Not improperly discriminate among different economic sectors;¹⁴
- Not discriminate against other IPEF-based service providers by modifying conditions of competition by treating cross-border data transfers less favorably than domestic ones;¹⁵
- Be designed to be interoperable with other IPEF members’ legal frameworks to the greatest extent possible;¹⁶ and
- Be developed in a transparent and accountable manner.

The bulleted list above reflects longstanding tenets of international law and practice, namely: (1) the freedom to pursue necessary public policy objectives; (2) the renunciation of discrimination against non-national persons, products, services, or technologies; (3) the commitment to minimize trade-restrictive effects; and (4) due consideration for trading partner laws.¹⁷

B. Other Topics that Implicate Cross-Border Data Transfers

While this submission focuses on the commitments regarding data transfers, localization, and customs duties above, several other IPEF provisions also implicate data transfers and digital trust. Among others,¹⁸ these provisions relate to personal data protection and cybersecurity, as explained below.

- Data Transfers & Personal Data Protection: Cross-border transfer mechanisms may be necessary to ensure data is protected even if transferred across borders. Where appropriate, the IPEF could promote such mechanisms (such as standard contracts, binding corporate rules, certification mechanisms, etc.), that help ensure that data is protected even as it is transferred across borders. The IPEF could also promote cross-border interoperability among different countries’ personal data protection rules through mechanisms such as the Global Cross-Border Privacy Rules Forum.
- Data Transfers & Cybersecurity: Data transfers help improve cybersecurity because they allow for cybersecurity tools to monitor traffic patterns, identify anomalies, and divert potential threats in ways that depend on global access to real-time data. Given the role of data transfers in promoting timely visibility and response to emergent cyberthreats, the IPEF could helpfully promote risk-based approaches that rely on internationally recognized standards and risk management best practices to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity events.¹⁹

III. Conclusion

For the reasons explained above, we respectfully urge all IPEF digital trade negotiators to include the “trusted and secure cross-border data flow” priorities from the September 9 IPEF Ministerial Statement among a package of “early harvest” digital outcomes. These “early harvest” outcomes should address, at a minimum, data transfers, localization mandates, and customs duties on electronic transmissions. Permitting unnecessary cross-border data restrictions to persist and proliferate across the Indo-Pacific region is incompatible with the potential of the IPEF framework to bind Indo-Pacific economies more closely together. Such restrictions impose significant costs on IPEF governments, workers, consumers, and enterprises – exacerbating digital fragmentation and the digital divide. Failing to address this economic and policy challenge would be a significant missed opportunity and would result in an agreement that would likely lack commercial significance or support from many industry and stakeholder groups.

The Global Data Alliance welcomes the opportunity to provide this submission and we look forward to continuing to work with you. Please let us know if you have any questions or comments.

Sincerely yours,

Joseph Whitlock

Joseph P. Whitlock
Executive Director
Global Data Alliance
josephw@bsa.org

¹ For more information on the Global Data Alliance, please see: <https://www.globaldataalliance.org/>

² While Alliance member companies have a range of interests in the IPEF negotiations, this submission focuses exclusively on the cross-border data aspects of the negotiations.

³ Global Data Alliance, *GDA Website – Automotive* (2022), at: <https://globaldataalliance.org/sectors/automotive/>

⁴ Global Data Alliance, *GDA Website – Energy* (2022), at: <https://globaldataalliance.org/sectors/energy/>

⁵ Global Data Alliance, *GDA Website – Finance* (2022), <https://globaldataalliance.org/sectors/finance/>

⁶ Global Data Alliance, *GDA Website – Healthcare* (2022), <https://globaldataalliance.org/sectors/healthcare/>;
Global Data Alliance, *GDA Website – Biopharmaceutical R&D* (2022),
<https://globaldataalliance.org/sectors/biopharmaceutical-rd/>

⁷ Global Data Alliance, *GDA Website – Supply Chain Logistics* (2022), <https://globaldataalliance.org/sectors/supply-chain-logistics/>

⁸ Global Data Alliance, *GDA Website – Telecommunications* (2022),
<https://globaldataalliance.org/sectors/telecommunications/>

⁹ These commitments should be built on prior agreements involving IPEF Parties. These agreements include the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP), the Australia-Singapore Digital Economy Agreement (DEA), the Digital Economy Partnership Agreement (DEPA), the UK-Japan Economic Partnership Agreement, as well as the United States-Mexico-Canada Agreement (USMCA) and the US-Japan Digital Trade Agreement, which contain the most advanced cross-border data provisions in any agreement.

¹⁰ As connectivity and data have become integrated into every aspect of our lives, data-related regulation has become common in many areas: data privacy, cybersecurity, intellectual property, online health services – to name a few. Globally, the number of data regulations grew by over 800% between 1995 and 2015, and exceeds 250 today. See OECD, *Trade and Cross-Border Data Flows*, OECD Trade Policy Papers (2019), at: <https://www.oecd-ilibrary.org/docserver/b2023a47-en.pdf?expires=1636811939&id=id&accname=quest&checksum=4D81CCF1C6E59168A9C5AE0E43F3F9FB>

¹¹ See e.g., US-Japan DTA Art. 11.2; USMCA Art. 19.11.2.

¹² See e.g., US-Japan DTA Art. 11.2(a); USMCA Art. 19.11.2(a).

¹³ See e.g., US-Japan DTA Art. 11.2(b); USMCA Art. 19.11.2(b).

¹⁴ See e.g., US-Japan DTA Art. 12-13; USMCA Chapter 17.

¹⁵ See e.g., US-Japan DTA Art. 11, footnote 9; USMCA Art. 19.11, footnote 5.

¹⁶ See e.g., US-Japan DTA Art. 15.3; USMCA Art. 19.8.4, 19.8.6.

¹⁷ In the WTO context, these tenets – which trace back to the 1947 General Agreement on Tariffs and Trade – now apply to all multilateral trade rules, including those relating to goods, services, investment, technical regulations, and customs procedures. In the same spirit, IPEF digital trade negotiators should explicitly extend these core tenets to trade rules relating to the cross-border movement of data.

¹⁸ Other topics that implicate data transfers and digital trust include:

- Data Transfers & Mandates to Force Technology Transfer or Source Code Disclosure: Data transfers enabled by software are critical to economic development. Unfortunately, some countries mandate involuntary access, transfer, or disclosure of proprietary source code as a condition of market access or for other improper purposes. While a regulatory body should be free to require an entity to make available source code for a specific investigation, enforcement action, or judicial proceeding, governments should not force technology transfer or source code disclosure for industrial policy, industrial espionage, cyber-exfiltration, or other improper purposes. Such measures not only increase the risk of malicious cyberactivity, but also discourage companies from providing cross-border access to their technologies or engaging in beneficial data transfers. By prohibiting such mandates, IPEF can continue to encourage cross-border access to technology.
- Data Transfers & Data Analytics: Recognizing that data transfers and the consolidation of data sets across borders are critical to data analytics and AI tools, IPEF provisions could helpfully promote AI risk management best practices, which are more compatible with the responsible application of these tools to data sets consolidated across borders than top-down restrictions that fail to acknowledge the rapidly

evolving nature of digital technology. Data transfers are integral to every stage of the AI life cycle, from the development of predictive models to the deployment and use of AI systems. The data used in AI systems often originates from many geographically dispersed sources, making it imperative that data can move freely and securely across borders. To secure for themselves the insights and other benefits that AI systems can provide, IPEF economies should agree to the responsible and secure cross-border movement of data for analytics and AI purposes.

- Data Transfers & Technical Barriers to Digital Trade: International standards development organizations (SDOs) convene companies from across the region to voluntarily contribute their innovations to the development of new international technology standards. Cross-border data transfers and technology access lie at the heart of this beneficial process. Unfortunately, technical regulations and mandatory national standards are sometimes misused (often in conjunction with data restrictions) to discriminate against non-national persons and technologies. By supporting the development and adoption of voluntary, internationally recognized standards, IPEF could help avoid the creation of new cross-border digital barriers.

¹⁹ Cross-border data transfers help improve cybersecurity because these transfers allow for cybersecurity tools to monitor traffic patterns, identify anomalies, and divert potential threats in ways that depend on global access to real-time data. Stronger cybersecurity is enabled by cross-border data analytics an assertive cyber-defense posture coordinated across IT networks and national boundaries. When governments mandate localization or restrict the ability to transfer and analyze data in real-time, they create unintended vulnerabilities. See generally, BSA, *Moving to the Cloud – A Primer on Cloud Computing* (2018), at https://www.bsa.org/files/reports/2018BSA_MovingtotheCloud.pdf

Annex: Evidentiary Support for IPEF Cross-Border Data Commitments

To deliver on IPEF’s promise of shared Indo-Pacific prosperity and economic opportunity, it is critical that the IPEF contain cross-border data commitments that can help all Parties benefit from cross-border access to information, knowledge, and digital tools. There is widespread evidence of these benefits, some of which is summarized below.

Data Transfers & Economic Growth: Cross-border data transfers – valued in the trillions of dollars¹ – benefit regional economic growth. The World Bank’s 2020 *World Development Report* found that, “[c]ountries would gain on average about 4.5 percent in productivity if they removed their restrictive data policies, whereas the benefits of reducing data restrictions on trade in services would on average be about 5 percent.”² Local enterprises rely on data flows to drive quality, reach international customers, achieve economies of scale, and improve output,³ often benefiting from cross-border access to tailored data-enhanced analytics and insights.⁴ Cross-border data commitments can promote economic growth and job creation among IPEF economies.

Data Transfers & Manufacturing: Cross-border data transfers are especially beneficial to manufacturing industries, which depend on access to international supply chains, and which increasingly integrate Internet-of-Things (IoT) technologies on the shop floor and across assembly lines. It has been estimated that 75% of the value of data transfers accrues to manufacturing and other industries.⁵ Conversely, data restrictions are harmful in this area. For example, a 2021 GSMA study conducted in three developing regions (in South America, South-East Asia and Africa) indicates that data localization measures on IoT applications and machine-to-machine (M2M) data processing could result in: (a) loss of 59-68% of their productivity and revenue gains; (b) investment losses ranging from \$4-5 billion; and (c) job losses ranging from 182,000-372,000 jobs.⁶ Cross-border data commitments can promote manufacturing across the IPEF region.

Data Transfers & Services: As services are increasingly enabled by digital means, cross-border data transfers have increased in importance. A 2020 World Economic Forum study found that, “approximately half of cross-border [services] trade is enabled by digital connectivity[, which] ... has allowed developing countries and micro, small and medium-sized enterprises (MSMEs) to export through greater visibility, easier market access and less costly distribution. ... Developing countries ... accounted for 29.7% of services exports in 2019.”⁷ Cross-border data commitments can help support the growth of services across the region.

Data Transfers & Trade Facilitation: Cross-border technology access and data transfers also [reduce supply chain-related transaction costs](#).⁸ One recent study estimates that digital tools helped MSMEs across Asia reduce export costs by 82% and transaction times by 29%.⁹ Likewise, the Asia Development Bank Institute estimates that electronic commerce platforms, which operate on the basis of cross-border data transfers, have helped some local firms reduce the cost of distance in trade by 60%.¹⁰ Cross-border data commitments in IPEF can help promote these efficiencies.

Data Transfers & Sustainable Agriculture: Cross-border access to green technologies, satellite-based data, and other information helps small-scale agricultural producers improve crop yields; mitigate crop risks (including losses from pests, disease, and weather-related events); reduce arbitrage by middlemen (up to 70 percent of smallholder production value is captured by intermediaries); and promote sustainability (agriculture accounts for 70 percent of water use, while one third of global food production is either lost or wasted).¹¹ Cross-border data commitments can help promote uptake of sustainable agricultural practices and technologies across the region.

Data Transfers & Sustainable Economic Development: Analyses by development banks consistently show that cross-border access to technology and data transfers promote sustainable economic growth. For example, there remain over 2.5 billion unbanked people worldwide, many living in remote locations lacking physical banking infrastructure.¹² The US Agency for International Development (USAID) estimates that, by enabling digital financial services that leverage cross-border data, the GDP of emerging economies could increase by more than \$3.5 trillion, or 6 percent, by 2025.¹³

Unfortunately, some Indo-Pacific economies are erecting costly data transfer restrictions vis-à-vis one another.¹⁴ As UNCTAD has explained, such “digital fragmentation”:

reduces market opportunities for domestic MSMEs to reach worldwide markets, [and] ... reduces opportunities for digital innovation, including various missed opportunities for inclusive development that can be facilitated by engaging in data-sharing through strong international cooperation. ... [M]ost small, developing economies will lose opportunities for raising their digital competitiveness.¹⁵

Economic development depends upon cross-border access to knowledge, digital tools, and commercial opportunities. Cross-border data commitments in IPEF can help promote such access.

Data Transfers & Privacy: Some argue that data localization requirements and cross-border data restrictions are necessary for privacy reasons – i.e., to ensure that companies process and use data consistent with a country’s data protection laws. This argument is incorrect. Cross-border restrictions are not necessary to protect privacy and can undermine data security. In lieu of such restrictive policies, countries with robust data protection frameworks often adhere to the accountability principle and interoperable legal frameworks that protect data consistent with national standards, even as the data is transferred across borders. Organizations that transfer data globally typically adopt a set of best practices and internal controls to ensure that the data is protected even when transferred outside of the country. To that end, organizations often rely on various approved data transfer mechanisms, as discussed above.¹⁶

Data Transfers & Cybersecurity: Some argue that cross-border data restrictions are necessary to ensure cybersecurity. However, *how* data is protected is more important to security than *where* it is stored, and transfer restrictions often result in *weaker*, not *stronger*, cybersecurity. Cross-border data transfers help improve cybersecurity because these transfers allow for cybersecurity tools to monitor traffic patterns, identify anomalies, and divert potential threats in ways that depend on global access to real-time data. Stronger cybersecurity is enabled by cross-border data analytics an assertive cyber-defense posture coordinated across IT networks and national boundaries.¹⁷ When governments mandate localization or restrict the ability to transfer and analyze data in real-time, they create unintended vulnerabilities.¹⁸

Data Transfers & Regulatory Compliance: Some claim that cross-border data restrictions ensure governmental access to data for regulatory or investigatory purposes. The location of the data, however, is not the determining factor. On the contrary, “data localization requirements can increase ... operational risks, hinder risk management and compliance, and inhibit financial regulatory and supervisory access to information.” Accordingly, regulatory authorities in many countries actually encourage the responsible transfer of data across borders. Likewise, data transfers are critical to other public policy priorities, including anti-money laundering; anti-corruption; and other legal compliance objectives.¹⁹

Data Transfers & Fraud Prevention: Prohibitions on cross-border data transfers in respect of financial data can have significant negative impacts on the effectiveness of fraud prevention and mitigation tools. Effective fraud mitigation as provided by banks, card networks and other players in

the financial services sector demands sophisticated monitoring and rapid detection at the time of transaction to interpret and weigh the risk of fraud of each payment transaction as weighed by the facts of that payment transaction as against norms for all payment transactions and that account. Fraud detection models are typically built on global transaction data or transaction data collected from multiple countries since fraud patterns are not limited by national boundaries. Fraud trends which appear in one region or country may apply in others as cardholders travel to different countries, cardholders transact online with merchants in different countries, and the perpetrators of fraud do not respect any national boundary lines. Thus, to build effective fraud models and to gain the necessary insights into fraudulent activity in order to help prevent them, these models must be built off of global or multi-country data sets, based both on the location of the merchant and the location of the cardholder.

Data Transfers & Innovation: Some claim that cross-border data restrictions promote innovation. On the contrary, [data localization mandates and data transfer restrictions undermine beneficial innovation processes](#)—from accessing global scientific and technical research databases, to engaging in cross-border research and development (R&D), to securing intellectual property rights for new inventions, and regulatory product approvals for new products and services.²⁰

Data Transfers & Healthcare: Healthcare R&D, the submission of health-technology-assessment and regulatory filings, and the provision of services in the life-science industries are increasingly cross-border endeavors which rely on the responsible and secure flow of large volumes of data. These transfers can support the adoption of data analytics and machine-learning technologies, and processing of data from multi-country clinical studies and other research activities. Supporting cross-border data transfers, in a way that is compatible with the best practices in ensuring patient and customer privacy, is essential for the innovation of healthcare products and services, collaboration across multiple public and private research organizations, and the early detection of regional or global health risks. Restricting such data transfers will undermine the ability to identify new treatments and improve healthcare delivery, to the ultimate detriment of patients in those countries that restrict transfers.²¹

Data Transfers & ICT Policies: From artificial intelligence to 5G to the cloud, governmental ICT policies can help coordinate public-private dialogue, support investment, and maximize the benefits of ICT technologies across the economy. Cross-border data restrictions often undermine these policies. For example, the benefits of a “cloud first” policy are most likely to arise in a cross-border context that allows for elastic and scalable delivery of computing resources, rapid load balancing, and ready access to best-in-class technology from all over the world. Using data localization mandates and transfer restrictions to ban cross-border access to cloud computing infrastructure and technology would deprive local enterprises (including MSMEs) and users of:

- Cross-border access to IT resources hosted abroad;
- Cross-border collaboration and communication with foreign business partners;
- Foreign transactions and business opportunities; and
- Improved resiliency resulting from data storage across multiple geographical locations

Data Transfers & COVID-19 Recovery: As governments seek to limit the spread of COVID-19, cross-border access to technology and data transfers have become essential for countries seeking to sustain jobs, health, and education. This is particularly true for the [remote work](#), [remote health](#), [supply chain management](#), and [innovation](#)-related technologies that depend on cross-border access to cloud computing resources.

¹ Global Data Alliance, *Cross-Border Data Transfers - Facts and Figures* (2020), at: <https://globaldataalliance.org/wp-content/uploads/2021/07/gdafactsandfigures.pdf>

² World Bank, *World Development Report* (2020), at: <https://www.worldbank.org/en/publication/wdr2020> . Conversely, the World Bank also found that, “restrictions on data flows have large negative consequences on the productivity of local companies using digital technologies...”

³ Data localization mandates and unnecessary data transfer restrictions hurt local innovation because a country that limits cross-border data transfers limits its own industries’ access to technologies and data sources that are critical to growth and innovation, business operations, and the transfer of technology. These include: (a) growth-enhancing software solutions; (b) scientific, research, and other publications; and (c) manufacturing data, blueprints, and other operational information. Faced with higher software costs and an unpredictable environment for R&D investments, local industries face challenges keeping technological pace with foreign competitors — threatening both domestic and export market sales. Furthermore, as data restrictions place an undue burden on industries operating in countries imposing them, they also undermine those countries’ attractiveness as a destination for investment and R&D.

⁴ Local enterprises face competitive harm if they are deprived of the insights that come from consolidating local data sets within larger regional or global data sets for purposes of data analysis. See generally, BSA, *Understanding Artificial Intelligence* (2017), at: https://www.bsa.org/sites/default/files/2019-03/BSA_2017UnderstandingAI.pdf ; BSA, *What’s the Big Deal with Data* (2017), at: <https://data.bsa.org/>; BSA, *Artificial Intelligence in Every Sector* (2019), at: https://www.bsa.org/sites/default/files/2019-03/BSA_2018_AI_Examples.pdf

⁵ See Global Data Alliance, *The Cross-Border Movement of Data: Creating Jobs and Trust Across Borders in Every Sector* (2020), at <https://www.globaldataalliance.org/downloads/GDAeverysector.pdf> ; See Global Data Alliance, *Jobs in All Sectors Depend Upon Data Flows* (2020), at <https://www.globaldataalliance.org/downloads/infographicgda.pdf>; Global Data Alliance, *Cross-Border Data Transfers Facts and Figures* (2020), at <https://www.globaldataalliance.org/downloads/gdafactsandfigures.pdf>

⁶ GSMA, *Cross-border Data Flows – The Impact of Localization on IOT* (2021).

⁷ World Economic Forum, *Paths Towards Free and Trusted Data Flows* (2020). Conversely, the World Bank 2021 *World Development Report* has noted that measures that “restrict cross-border data flows ... [may] materially affect a country’s competitive edge in the burgeoning trade of data-enabled services.” World Bank, *World Development Report – Data For Better Lives* (2021), at: <https://openknowledge.worldbank.org/bitstream/handle/10986/35218/9781464816000.pdf>

⁸ Global Data Alliance, *Cross-Border Data Transfers and Supply Chain Management* (2021), at <https://globaldataalliance.org/downloads/03182021gdaprimersupplychain.pdf>

⁹ Micro-Revolution: The New Stakeholders of Trade in APAC, Alphabet, 2019.

¹⁰ Asia Development Bank Institute, *The Development Dimension of E-Commerce in Asia: Opportunities and Challenges* (2016), at: <https://www.adb.org/sites/default/files/publication/185050/adbi-pb2016-2.pdf>

¹¹ See e.g., Global Data Alliance, *Access to Global Markets, Innovation, Finance, Food, and Healthcare* (2021); Every Sector Is a Software Sector: Agriculture, https://software.org/wp-content/uploads/Every_Sector_Software_Agriculture.pdf; World Bank, *Agriculture and Food* (2020), <https://www.worldbank.org/en/topic/agriculture/overview>; IDB Climate Smart Agriculture, *Thematic Paper: Climate-Smart Agriculture* (Revised Version), p. 5, <http://www.iadb.org/document.cfm?id=EZSHARE-1914875107-52>. The IDB explains the underlying challenge that cross-border access to technologies and export markets can help ameliorate: “Smallholders typically capture a low share of the final value of its products and encounter non-transparent commercialization markets and difficulties in buying inputs and selling their products at fair prices. On top of that, small farm holders typically face limited access to export to new markets and unfavorable prices in international trade, and they are particularly vulnerable to volatility in commodity prices.”

¹² USAID, US Global Development Lab website, available at: <https://www.usaid.gov/digital-development/digital-finance>

¹³ See US Agency for International Development, *Digital Strategy 2020-2024* (2020), at: https://www.usaid.gov/sites/default/files/documents/15396/USAID_Digital_Strategy.pdf; see also See Global Data Alliance, *Access to Global Markets, Innovation, Finance, Food, and Healthcare* (2021). Technologies that leverage data transfers help increase access – particularly as 95% of the world’s population is already covered by mobile broadband networks and as new low-earth orbit satellite technologies bring connectivity to previously unserved communities. See e.g., Ericsson, *Ericsson Mobility Report* (November 2019), at:

<https://www.ericsson.com/en/mobility-report/reports/november-2019>; Global Data Alliance, *Cross-Border Data Transfers & Telecommunication Network Technologies* (2021), at: <https://globaldataalliance.org/wp-content/uploads/2021/10/10042021cbdttelecom.pdf>

¹⁴ See e.g., USTR, *2021 National Trade Estimate Report on Foreign Trade Barriers* (March 2021), at: <https://ustr.gov/sites/default/files/files/reports/2021/2021NTE.pdf>

¹⁵ UNCTAD, *Digital Economy Report* (2021), at: https://unctad.org/system/files/official-document/der2021_en.pdf

¹⁶ For additional information, see <https://www.globaldataalliance.org/downloads/02112020GDAcrossborderdata.pdf>

¹⁷ See generally, BSA, *Moving to the Cloud – A Primer on Cloud Computing* (2018), at https://www.bsa.org/files/reports/2018BSA_MovingtotheCloud.pdf Cloud services delivered across-borders provide security advantages over alternative IT delivery approaches (on-premises or local cloud services):

- Physical Security: Certified personnel can carefully monitor servers 24/7 to prevent physical breaches, and can apply consistent protocols over a small number of locations.
- Data Security: CSPs can ensure data integrity through use of state-of-the-art encryption protocols for data at-rest and in-transit. CSPs can establish redundant backups of data in geographically dispersed data centers, mitigating risk of loss in the event of power outages or natural or manmade disasters.
- Advanced Threat Detection: CSPs leverage state-of-the-art enhanced security intelligence. They use regular penetration testing to simulate real-world attacks and evaluate security protocols against emerging threats.
- Automated Patch Deployment: Automated and centralized patch deployment and realtime updates to network security protocols work to protect systems from newly identified vulnerabilities.
- Incident Management and Response: CSPs maintain global teams of incident response professionals to respond and mitigate the effects of attacks and malicious activity.
- Certification: CSPs are typically certified to international security standards, and go through regular audits to maintain their certifications.

¹⁸ See *id.*, p. 1.

¹⁹ See e.g., United States-Singapore Joint Statement on Financial Services Data Connectivity, at: <https://www.mas.gov.sg/news/media-releases/2020/united-states-singapore-joint-statement-on-financial-services-data-connectivity>

²⁰ See Global Data Alliance, *Cross-Border Data Transfers and Innovation* (2021), at <https://globaldataalliance.org/downloads/04012021cbdtinnovation.pdf>

²¹ Global Data Alliance, *GDA Website – Healthcare* (2022), <https://globaldataalliance.org/sectors/healthcare/>; Global Data Alliance, *GDA Website – Biopharmaceutical R&D* (2022), <https://globaldataalliance.org/sectors/biopharmaceutical-rd/>

EXHIBIT 12

May 26, 2023

The Honorable Gina Raimondo
Secretary
U.S. Department of Commerce
1401 Constitution Ave.
Washington, DC 20520

The Honorable Katherine Tai
United States Trade Representative
Executive Office of the President
NW 600 17th Street NW
Washington, DC 20508

Dear Secretary Raimondo and Ambassador Tai:

The U.S. business and agriculture community welcomed the administration's launch of the Indo-Pacific Economic Framework (IPEF) talks to advance U.S. commercial interests in a critical region. We are eager to support stronger U.S. engagement in the Indo-Pacific region and to work in partnership with the administration and our regional allies to promote fair and inclusive trade, supply chain resilience, and the clean economy transition. However, we are growing increasingly concerned that the content and direction of the administration's proposals for the talks risk not only failing to deliver meaningful strategic and commercial outcomes but also endangering U.S. trade and economic interests in the Indo-Pacific region and beyond.

The U.S. business and agriculture community regrets the administration's decision not to engage in negotiations to remove tariffs and other market access barriers facing U.S. manufacturing, services, financial services, and agricultural exports. However, it is unclear why some traditional U.S. trade priorities that could deliver meaningful benefits for American exporters are being sidelined in the IPEF talks. For example, the United States has long pursued trade rules that seek to address standards-related and other technical barriers to trade, measures that discourage trade in remanufactured goods, inadequate intellectual property protections, and sector-specific regulatory barriers that impede exports of autos, chemicals, cosmetics, pharmaceuticals, medical devices, and ICT products; the same is true for sanitary and phytosanitary standards and their importance to U.S. agricultural exports. Obtaining IPEF commitments in these areas would help facilitate trade in sectors where the competitiveness of U.S. companies is stymied by the proliferation of non-tariff barriers overseas. These barriers also undermine supply chain resiliency, potentially sapping the benefit of future IPEF commitments. The administration's interactions to date with the stakeholder community offer no insight into how or why these non-market access issues of high importance to trade have been left out of the IPEF talks.

Further, we are deeply concerned about statements from U.S. officials and reports from the third IPEF round that suggest the administration is wavering in its promotion of high standard rules for digital trade. Data is the lifeblood of today's global economy, underpinning and enabling businesses of all sizes and in all sectors, including in manufacturing, which is increasingly data-driven. Rules in recent U.S. trade agreements seek to ensure that data can flow freely across borders, businesses and entrepreneurs are not compelled to relinquish proprietary data, and the digital output of creative industries is not disadvantaged by the mere fact that it is owned by Americans or produced in the United States. Nothing in the rules concluded by the United States and its democratic allies—including in the USMCA, which secured large, bipartisan congressional majorities—inhibits the ability of governments to regulate in the interest of privacy, protection against bias, pursuit of fair market competition, or other public policy objectives. These rules are integral to U.S. political and economic values.

The United States should use the IPEF talks to build on the outcomes achieved in past negotiations and address evolving challenges to U.S. trade. An IPEF that instead derogates

from these outcomes and abandons the core principle of nondiscrimination risks doing material harm to U.S. economic interests by emboldening restrictive foreign trade and data practices, undermining the efforts of like-minded allies to promote high standard global norms, and ceding U.S. leadership on rulemaking for the digital economy.

Getting these trade rules right matters to the 41 million Americans whose jobs depend on trade, the manufacturers who export nearly half of all U.S. industrial production to customers abroad, the service providers whose ability to tap export markets is being transformed by digital technologies, and the farmers and ranchers for whom export markets at times represent more than half of sales. A “worker centric” trade agenda must reflect how American companies and the workers they employ suffer together when we are barred from selling the goods and services we produce in foreign markets.

In light of the concerns cited above, we strongly urge the administration to change course and use the IPEF to deliver outcomes that advance the interests of American workers, farmers, and companies.

Sincerely,

ACT The App Association	National Association of Manufacturers
American Chemistry Council	National Foreign Trade Council
American Council of Life Insurers	National Pork Producers Council
American Forest & Paper Association	National Retail Federation
American Seed Trade Association (ASTA)	North American Association of Food Equipment Manufacturers (NAFEM)
Autos Drive America	North American Meat Institute
BSA The Software Alliance	Pharmaceutical Research and Manufacturers of America (PhRMA)
Business Roundtable	Retail Industry Leaders Association
Coalition of Services Industries (CSI)	Securities Industry & Financial Markets Association (SIFMA)
Computer and Communications Industry Association (CCIA)	Software & Information Industry Association (SIIA)
Consumer Technology Association	United States Council for International Business
Distilled Spirits Council of the U.S.	U.S. Apple Association
Global Data Alliance	USA Rice
Hardwood Federation	U.S. Chamber of Commerce
Information Technology Industry Council (ITI)	U.S. Dry Bean Council
International Dairy Foods Association	
International Fresh Produce Association	
Leather & Hide Council of America	
MEMA, The Vehicle Suppliers Association	

cc: Jake Sullivan, National Security Advisor
Lael Brainard, Director of the National Economic Council
The Honorable Antony Blinken, Secretary of State
The Honorable Tom Vilsack, Secretary of Agriculture
Members of the House Committee on Ways and Means
Members of the Senate Committee on Finance

EXHIBIT 13

December 7, 2022

The Honorable Gina Raimondo
Secretary of Commerce
U.S. Department of Commerce
1401 Constitution Ave. NW
Washington, DC 20520

The Honorable Katherine Tai
United States Trade Representative
Executive Office of the President
600 17th St. NW
Washington, DC 20508

Dear Secretary Raimondo and Ambassador Tai:

On behalf of the undersigned organizations, we welcome the Biden Administration's commitment to promote free, fair, and inclusive trade and investment through the Indo-Pacific Economic Framework (IPEF). We agree that strengthening trade, investment, and economic ties with the region offers broad and substantial benefits to all Americans and to U.S. national security interests. In particular, we urge you to include in the IPEF strong, binding digital trade rules, without which its promise for U.S. workers and companies will be greatly diminished.

The case for enhanced U.S. engagement with the Indo-Pacific region is strong. With 1.5 billion people in the region projected to join the middle class this decade, the market presents significant opportunities for American goods and services. The Indo-Pacific already accounts for \$1.75 trillion in trade with the United States and for 30% of U.S. goods and services exports, supporting millions of American jobs.

Securing an ambitious IPEF would put the United States back on the economic and diplomatic playing field in the region. Our trading partners are not waiting on U.S. participation to advance initiatives that will define the rules of the road for digital trade. They have moved ahead with the Regional Comprehensive Economic Partnership (RCEP), the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP), and the Digital Economy Partnership Agreement. China was a leader in creating the first of these and is seeking to join the other two. The United States needs a bold response.

While our organizations have urged you to pursue strong provisions in a number of areas, securing high-standard digital trade rules in the IPEF is among the highest priorities. Such rules can help American workers and companies seize the benefits of international trade in novel ways:

- Digital trade is opening markets to American small businesses, whose reach abroad is growing dramatically thanks to e-commerce platforms and digital advertising tools that allow them to find new customers; payment systems that ensure quick, economical, and safe transactions; cloud companies that allow small businesses to operate with the sophistication of a major multinational business; and shipping, customs clearance, and fulfillment providers that

enable them to send products across the region. Innovative devices designed and produced in the United States, including by small businesses, enable the delivery of these services. A recent Global Innovation Forum [survey](#) of small businesses in the region revealed that strong digital trade commitments in the IPEF would support an increase in export sales of as much as 35% and a rise in U.S. economic output of \$72 billion.

- Digital trade is enabling businesses of all sectors to compete more effectively on the global stage—from manufacturers to medicine developers, from farmers to financial services firms—as they incorporate digital tools and cross-border data flows to develop new products and innovations, provide value-added services to their customers, and run efficient and resilient global businesses.
- Digital trade is fueling a boom in U.S. services exports, allowing continued expansion during the pandemic. About two-thirds of all professional and business services can be exported today. These growing sectors provide excellent jobs to well over 20 million Americans, and yet they are just beginning to seize the export opportunities digital trade now offers.

Unfortunately, rising digital protectionism abroad threatens to cut U.S. businesses off from these burgeoning opportunities. Scores of countries have imposed data localization measures, cross-border data flow restrictions, and other trade and regulatory barriers that threaten this growth. A July 2021 [study](#) by the Information Technology & Innovation Foundation found that “the number of data-localization measures in force around the world has more than doubled in four years. In 2017, 35 countries had implemented 67 such barriers. Now, 62 countries have imposed 144 restrictions—and dozens more are under consideration.”

A strong digital trade chapter in the IPEF can counter this trend. The excellent digital trade chapter in the U.S.-Mexico-Canada Agreement and the U.S.-Japan Digital Trade Agreement are models that should serve as a floor for the IPEF, and negotiators should draw on other innovative digital provisions developed by like-minded trading partners in the region. The IPEF’s digital trade provisions should include a ban on forced localization of data, guarantees that firms will be able to move data across borders, a prohibition on government requirements to access source code and algorithms, a commitment to provide non-discriminatory treatment for digital products, and a prohibition on parties imposing customs duties on electronic transmissions. These disciplines should apply to all sectors, without exception, including all services and financial services sectors, and they should be binding and enforceable.

The digital transformation of commerce necessitates better data governance and digital policies across the Indo-Pacific region consistent with our values and with trade principles such as non-discrimination, interoperability and least-trade-restrictive regulation, and due process and the rule of law. A successful IPEF initiative

would set new digital governance rules and digital policies that foster innovation, facilitate digital trade, enable fair and non-discriminatory regulation, enhance transparency, advance cooperation on cybersecurity and emerging technologies such as AI, foster deployment of secure and trusted next-generation networks, support digital inclusion, and promote digital enablement and skilling in the United States and across the Indo-Pacific.

Given the broad bipartisan, bicameral, and stakeholder support for U.S. leadership in the Indo-Pacific, we urge the Administration to move quickly and resolutely to advance an ambitious IPEF that includes strong digital trade provisions. The business community stands ready to partner with the Administration, Congress, and our trading partners to make sure the IPEF succeeds.

Sincerely,

ACT | The App Association
Advanced Medical Technology Association (AdvaMed)
American Council of Life Insurers
Autos Drive America
Biotechnology Innovation Organization (BIO)
BSA | The Software Alliance
Coalition of Services Industries
Computer & Communications Industry Association (CCIA)
Consumer Technology Association
Corn Refiners Association
Information Technology Industry Council
National Association of Manufacturers
National Foreign Trade Council
National Retail Federation
Pharmaceutical Research and Manufacturers of America
Software & Information Industry Association (SIIA)
The Global Data Alliance
United States Council for International Business
US-ASEAN Business Council
U.S. Chamber of Commerce

cc: Jake Sullivan, National Security Advisor
Brian Deese, Director of the National Economic Council
The Honorable Antony Blinken, Secretary of State
The Honorable Tom Vilsack, Secretary of Agriculture

EXHIBIT 14



CROSS-BORDER DATA POLICY PRINCIPLES

A forward-leaning policy on cross-border data transfers is a particularly effective tool to aid policymaker efforts to drive innovation, increase employment, and rebuild economies.¹ Recognizing the relationship between digital connectivity and economic growth has helped drive numerous [international negotiations](#) in the area of cross-border data policy.²

However, digital protectionism and data mercantilism are also growing, often associated with measures that block the cross-border transfer of data and mandate data localization.³ There remains persistent interest in these measures, even though their costs are borne primarily by the countries that adopt them.⁴

Building digital trust is an important factor in discouraging protectionist data policies. Governments should work toward legal frameworks that support a cross-border digital environment that is both open and secure, where [cross-border data transfers enhance online security and privacy](#), so that everyone can engage in remote interactions without fear of compromise.⁵ And private enterprises must also do more. This may include developing or adopting codes of conduct, internal controls, or accountability mechanisms that advance data security and privacy.

For these reasons, it is of increasing importance that like-minded countries cooperate to strengthen and reinforce an international **policy consensus** that is focused on **data transfers** and built on a **foundation of trust**.⁶ The Global Data Alliance sets out the following Cross-Border Data Policy Principles, identifying six major pillars that can strengthen this international consensus on data transfers.

PRINCIPLE 1

Countries should maintain the longstanding presumption favoring the seamless and responsible movement of data across borders

PRINCIPLE 2

Any rules impacting cross-border data transfers should be developed and maintained in accordance with good regulatory practices

PRINCIPLE 3

Any rules impacting cross-border data transfers should be non-discriminatory

PRINCIPLE 4

Any rules impacting cross-border data transfers should be necessary to achieve a legitimate objective and not impose greater restrictions than necessary

PRINCIPLE 5

Countries should support the use of accountability models aligned with international best practices to foster responsible data transfer practices

PRINCIPLE 6

Countries should work together to create trust-based frameworks that are interoperable and support the seamless and responsible movement of information across borders

“The digital economy is driven by massive cross-border information flows. Sharing data across borders allows business to access global market[s], interact with customers, communicate with suppliers and affiliates around the globe, and thereby increase efficiency and productivity.”

APEC, *Facilitating Digital Trade For Inclusive Growth* (2017)

PRINCIPLE 1

Countries should maintain the longstanding presumption favoring the seamless and responsible movement of data across borders

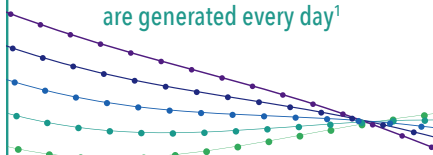
A **presumption favoring the movement of data across digital networks** reflects the reality of international economic relations today: Data moves seamlessly and securely across globally or regionally distributed cloud-based digital networks that do not match up neatly with national boundaries.⁷

Digital networks lie at the heart of our interconnected global economy. They support millions of daily transactions occurring all over the world, across every sector and at every stage of the value chain, including at the R&D, product design, regulatory approval, manufacturing, finance, marketing, sales, and post-sale service stages. Countries should not disturb the longstanding practice and presumption that data can move seamlessly and responsibly across these networks.

Cross-border data transfers are already estimated to contribute trillions of dollars to global GDP.⁸ Sixty percent of global GDP is expected to be digitized by 2022, and six billion consumers and 25 billion devices are expected to be digitally connected by 2025.⁹ Furthermore, 75 percent of the value of data transfers accrues to traditional industries like agriculture, logistics, and manufacturing.¹⁰ The ability to transfer data across borders also directly contributes toward important policy objectives that protect privacy, security, and regulatory compliance.¹¹ Many Regional Trade Agreements (RTAs) reflect this presumption.¹²

Growing the Global Economy

2.5 quintillion data bytes are generated every day¹



Data transfers contributed **\$2.8 trillion** to global GDP, growing 45x every ten years²



60% of global GDP will be digitized by 2022, with growth in every industry driven by data flows and digital technology³

¹ *World's Top Global Mega Trends to 2025 and Implications to Business, Society, and Cultures*, Frost & Sullivan, 2014.

² *Trade and Cross-Border Data Flows*, OECD, 2019.

³ *FutureScape—Worldwide IT Industry 2019 Predictions*, IDC, 2018.

Connecting People to Economic Opportunities



6 billion connected consumers



25 billion connected devices

by 2025^{1,2}

¹ *The Mobile Economy 2020*, GSMA, 2020.

² *The Digitization of the World From Edge to Core*, IDC, 2018.

Benefitting All Sectors

75% of the value of data transfers accrues to traditional industries like agriculture, logistics, and manufacturing¹



For SMEs in Asia—digital tools **reduce export costs by 82%**, and **transaction times by 29%**²

¹ *Internet matters: The Net's sweeping impact on growth, jobs, and prosperity*, McKinsey Global Institute, 2011.

² *Micro-Revolution: The New Stakeholders of Trade in APAC*, Alphabet, 2019.

“ Cross-border data flows are especially important for micro, small and medium-sized enterprises (MSMEs), enabling a new breed of ‘micro multinationals’ which is ‘born global’ and is constantly connected. ... Better and faster access to critical knowledge and information also helps MSMEs overcome informational disadvantages, notably with respect to larger firms, reducing barriers to engaging in international trade and allowing them more readily to compete with larger firms.”

OECD, *Mapping Approaches to Data and Data Flows* (2020)

PRINCIPLE 2

Any rules impacting cross-border data transfers should be developed and maintained in accordance with good regulatory practices

The second pillar of an international policy consensus on data transfers involves **transparent, accountable, and evidence-driven regulatory practices**. Adhering to these practices helps ensure that any rules impacting cross-border data are well justified, enjoy the support and trust of the public, and do not unintentionally harm international commerce and innovation.

In the design, development, issuance, implementation, and review of measures that may impact cross-border data transfers, governments should:

- Be transparent;¹³
- Draw from the best reasonably available evidence relevant to the proposed cross-border data policy;¹⁴
- Analyze that evidence according to sound, objective, and verifiable methods (including regulatory impact assessments—as discussed further under Principle 4 below);
- Provide opportunity for input from the public, experts, and interested stakeholders;¹⁵ and
- Include other procedural safeguards and due process.¹⁶

A robust and thorough set of regulatory good practices to evaluate the foregoing factors can help policymakers improve the quality and effectiveness of proposed measures, and eschew unintended consequences that may be particularly pronounced when such measures unnecessarily restrict cross-border data transfers.¹⁷

“ Digital technologies and data profoundly affect international trade by reducing trade costs; facilitating the co-ordination of global value chains; diffusing ideas and technologies across borders; and connecting greater numbers of businesses and consumers globally. In particular, goods are increasingly bundled with services, and new and previously non-tradeable services are now traded across borders.”

OECD, *Digital Economy Outlook* (2020)

“ [A]pproximately half of cross-border [services] trade is enabled by digital connectivity[, which] ... has allowed developing countries and micro, small and medium-sized enterprises (MSMEs) to export through greater visibility, easier market access and less costly distribution. Developing countries ... accounted for 29.7% of services exports in 2019.

WEF, *Paths Towards Free and Trusted Data Flows* (2020)

PRINCIPLE 3

Any rules impacting cross-border data transfers should be non-discriminatory

The third pillar supporting an international policy consensus on data transfers requires a **commitment to principles of non-discrimination and national treatment in terms of the nationality of persons, products, services, or technologies**. Subject to legitimate public policy limitations, a rule impacting cross-border data transfers would raise concerns if it distorted the market or altered conditions of competition based on the national origin of the persons, the products or services, or the technologies involved. In some cases, concerns may also arise if data transfer rules are designed to provide economic advantages to transfers within a country's borders, and to domestic persons, their products or services, or their technologies, than are afforded to cross-border transfers and non-national persons, products, services, or technologies. Likewise, countries should refrain from discriminatory treatment among sectors, for example by blocking or impeding data transfers in particular sectors.

For the foregoing reasons, any rules relating to cross-border data transfers should not modify conditions of competition or serve protectionist ends by:

- Discriminating against foreign persons, products, or technologies;
- Treating data transfers into or out of the country less favorably than data transfers within the country; or
- Discriminating among different technologies.

Such measures should also not be applied in a manner that would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade. As outlined above and in many RTAs negotiated to date, principles of non-discrimination and national treatment are critical to advancing an international policy consensus on data transfers.¹⁸

“ [F]or data to flourish as an input to innovation, it benefits from flowing as freely as possible, given necessary privacy protection policies. This may, at least in part, explain why binding rules on cross-border data transfers and localization restrictions have been introduced in a number of RTAs and have been discussed [at the WTO].”

WTO, *Government Policies to Promote Innovation in the Digital Age*, 2020 World Trade Report (2020)

PRINCIPLE 4

Any rules impacting cross-border data transfers should be necessary to achieve a legitimate objective and not impose greater restrictions than necessary

The fourth pillar underlying an international policy consensus on data transfers should embody a commitment to **specifically tailor any rules that would impact cross-border data transfers to legitimate and justified policy objectives and to refrain from imposing restrictions on data transfers that are greater than necessary.**

This standard is reflected in many RTAs negotiated to date¹⁹ and in the administrative and regulatory processes adopted by many governments. As part of their administrative and regulatory practice, governments typically evaluate costs, benefits, and reasonably available alternatives as part of their assessment of whether proposed rules are necessary to achieve a specific public policy objective. Often referred to as regulatory impact assessments, these regulatory evaluations are particularly salient to data transfer restrictions, which can result in excessive economic costs and impacts. Such assessments should evaluate from a cross-border policy perspective:

- The particular public policy outcome that the proposed measure is intended to achieve;
- Whether the cross-border data restrictive features of the proposed measure are needed to achieve that outcome;
- Whether other regulatory or non-regulatory alternatives could feasibly address that need or achieve that outcome with fewer data transfer restrictions;
- The potential impacts of various alternatives over time (e.g., economic, social, environmental, public health, and safety effects) on the government, enterprises, and other persons who depend upon the ability to access technologies and transfer data across borders;
- The grounds for concluding that a particular policy alternative is preferable to others.

As a matter of international and domestic law, this type of assessment is critical to evaluate the disruptive potential of data transfer restrictions in an international commercial ecosystem. Regulatory impact assessments can help answer questions for policymakers in the process. For example, policymakers sometimes underestimate the costs of transfer restrictions, while overestimating their benefits. Policymakers also sometimes lack adequate information regarding non-regulatory solutions—e.g., evidence regarding internal controls that companies have adopted to keep data secure and private and to make it readily available in response to valid investigatory or regulatory requests. In some cases, there has been little substantiation or quantification of the risks that the measure purports to address, and little analysis of whether the proposed measure (and its most restrictive aspects) are necessary and proportionate to address any such risks.²⁰

This analysis is important because **how** data is protected is typically more salient than **where** it is stored.

As outlined above and in many RTAs negotiated to date, rules impacting cross-border data transfers should be necessary to achieve a legitimate and justified public policy objective and impose no more restrictions on data transfers than necessary.

“[C]ross-border data flows... allow companies not only to sell their goods and services, but also to coordinate their logistics and the activities of their subsidiaries and partner offices across the globe.... Indeed, the internet is now one of the most important business platforms for companies, domestically and internationally.”

WTO, *Towards a New Digital Era*, 2018 World Trade Report (2018)

Data transfers are critical to economic opportunity for all. For example:

Farmers rely on cross-border access to meteorological and market data to plant and harvest crops, and to find buyers for those crops in global markets

Workers and citizens depend upon data transfers for remote work, online education, and remote services (e.g., telemedicine)

Employers and employees rely on data transfers to collaborate in the research, design, engineering, manufacturing, marketing, and post-sale service of new products

Governments and enterprises rely on data transfers to manage risks relating to health, consumer protection, cybersecurity, anti-money laundering, and other policy priorities

GDA, *Jobs in All Sectors Depend On Data Flows* (2020); GDA, *Creating Jobs and Trust Across Borders in Every Sector* (2020)

PRINCIPLE 5

Countries should support the use of accountability models aligned with international best practices to foster responsible data transfer practices

The fifth pillar incorporates the accountability model, first established by the Organisation for Economic Co-operation and Development (OECD) and subsequently endorsed and integrated into other legal systems and privacy principles.²¹ This model provides an approach to cross-border data governance that effectively protects the individual and fosters streamlined, robust data transfers. Under legal frameworks that adopt the accountability model, organizations are required to implement procedures to ensure that data they transfer outside of the country continues to be protected, regardless of where it is stored.

Accountability models comport with a general view that the standards of protection applicable to data in the country of origin should continue to attach to the data as it is transferred across digital networks, including to data centers in other jurisdictions. When data subjects in the country of origin can be assured that the data protections they expect in the country of origin also apply in countries to which the data is subsequently transferred, it obviates one frequent claimed basis for data localization measures.

Wherever possible, countries developing rules that impact data transfers should support and rely upon international consensus-based standards, rather than advance unique, single-country standards that may be incompatible with international standards. Such an approach helps facilitate accountability by increasing alignment among countries and reducing the risks of regulatory inconsistency among countries.

“ Countries that impose local data storage and retention requirements to secure better [data] access for themselves can expect multinational businesses to stay away and other countries to retaliate. Similarly, countries that regulate data processing too rigidly and with specific restrictions on cross-border data transfers provoke reciprocal restrictions by other countries, resulting in reduced access to global data and technology, pressures for compromises in bilateral trade negotiations, and accumulating complexities. Cross-border data transfers require give and take.”

WEF, *A Roadmap for Cross-Border Data Flows* (2020)

“Data localization requirements can increase cybersecurity and other operational risks, hinder risk management and compliance, and inhibit financial regulatory and supervisory access to information. Data mobility in financial services supports economic growth and the development of innovative financial services and benefits risk management and compliance programs, including by making it easier to detect cross-border money laundering and terrorist financing patterns, defend against cyberattacks, and manage and assess risk on a global basis.”

US-Singapore Joint Statement (2020)

PRINCIPLE 6

Countries should work together to create compatible trust-based frameworks support the seamless and responsible movement of information across borders

The sixth pillar is for governments to take steps to build interoperable systems that facilitate an international consensus on data transfers.

Continuing to enjoy the transformative benefits enabled by the seamless and responsible movement of data requires a commitment to digital trust. Building digital trust requires both domestic and international action. That means domestic and international legal frameworks help economies realize the benefits of cross-border data transfers and cloud-based technology without sacrificing expectations of privacy,²² security,²³ and safety.²⁴ In the international context, this may include:

- **Cross-Border Interoperability Mechanisms:** An important complement to international regulatory convergence efforts are mechanisms that ensure that different national legal regimes are “interoperable”—i.e., compatible—with one another. In the context of personal information protection, such mechanisms may include (among other things) private codes of conduct; contractual arrangements; certifications, seals, or marks; white-listing or mutual recognition arrangements; and participation in government programs. These coordination mechanisms help bridge current gaps in international privacy norms while facilitating the safe and secure transfer of personal information.
- **International Frameworks Regarding Regulation of Data Transfers and Localization:** Another trust-building mechanism involves negotiating agreements to prohibit unnecessary data transfer restrictions and data localization mandates. Thus, these agreements reaffirm the core principle that the seamless and responsible movement of information across digital networks is foundational to a healthy, integrated global economy. These agreements also can more precisely define the relationship between rules impacting data transfers and specific policy objectives. Overall, these agreements support legal certainty, helping grow digital trust, economic development, and technological innovation.²⁵

“A study conducted on three developing regions (in South America, South-East Asia and Africa) indicates that data localization measures on IoT applications and M2M data could cut 59-68% of their productivity and revenue gains. Such losses of competitiveness also lead to reductions of \$4-5 billion in investments and 182,000-372,000 jobs...”

WEF, Paths Towards Free and Trusted Data Flows (2020)

“**Cross-border flow of data, information, ideas and knowledge generates higher productivity, greater innovation, and improved sustainable development. At the same time, we recognize that the free flow of data raises certain challenges. By continuing to address [these] challenges..., we can further facilitate data free flow and strengthen consumer and business trust.**”

[G20 Ministerial Statement on Trade and Digital Economy \(2019\)](#)

Conclusion

It is of increasing importance that like-minded countries cooperate to strengthen the pillars of an international **policy consensus** that is focused on **data transfers** and built on a **foundation of trust**. Advancing international policies on cross-border data transfers offer policymakers an effective tool to build digital trust and drive innovation, increase employment, and rebuild economies. We encourage policymakers to consider the foregoing cross-border data policy principles in their discussions in international bodies.

“**Any future WTO JSI e-commerce” agreement should discipline unnecessary or discriminatory data localization mandates and data transfer restrictions. Any agreement should also be guided by principles of transparency and interoperability among legal frameworks; should apply across all economic sectors; and should require all countries to adopt or maintain legal frameworks to protect personal information.**”

[Multi-Industry Statement on Cross-Border Data Transfers and Data Localization Disciplines in WTO Negotiations on E-Commerce, Statement by 78 Associations from Africa, Asia, Australia, Europe, and the Americas \(Jan. 26, 2021\)](#)

ENDNOTES

- ¹ The Global Data Alliance (globaldataalliance.org) 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. The Alliance supports policies that help instill trust in the digital economy while safeguarding the ability to transfer data across borders and refraining from imposing data localization requirements that restrict trade. Alliance members include BSA members and American Express, Amgen, AT&T, Citi, ITB, LEGO, Mastercard, Medtronic, Panasonic, Pfizer, RELX, Roche, UDS, United Airlines, Verizon, Visa, and WD-40 Company. These companies are headquartered across the globe and are active in the advanced manufacturing, aerospace, automotive, consumer goods, electronics, energy, financial services, health, supply chain, and telecommunications sectors, among others. BSA | The Software Alliance administers the Global Data Alliance. See Global Data Alliance, *About the Global Data Alliance* (2020), <https://www.globaldataalliance.org/downloads/aboutgda.pdf>.
- ² See Global Data Alliance, *International Negotiations on Cross-Border Data Transfers & Data Localization* (2020), <https://www.globaldataalliance.org/downloads/06022020GDAlnternationalNegotiations.pdf>.
- ³ See e.g., Global Data Alliance, *Submission to USTR on National Trade Estimate of Foreign Trade Barriers* (2020), <https://www.globaldataalliance.org/downloads/10292020GDA2020NTESubmission.pdf>.
- ⁴ Severing or limiting connections to foreign markets through such self-imposed restrictions tends to hinder economic development, reduce innovation and productivity growth, and depress export competitiveness. Matthias Bauer, Hosuk Lee-Makiyama, Erik van der Marel, et al, *The Costs of Data Localisation: Friendly Fire on Economic Recovery*, ECIPE (2014), https://ecipe.org/wp-content/uploads/2014/12/OCC32014_1.pdf; Martina F. Ferracane, Janez Kren, and Erik van der Marel, *The Costs of Data Protectionism*, VOX (2018), <https://voxeu.org/article/cost-data-protectionism>; Martina F. Ferracane and Erik van der Marel, *Do Data Policy Restrictions Impact the Productivity Performance of Firms and Industries?* ECIPE (2019), <https://ecipe.org/publications/do-data-policy-restrictions-impact-the-productivity-performance-of-firms-and-industries/>; Susan Lund and James Manyika, *Defending Digital Globalization*, McKinsey Global Institute (2017), <https://www.mckinsey.com/mgi/overview/in-the-news/defending-digital-globalization>; Anupam Chander and Uyên P. Lê, *Data Nationalism*, Emory Law Journal 64, No. 3 (2015), <https://scholarlycommons.law.emory.edu/elj/vol64/iss3/2/>.
- ⁵ See Global Data Alliance, *Position Paper on Cross-Border Data Transfers & Data Localization* (2020) <https://www.globaldataalliance.org/downloads/02112020GDACrossborderdata.pdf> (Cross-border data transfers foster online security and privacy by enabling cybersecurity tools to identify anomalies, divert potential threats, and patch vulnerabilities through global, real-time monitoring of traffic patterns and data exceptions. When governments mandate localization or restrict the ability to transfer and analyze data in real-time, they create unintended security gaps and blind spots that criminals can exploit. Cross-border data transfers also foster compliance with regulatory requirements by firms engaged in services including transportation, logistics, and financial services).
- ⁶ See Global Data Alliance, *Trends in International Negotiations regarding Cross-Border Data Transfers* (2020), <https://www.globaldataalliance.org/downloads/06022020GDAlnternationalNegotiations.pdf>.
- ⁷ See e.g., Research Institute of Economy Trade and Industry of Japan, *The Digital Economy for Economic Development: Free Flow of Data and Supporting Policies*, p. 4 (2019), at: <https://t20japan.org/wp-content/uploads/2019/03/t20-japan-tf8-4-digital-economy-economic-development.pdf>.
- ⁸ See Global Data Alliance, *Cross-Border Data Transfers Facts and Figures* (2020), <https://www.globaldataalliance.org/downloads/gdafactsandfigures.pdf>.
- ⁹ *Ibid.*
- ¹⁰ *Ibid.*
- ¹¹ With COVID-19, these trends have become even more pronounced. See Global Data Alliance, *Cross-Border Data Transfers and Remote Work* (Oct. 2020), <https://globaldataalliance.org/downloads/10052020cbdtremotework.pdf> (showing that before COVID-19, 5-15 percent of US employees worked remotely; as of mid-2020, more than 50 percent of US employees do); Global Data Alliance, *Cross-Border Data Transfers and Remote Health Services* (Sept. 2020), <https://globaldataalliance.org/downloads/09152020cbdtremotehealth.pdf> (showing that remote health services are expected to grow by 700 percent by 2025, and some regions have seen even more rapid growth—up to 40-fold—for non-urgent telemedicine visits).
- ¹² Global Data Alliance, *Dashboard—Trade Rules on Data Transfers* (2020), <https://www.globaldataalliance.org/downloads/gdadashboard.pdf>.
- ¹³ For example, governments should adopt pre-publication and final publication processes that specify implementation timelines, how various substantive concerns are addressed, the evaluation of evidence and expert input, and alternatives or other steps taken to mitigate negative impacts of the measure. See e.g., USMCA Arts. 28.9 and 28.11.
- ¹⁴ For example, governments should seek out the best reasonably obtainable information relevant to the proposed policy, be transparent regarding information sources and any significant assumptions, and use sound statistical methodologies in analyzing that information. See e.g., USMCA Art. 28.5.
- ¹⁵ For example, governments should adopt procedural safeguards to ensure that any proposed measure that would impact cross-border data transfers is well-informed through input from experts, interested stakeholders, and the public. Such safeguards include:
 - Advance publication, including an explanation of the measure's underlying objectives, the statutory or other legal basis underlying those objectives, and how the measure would achieve those objectives in light of available evidence;
 - Opportunities for public comment; and
 - Use of expert advisory groups, public-private consultative mechanisms, evaluation of best practices, and other means of protecting the public interest in thoughtful, deliberative policymaking.See e.g., USMCA Arts. 28.7, 28.9, and 28.10.
- ¹⁶ For example, governments should offer a retrospective review mechanism that allows for future enhancements or revisions of the measure, including from the perspective of cross-border data policy. The mechanism should permit the government to evaluate:
 - How effective the measure has proven in achieving stated objectives;
 - Whether changed circumstances or new information would justify a review of some aspects of the measure; and
 - Whether there are any new opportunities to eliminate unnecessary regulatory burdensSee e.g., USMCA Art. 28.13.
- ¹⁷ Commentary on good regulatory practices in relation to cross-border data policy includes: OECD, *Principles for Market Openness in the Digital Age*, Working Party Report, TAD/TC/WP(2018)17/FINAL (2018), [https://ab46bb92-a539-4d61-9a28-f77eb5f41c00.usfiles.com/ugd/ab46bb_830a70b4f8dc4508a38d3e480ffa9cb2.pdf](http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP(2018)17/FINAL&docLanguage=En; Joshua Meltzer, How APEC can address restrictions on cross-border data flows (2021), <a href=); OECD, *Trade in the Digital Era* (2019), <http://www.oecd.org/going-digital/trade-in-the-digital-era.pdf>; World Economic Forum, *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows*, White Paper (2020), p. 18 https://www.imfrri.gr.jp/content/files/Open/Related%20Information%20/WEF_May2020.pdf (“[P]olicy-makers should ensure that domestic measures affecting data are enacted in a transparent manner that allows opportunities for broad stakeholder input; are evidence-based and consider the technical and economic feasibility of requirements; require the publication of impact assessments to ensure the appropriateness and effectiveness of regulatory approaches; and are targeted and proportionate, and restrict trade as little as possible.”); UNCTAD, *Data protection regulations and international data flows: Implications for trade and development* (2016), at: https://unctad.org/system/files/official-document/dtstict2016d1_summary_en.pdf (recommending that the impact on smaller businesses be assessed with respect to proposed data protection legislation and data flow restrictions); Indian Council for Research on International Economic Relations, *Regulatory Burden on Micro, Small and Medium Businesses Due to Data Localisation Policies*, (Sept. 2019), at <http://icrier.org/pdf/Regulatory-Burden.pdf>; OECD, *Going Digital: Shaping Policies, Improving Lives* (2019), Molinuevo & Saez, *Regulatory Impact Assessment Toolkit*, The World Bank (2014), at: <https://openknowledge.worldbank.org/bitstream/handle/10986/17255/9781464800573.pdf?sequence=1>; ICTSD, *Advancing Sustainable Development Through Services Regulation* (2017).
- ¹⁸ Global Data Alliance, *Dashboard—Trade Rules on Data Transfers* (2020), <https://www.globaldataalliance.org/downloads/gdadashboard.pdf>.

- ¹⁹ Global Data Alliance, *Dashboard—Trade Rules on Data Transfers* (2020), <https://www.globaldataalliance.org/downloads/gdadashboard.pdf>.
- ²⁰ See e.g., OECD, *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, Art. 12 (2013), https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (“Any restrictions to transborder flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing.”)
- ²¹ See OECD, *Guidelines governing the protection of privacy and transborder flows of personal data*, Arts. 14-18 (2013), http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.
- ²² Ensuring continued benefits from cross-border data transfers depends on users’ faith that their information will not be used or disclosed in unexpected ways. At the same time, to maximize the benefit of cloud-based technologies, providers must be free to move data across borders in an efficient and commercially viable manner.
- ²³ Users must be assured that governments and enterprises understand and properly manage the risks inherent in storing and running applications in the cloud. This requires implementing cutting-edge cybersecurity solutions without being required to use specific technologies.
- ²⁴ Laws online must provide meaningful deterrence and clear causes of action to deal with online threats and cybercrime. Legal systems should provide an effective mechanism for law enforcement, and for cloud providers themselves, to combat unauthorized access to data stored in the cloud.
- ²⁵ To date, many countries have made, or are negotiating, such commitments under international agreements, including under the United States-Mexico-Canada Agreement (USMCA), the US-Japan Digital Trade Agreement, the Comprehensive and Progressive Trans-Pacific Partnership Agreement (CPTPP), the Digital Economy Partnership Agreement (DEPA), the Australia-Singapore Digital Economy Agreement (DEA), the UK-Japan Comprehensive Economic Partnership Agreement, the US-Japan Digital Trade Agreement, and the WTO Joint Statement Initiative digital trade negotiations. This positive trend should continue.

EXHIBIT 15



GLOBAL DATA ALLIANCE

TRUST ACROSS BORDERS

CROSS-BORDER DATA TRANSFERS & DATA LOCALIZATION

The Global Data Alliance is a cross-industry coalition of companies, with headquarters in different regions of the world, that are committed to high standards of data privacy and security. Alliance companies rely on the ability to transfer data responsibly around the world to create jobs and make local industries more competitive. Cross-border data transfers power innovation and growth across the globe and all sectors of the economy—from manufacturing and farming to local start-ups and service providers.

Cross-border data transfers also enable the deployment of tools that facilitate teleworking, virtual collaboration, online training, and the remote delivery of services, including virtual healthcare solutions. These tools—which include cloud-based libraries and databases, video-conferencing applications, and interactive collaboration platforms—help foster cross-office R&D and innovation; build workforce productivity and skills; contain costs and carbon emissions; and promote public health and safety.

Data transfers enable the digital tools and insights that are critical to enabling entrepreneurs and companies of all sizes, in every country, to create new kinds of jobs, boost efficiency, drive quality, and improve output.

The Alliance has come together to advance policies around the world that promote the responsible movement of data across borders without imposing unnecessary data localization mandates or restrictions on data transfers. Data localization requirements and restrictions on international data transfers are estimated to reduce growth by billions of dollars in countries that implement them. These measures hurt local companies by preventing them from accessing innovative technologies, which can preclude local industry from participating in global supply chains and accessing customers in foreign markets. Goods and services that use data in various phases of their lifecycles are

more competitive if they can use data from around the world. In addition, because data transfer restrictions create a significant burden on the implementing country's overall competitiveness, they also undermine the country's attractiveness as a destination for investment and R&D.

Several grounds are frequently cited as the basis for imposing data restrictions, but they are based on misconceptions, as discussed in this document. The Alliance will work to correct such misconceptions and show policymakers that they can achieve their goals without impeding the free flow of data.



CYBERSECURITY

It has been argued that data localization and data transfer restrictions are necessary to ensure cybersecurity. In fact, how data is protected is much more important to security than where it is stored. Data localization requirements and limits on data transfers often undermine data security. When governments restrict a company's ability to move data, they create unnecessary obstacles to data security. Cross-border data transfers are important for cybersecurity for several reasons. Companies may choose to store data at geographically diverse locations to obscure the location of data and reduce risk of

The Alliance has come together to advance policies around the world that promote the responsible movement of data across borders without imposing unnecessary data localization mandates or restrictions on data transfers.

The Alliance works to promote the responsible movement of data across borders without unnecessary data restrictions, while accounting for countries' legitimate policy concerns.

physical attacks, to enable companies to reduce network latency, and to maintain redundancy and resilience for critical data in the wake of physical damage to a storage location. In addition, cross-border data transfers allow for cybersecurity tools to monitor traffic patterns, identify anomalies, and divert potential threats in ways that depend on global access to real-time data. When governments mandate localization or restrict the ability to transfer and analyze data in real-time, they create unintended vulnerabilities.



PRIVACY

It has also been argued that data localization and data transfer restrictions are necessary to ensure that companies process and use data consistent with a country's data protection laws. This is not the case. In reality, organizations that transfer data globally should implement procedures to ensure that the data is protected even when transferred outside of the country. Where differences exist among data protection regimes, governments should create tools to bridge those gaps in ways that both protect privacy and facilitate global data transfers. Taking into account widely accepted privacy principles and industry best practices, governments should also aim to ensure that privacy frameworks are interoperable and allow for the seamless flow of data across borders.



LAW ENFORCEMENT

Some claim that data localization and data transfer restrictions are necessary to ensure that regulators and law enforcement authorities will have access to data relevant to conduct investigations. The location of the data, however, is not the determining factor. Responsible service providers work to respond to lawful requests for data consistent with their obligations to their customers and to protect consumer privacy. If the service provider has a conflicting legal obligation not to disclose data, law enforcement has several options: International agreements—including Mutual Legal Assistance Treaties (MLATs) or Agreements (MLAAs), multilateral treaties, and other agreements, such as those authorized by the United States Clarifying Lawful Overseas Use of Data (CLOUD) Act—can establish foundations for mutual legal assistance and reciprocal transfers of law enforcement data. Courts may also issue requests to authorities abroad for the transfer of data through letters rogatory.

These are some, but not the only, grounds upon which countries seek to impose data restrictions. The Alliance will work to promote the responsible movement of data across borders without unnecessary data restrictions, while accounting for countries' legitimate policy concerns.



GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

The Global Data Alliance is administered by

BSA | The Software Alliance 20 F Street, NW, Suite 800 Washington, DC 20001

BANGKOK • BEIJING • BRUSSELS • NEW DELHI • SÃO PAULO • SEOUL • SINGAPORE • TOKYO • WASHINGTON, DC

EXHIBIT 16

INTRODUCTION

The ability to responsibly transfer data around the globe supports cross-border economic opportunity, cross-border technological and scientific progress, and cross-border digital transformation and inclusion, among other public policy objectives. To assess where policies have helped create an enabling environment for cross-border data and its associated benefits, the [Global Data Alliance](#)¹ has developed the **Cross-Border Data Policy Index**.

The *Cross-Border Data Policy Index* offers a quantitative and qualitative assessment of the relative openness or restrictiveness of cross-border data policies across nearly 100 economies. Global economies are classified into four levels. At Level 1 are economies that impose relatively fewer limits on the cross-border access to knowledge, information, digital tools, and economic opportunity for their citizens and legal persons. Many of these economies have also taken proactive steps to create a conducive environment for digital transformation.

Economies' restrictiveness scores increase as they are found to impose greater limits on cross-border data, thereby eroding opportunities for digital transformation while also impeding other policy objectives relating to health, safety, security, and the environment. The Index does not examine the underlying motivations for such restrictions, whether they are focused on domestic economic protectionism, digital authoritarianism, or other motivators.

CROSS-BORDER DATA POLICY BENEFITS AND COSTS

BENEFITS OF CROSS-BORDER DATA

↑ 145% increase
in exports with every
0.1 point reduction in
digital restrictions²

↓ 82% reduction
in MSME
export costs³

↓ Up to 30% reduction
in developing country
trade costs⁴

COSTS OF CROSS-BORDER DATA RESTRICTIONS

↓ GDP losses
of 0.7%–1.7%⁵

↓ Investment losses
up to 4%⁶

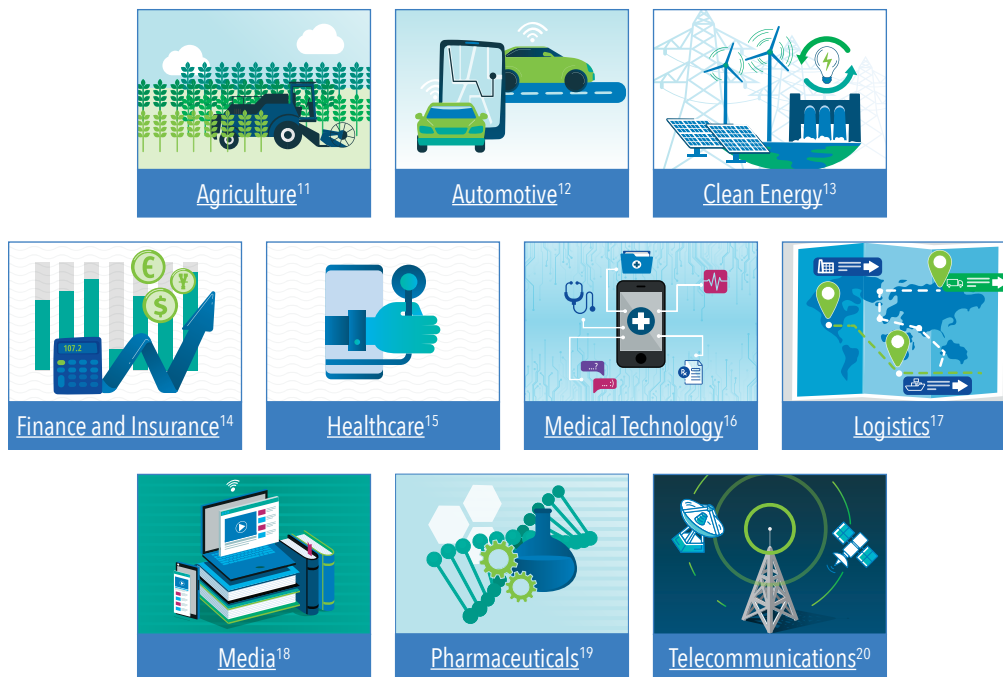
The World Bank: "Restrictions on data flows have large negative consequences on the productivity of local companies using digital technologies and especially on trade in services. Studies show that countries would gain on average about 4.5 percent in productivity if they removed their restrictive data policies, whereas the benefits of reducing data restrictions on trade in services would on average be about 5 percent."⁷

As governments increasingly declare data transfers to be illegal on vague or previously unknown grounds, citizens and enterprises lose confidence that they will be able to access data for their educational, health, safety, security, or work-related needs.

CROSS-BORDER DATA AND ECONOMIC POLICY

Cross-border data is an effective vehicle to promote [sustainable economic development](#), raise living standards, and promote [digital transformation](#), especially for smaller economies. Cross-border data is also important for [micro-, small-, and medium-sized enterprises](#) (MSMEs) that benefit disproportionately from cross-border market opportunities yet lack the resources of larger entities to navigate diverse data barriers in different markets.⁸

Cross-border data is necessary to digital transformation at [every stage of the value chain](#)⁹ across [every sector](#),¹⁰ including the following:



For more detail, please see the Global Data Alliance [Sectors Page](#).²¹

CROSS-BORDER DATA AND OTHER PUBLIC POLICY OBJECTIVES

Data transfers are important to many [governmental policy objectives](#): Not only do restrictive cross-border policies fail to protect [privacy and personal data](#),²² but they also hurt [developing countries](#)²³ and [small businesses](#);²⁴ impede [financial equity and inclusion](#);²⁵ undermine data security and [cybersecurity](#);²⁶ threaten [human rights](#);²⁷ slow science and [innovation](#);²⁸ and impair various [health and safety](#),²⁹ [environmental](#),³⁰ and other [regulatory compliance](#) priorities.³¹ For more detail, please see the Global Data Alliance [Issues Page](#).³²

Level 2–4 economies are characterized by a cross-border policy environment that is increasingly restrictive and decreasingly likely to benefit from cross-border digital transformation, cross-border scientific exchange, and cross-border economic opportunity.

Level 1 economies have cultivated policy environments allowing for the cross-border sharing of information, thus positioning their populations to enjoy the educational, economic, health, safety, and security benefits of cross-border data.

RANKINGS

The following economies have proposed or adopted policies with a relatively high degree of cross-border data restrictiveness and a low degree of openness to cross-border digital transformation, inclusion, and opportunity:

LEVEL 4: Extremely Restrictive

China	Russia
-------	--------

LEVEL 3: Highly Restrictive

India	Saudi Arabia
Indonesia	Turkey
Kazakhstan	Vietnam

LEVEL 2: Restrictive

Bangladesh	South Africa
European Union and its Member States	South Korea
Nigeria	United Arab Emirates
Senegal	

Increasing cross-border data restrictiveness can undermine an economy's digital adaptability and resilience.

CROSS-BORDER DATA AND PROMOTING EDUCATION, HEALTH, INNOVATION, SAFETY, SECURITY, AND THE ENVIRONMENT

Cross-border data supports diverse governmental policy objectives:



Cybersecurity, including through an enhanced ability to detect and respond to cybersecurity threats via real-time cross-border data visibility and risk management.



Digital Transformation of governmental and non-governmental services (e.g., education, health, and safety) through the adaptation of digital technologies across the economy.



Economic Development, including through greater digital connectivity, including for the benefit of MSMEs and underrepresented segments of the population.



Education, by enabling educators and learners to maintain access to research, scholarship, textbooks, and other learning tools from across the world.



Environmental Sustainability, including through improved cross-border carbon emissions tracking and predictive climate modeling based on multi-regional data.



Financial Inclusion, as well as fraud prevention, anti-money laundering, anti-corruption, and other financial transparency objectives.



Health, including through international R&D, cross-border healthcare regulatory collaboration, and global medical humanitarian assistance and healthcare delivery.



Human Rights, by permitting all citizens cross-border access to information without undue interference from authoritarian regimes.



Privacy, including by protecting personal data across digital networks, and by promoting interoperability among personal data protection frameworks in different jurisdictions.



Science and Technology, including through cross-border access to knowledge and research needed to meet global challenges, and to develop IP.



Trustworthy Artificial Intelligence, including through cross-border data analytics—responsibly deployed to mitigate the potential for bias in high-risk applications—to help address shared global challenges.

CROSS-BORDER DATA RESTRICTIONS ARE GROWING

↑ 600% growth
in restrictions³³

↑ 5x higher
cross-border digital restrictiveness
in 2022 than in 2021³⁴

LEVEL 1: Relatively Open Digital Policies

Open to Cross-Border Digital Economic Opportunity and Digital Transformation

Level 1: 45 Economies

The 45 Level 1 economies include Argentina, Australia, Brazil, Canada, Chile, Japan, Mexico, Peru, New Zealand, Norway, Singapore, Switzerland, Taiwan, the UK and the US, among others. Many Level 1 economies have maintained open cross-border digital policy environments and have adopted optimal policies regarding future digital transformation and digital inclusion. This may include policies that:

- Allow cross-border data to play an integral role in research and development (R&D) activities;
- Promote the use of cross-border data for health and safety regulatory processes;
- Ensure that innovators can transfer data to protect their intellectual property (IP);
- Enable educators and learners to maintain access to knowledge from around the world;
- Respect human rights and access to information without digitally authoritarian rules; and
- Promote the adoption of services to benefit small-scale farmers and small businesses through improved access to cross-border market information and opportunities from abroad.

Many Level 1 economies recognize that cross-border data can help promote the dissemination of knowledge in a manner conducive to social and economic welfare. Many of these economies have also entered into international agreements containing binding commitments not to impose discriminatory or unnecessary restrictions on data transfers vis-à-vis their trading partners.

“[D]omestic measures that may impact the international movement of data should be:

- Developed in a transparent and accountable manner;**
 - Non-discriminatory;**
 - Necessary to achieve a legitimate objective;**
 - Consistent with relevant international standards; and**
 - Interoperable with other countries’ legal frameworks.”³⁵**
-

United Nations: “[R]egulatory fragmentation in the digital landscape...is most likely to adversely impact low-income countries, less well-off individuals, and marginalized communities the world over, as well as worsen structural discrimination against women. A future of exclusionary digital development must be avoided at all costs.”³⁶

LEVEL 2: Restrictive

Decreasing Cross-Border Digital Openness Impedes the Potential of Cross-Border Data to Support Economic and Other Policy Objectives

Level 2: 33 Economies

The 33 Level 2 economies are Bangladesh, Nigeria, Senegal, South Africa, South Korea, and the United Arab Emirates, along with the 27 Member States of the European Union. Beneficially, many of these economies have assumed a forward-leaning policy stance on digital policy. Regrettably, this policy stance has often also included an embrace of unnecessary cross-border digital restrictions.

For example, between mid-2020 and mid-2023, the EU’s cross-border data restrictiveness score increased sixfold with the successive introduction of proposals to limit the cross-border movement of information across new and expanded data types, sectors, and functionalities—frequently in the name of ‘digital sovereignty.’ Previously, the EU’s score had remained relatively stable at 2.0 points from the first half of 2018 (when GDPR went into effect) until the latter half of 2020 (when more expansive proposed restrictions premised on ‘digital sovereignty’ began to emerge).³⁷

Cross-border data restrictions often:

- Are not necessary to achieve—and may even undermine—the stated purpose of the privacy, cybersecurity, or other digital policy measure into which they are embedded;
- Are adopted with little consideration of economic costs or other collateral policy impacts; and
- Contain elements that discriminate against non-national persons, technologies, products, or services.

These cross-border digital barriers can result in a policy environment that is relatively closed, resulting in suboptimal cross-border access to knowledge and digital tools. This policy environment also creates business uncertainty regarding the ability to engage in commercial activities critical to international investment, trade, R&D, and advanced manufacturing and services.³⁸

CROSS-BORDER DATA BARRIERS OFTEN:

1

Depart from the stated purpose of the measures into which they are embedded.

2

Are developed without full consideration of their collateral impacts.

3

Overstate their purported benefits.

4

Discriminate against non-national persons, technologies, products, or services.

5

Impede opportunities for cross-border digital transformation, innovation, and sustainable economic development.

LEVEL 3: Highly Restrictive

Numerous and Diverse Restrictions Substantially Impede Cross-Border Digital Transformation, Sustainable Economic Development, and Other Policy Priorities Across Multiple Sectors

Level 3: Six Economies

The six Level 3 economies are India, Indonesia, Kazakhstan, Saudi Arabia, Turkey, and Vietnam. Economies in this group have adopted cross-border data barriers characteristic of Level 2 economies, but they have done so with greater frequency and intensity.

First, from a quantitative perspective, the potential for digital transformation and digital inclusion may be severely limited by multiple cross-border data barriers that impede access to digital tools and technologies needed by local enterprises, educational institutions, and other entities. Second, in terms of their qualitative diversity, such digital barriers may be adopted across numerous governmental ministries, including authorities with jurisdiction over information and communication technologies, personal data protection, cybersecurity, national security, healthcare, financial services, intellectual property, international trade and customs, and foreign investment matters.

LEVEL 4: Extremely Restrictive

Comprehensive and Systemic Cross-Border Data Restrictions Across the Economy and Society

Level 4: Two Economies

The two Level 4 economies are China and Russia. Cross-border data barriers in Level 4 economies are more numerous and more onerous than anywhere else. These barriers typically cover more sectors and more data types, may include ad hoc pre-transfer governmental approval requirements, and depend upon often unfettered governmental discretion to enforce vague legal standards under the threat of onerous penalties. These barriers are sometimes explicitly predicated on national security and authoritarian maintenance over "social order." They frequently contain few, if any, due process safeguards against intrusive governmental decisions on data access or data transfer. In these contexts, it can be difficult for enterprises to predict their own legal exposure or have confidence that future data transfers of business-related information will be permitted.

UNCTAD: "Divergent data nationalism...reduces market opportunities for domestic MSMEs to reach worldwide markets, [and]...reduces opportunities for digital innovation, including various missed opportunities for inclusive development that can be facilitated by engaging in data-sharing through strong international cooperation....[M]ost small, developing economies will lose opportunities for raising their digital competitiveness."³⁹

APPENDIX: METHODOLOGY AND RANKINGS

What Does the Index Measure?

The *Cross-Border Data Policy Index* assesses, across several text-based metrics, each economy's national laws, regulations, and other measures that either restrict data transfers or mandate data localization.⁴⁰ The Index is built on legal analyses of measures relating to artificial intelligence, cybersecurity, privacy, law enforcement access, and international trade (among other topics).

Each measure that contains a localization requirement or a cross-border data restriction is assessed. These measures may include:

1. Policies that expressly require data to stay in-country;
2. Policies that impose unreasonable conditions on transferring data abroad;
3. Policies that prohibit the transfer of data abroad;
4. Policies that require the use of domestic data centers or other equipment;
5. Policies that require data centers to be owned or operated by nationals;
6. Policies that prohibit the application of non-national laws to digital infrastructure or data; and
7. Policies that impose import or export duties or other restraints on data transfers as they traverse digital networks.

The cross-border digital barriers embedded within these policy measures are quantitatively and qualitatively assessed. The quantitative analysis calculates the number of policy barriers adopted or proposed in jurisdiction. The qualitative assessment covers factors such as the types of data involved (e.g., personal, non-personal, sectoral, or other) and the intensity and degree of the restriction (e.g., the scope of permissible exceptions from the restriction).

Each measure is assigned a numerical weight based on the answers to the following questions:

1. Is the measure proposed or in effect?
2. Does the measure have a narrow scope (e.g., sector-specific) or a broad scope (e.g., cross-sectoral)?
3. Does the measures focus on personal data?
4. Does the measure extend to non-personal data?
5. Does the measure prohibit data transfers even if the data subject has consented?
6. Does the measure fail to make available a range of data transfer mechanisms (including standard contracts or binding corporate rules), such as requiring pre-transfer ad hoc approval from governmental authorities?
7. Does the measure preclude data mirroring (i.e., by requiring all copies of data to reside exclusively on localized infrastructure)?
8. Has the economy in question made meaningful binding international commitments (e.g., in trade agreements) not to unnecessarily restrict data transfers and not to impose data localization requirements?

Each economy's relative cross-border data openness or restrictiveness ranking is determined by totaling the sum of the numerical weights calculated for each measure at one-half point (0.5) increments. Economy rankings range from zero to 50 points, representing 101 distinct potential values from 0, 0.5, 1.0, 1.5 through 49.5 and 50.0. The higher an economy's score, the more restrictive its cross-border data policy environment. For example, the economy with the highest restrictiveness score is the People's Republic of China, at 46 points. The cross-border data restrictiveness score for India is 25.5; Indonesia is 19; Vietnam is 16.5; and the EU is 13.5. Finally, the economies are grouped into four major categories based on this analysis. Please see the full listing on page 13.

Legal rules that impede transfers of broad categories of data—such as “non-personal data” or “important data”—undermine digital transformation and trust.

Examples include China's Data Transfer Security Assessment requirements, the EU's Data Act proposal and EUCS proposal, and India's former Non-Personal Data Governance Framework.

Comparison with Other International Digital Indices

The Global Data Alliance's *Cross-Border Data Policy Index* builds upon the international digital policy indices identified below:

- BSA *Global Cloud Computing Scorecard*;⁴¹
- ECIPE *Report on Restrictions on Cross-Border Data Flows*;⁴²
- ITIF *Report on Barriers to Cross-Border Data Flows*;⁴³
- OECD *Digital Services Trade Restrictiveness Index (DSTRI)*;⁴⁴
- OECD *Services Trade Restrictiveness Index (STRI)*;⁴⁵
- Salesforce *Data Beyond Borders 3.0 Report*;⁴⁶
- Tufts University *Digital Intelligence Index*;⁴⁷ and
- UK *Report on the Extent and Impact of Data Localisation*;⁴⁸

Many of these indices offer a country-level analysis of various econometric contributors to cross-border digital transformation, cloud readiness, and digital trade, as well as cross-border digital restrictiveness. These indices typically measure a basket of economic and policy indicators. For example, the OECD DSTRI analyzes economy-level metrics relating to infrastructure and connectivity, intellectual property (IP) rights, electronic transactions, e-payment systems, and other barriers. Similarly, the BSA *Global Cloud Computing Scorecard* analyzes economy-level

metrics relating to data privacy, security, cybercrime, IP rights, support for international standards, digital trade, IT readiness, and broadband deployment.

In contrast, the GDA *Cross-Border Data Policy Index* is focused exclusively on the legal measures that mandate data localization, restrict data transfers, or otherwise limit cross-border data. The GDA Index is developed through a textual analysis of these legal measures, including an assessment of their legal drafting and operation, and their likely breadth and depth of impact.

The GDA Index also seeks to generate a real-time, predictive snapshot of each jurisdiction's dynamic evolution toward relatively greater or lesser cross-border data restrictiveness. It does so by assessing not only cross-border data rules that are in effect, but also cross-border data proposals that are in development. Many economies offer a relatively stable and predictable cross-border data policy environment. However, this is not true for all.

Notwithstanding these differences in methodologies, there is broad consensus in findings across various indices. China consistently is found to have the most cross-border data and other digital restrictions. India, Indonesia, Russia, and Vietnam (among others) are also consistently found to reflect a high degree of restrictiveness. Recent rankings also note the increasing cross-border restrictiveness of the European Union.

G7 HIROSHIMA LEADERS' COMMUNIQUÉ (2023)⁴⁹

- ✓ We reaffirm that cross-border data flows, information, ideas and knowledge generate higher productivity, greater innovation, and improved sustainable development, while raising [other] challenges.
- ✓ We welcome the OECD Declaration on [Trusted] Government Access to Personal Data...as an instrument to increase trust in cross-border data flows among countries committed to democratic values and the rule of law.
- ✓ We emphasize our opposition to internet fragmentation and the use of digital technologies to infringe on human rights.
- ✓ We should counter unjustified obstacles to the free flow of data, lacking transparency, and arbitrarily operated.
- ✓ We seek to increase trust across our digital ecosystem and to counter the influence of authoritarian approaches.

LEVEL 1

Relatively Open: Economies with a numerical score between 0 and 5.5 (45 economies)

- Algeria
- Angola
- Argentina
- Australia
- Bolivia
- Botswana
- Brazil
- Burkina Faso
- Canada
- Chad
- Chile
- Colombia
- Congo
- Costa Rica
- Ecuador
- Gabon
- Ghana
- Iceland
- Israel
- Japan
- Kenya
- Lichtenstein
- Madagascar
- Malaysia
- Mauritania
- Mexico
- Morocco
- Namibia
- Niger
- Norway
- Paraguay
- Peru
- Philippines
- Singapore
- Sri Lanka
- Switzerland
- Taiwan
- Tanzania
- Thailand
- Tunisia
- Uganda
- Ukraine
- Uruguay
- United Kingdom
- United States

LEVEL 2

Restrictive: Economies with a numerical score between 6 and 15.5 (8 entries comprising 33 economies, including the 27 EU Member States)

- Bangladesh
- European Union member (Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece,
- Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, and Sweden)
- Nigeria
- Senegal
- South Africa
- South Korea
- United Arab Emirates

LEVEL 3

Highly Restrictive: Economies with a numerical score between 16 and 25.5 (6 economies)

- India
- Indonesia
- Kazakhstan
- Saudi Arabia
- Turkey
- Vietnam

LEVEL 4

Extremely Restrictive: Economies with a numerical score between 26 and 50 (2 economies)

- China
- Russia

World Economic Forum: "Countries that impose local data storage and retention requirements to secure better [data] access for themselves can expect multinational businesses to stay away and other countries to retaliate. Similarly, countries that regulate data processing too rigidly and with specific restrictions on cross-border data transfers provoke reciprocal restrictions by other countries, resulting in reduced access to global data and technology, pressures for compromises in bilateral trade negotiations, and accumulating complexities. Cross-border data transfers require give and take."⁵⁰

Endnotes

- 1 The Global Data Alliance (GDA) represents companies that are committed to high standards of data responsibility, privacy, and security, and that rely on the ability to transfer data around the world to innovate and create jobs. The GDA works to advance policies that promote the responsible handling of data without imposing unnecessary data localization mandates or restrictions on data transfers. The GDA produces draft treaty and legal texts, regulatory analysis, and sector- and issue-focused studies on cross-border data and digital trust. For more information, please visit the GDA website at www.globaldataalliance.org.
- 2 A 0.1-point reduction in a country's level of digital services trade restrictiveness is associated with a 145% increase in overall exports. The effect is highest for digitally deliverable services (277%), "other services" exports (206%), agriculture and food exports (176%), and manufacturing exports (117%). Javier López González, Silvia Sorescu, and Pinar Kaynak, *Of Bytes and Trade: Quantifying the Impact of Digitalisation on Trade*, OECD (2023), <https://read.oecd.org/10.1787/11889f2a-en?format=pdf>.
- 3 For MSMEs in Asia, digital tools reduce export costs by 82%, and transaction times by 29%. Alphabeta, *Micro-Revolution: The New Stakeholders of Trade in APAC* (2018), <https://accesspartnership.com/new-stakeholders-trade-apac/>.
- 4 Trade costs fall as data transfer restrictions are removed, including for Thailand (-30%), India (-28%), and Indonesia (-26%). OECD, *OECD Services Trade Restrictiveness Index: Policy Trends up to 2023* (2023), https://issuu.com/oecd-publishing/docs/stri_policy_trends_up_to_2023_final. Furthermore, non-OECD economies' relative share of digital trade increased by 50% from 1995 to 2018. See Javier López González, Silvia Sorescu, and Pinar Kaynak, *Of Bytes and Trade: Quantifying the Impact of Digitalisation on Trade*, OECD (2023), <https://read.oecd.org/10.1787/11889f2a-en?format=pdf>.
- 5 Forced data localization has been estimated to reduce GDP by 0.7%–1.7%, particularly as such measures reduce trade, slow productivity, and increase prices for affected industries. See APEC, *Economic Impact of Adopting Digital Trade Rules* (2023), <https://www.apec.org/publications/2023/04/economic-impact-of-adopting-digital-trade-rules-evidence-from-apec-member-economies>.
- 6 Ibid. Data localization has been associated with investment decreases of up to 4% because such restrictions reduce the attractiveness and competitiveness of an economy.
- 7 World Bank, *World Development Report* (2020), <https://www.worldbank.org/en/publication/wdr2020>.
- 8 Global Data Alliance, *Cross-Border Data Transfers & Sustainable Economic Development* (2023), <https://globaldataalliance.org/issues/economic-development/>; USAID Digital Strategy, 2020–2024, <https://www.usaid.gov/usaaid-digital-strategy>, p. 37. As the US Agency for International Development has explained, "[d]igital ecosystems have the potential to equip informal merchants, women entrepreneurs, smallholder farmers, and MSMEs engaged in cross-border trade with access to markets, information, and finance. These diverse users require trustworthy services that reflect their needs... [D]igital trade that spans borders depends on free data flows, digitized customs, and innovations in trade finance made possible by new approaches to lending."
- 9 Global Data Alliance, *Jobs in All Sectors Depend Upon Data Flows* (2020), <https://globaldataalliance.org/wp-content/uploads/2021/07/infographicgda.pdf>.
- 10 Global Data Alliance, *The Cross-Border Movement of Data: Creating Jobs and Trust Across Borders in Every Sector* (2020), <https://globaldataalliance.org/wp-content/uploads/2021/07/GDAeverysector.pdf>.
- 11 Global Data Alliance, *Agriculture* (2022), <https://globaldataalliance.org/sectors/agriculture/>.
- 12 Global Data Alliance, *Automotive* (2022), <https://globaldataalliance.org/sectors/automotive/>.
- 13 Global Data Alliance, *Energy* (2022), <https://globaldataalliance.org/sectors/energy/>.
- 14 Global Data Alliance, *Finance* (2022), <https://globaldataalliance.org/sectors/finance/>.
- 15 Global Data Alliance, *Healthcare* (2022), <https://globaldataalliance.org/sectors/healthcare/>.
- 16 Global Data Alliance, *Medical Technology* (2023), <https://globaldataalliance.org/sectors/medical-technology/>.
- 17 Global Data Alliance, *Supply Chain Logistics* (2022), <https://globaldataalliance.org/sectors/supply-chain-logistics/>.
- 18 Global Data Alliance, *Media and Publishing* (2022), <https://globaldataalliance.org/sectors/media-publishing/>.
- 19 Global Data Alliance, *Biopharmaceutical R&D* (2022), <https://globaldataalliance.org/sectors/biopharmaceutical-rd/>.
- 20 Global Data Alliance, *Telecommunications* (2022), <https://globaldataalliance.org/sectors/telecommunications/>.
- 21 Global Data Alliance, *Sectors* (2023), <https://globaldataalliance.org/sectors/>.
- 22 Global Data Alliance, *Cross-Border Data Transfers & Privacy* (2023), <https://globaldataalliance.org/issues/privacy/>.
- 23 Global Data Alliance, *Cross-Border Data Transfers & Economic Development* (2023), <https://globaldataalliance.org/issues/economic-development/>.
- 24 Global Data Alliance, *Cross-Border Data Transfers & Small Businesses* (2023), <https://globaldataalliance.org/issues/small-businesses/>.
- 25 Global Data Alliance, *Finance* (2020), <https://globaldataalliance.org/sectors/finance/>.
- 26 Global Data Alliance, *Cross-Border Data Transfers & Cybersecurity* (2023), <https://globaldataalliance.org/issues/cybersecurity/>.
- 27 Freedom House, *Countering an Authoritarian Overhaul of the Internet* (2022), <https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet>. Freedom House explains the nexus between data transfer restrictions and human rights abuse as follows: "In at least 23 countries covered by Freedom the Net, laws that limit where and how personal data can flow were proposed or passed during the coverage period... The transfer of data across jurisdictions is central to the functioning of the global internet and benefits ordinary users, including by improving internet speeds, enabling companies to provide critical services worldwide, and allowing the storage of records in the most secure data centers available... [S]ome [countries] have buried problematic obligations that either mandate domestic data storage, feature blanket exceptions for national security or state actors without safeguards, or delegate increased decision-making power to politicized regulators—all of which renders users vulnerable to government abuse despite improvements pertaining to the use of personal data for commercial purposes. Such contradictory "data washing" measures ultimately fail to strengthen privacy and further fragment the internet..."
- 28 Global Data Alliance, *Cross-Border Data Transfers & Innovation* (2023), <https://globaldataalliance.org/issues/innovation/>.
- 29 Global Data Alliance, *Biopharmaceutical R&D* (2022), <https://globaldataalliance.org/sectors/biopharmaceutical-rd/>; Global Data Alliance, *Medical Technology* (2023), <https://globaldataalliance.org/sectors/medical-technology/>; Global Data Alliance, *Healthcare* (2022), <https://globaldataalliance.org/sectors/healthcare/>.
- 30 Global Data Alliance, *Cross-Border Data Transfers & Environmental Sustainability* (2023), <https://globaldataalliance.org/issues/environmental-sustainability/>.
- 31 Global Data Alliance, *Cross-Border Data Transfers & Regulatory Compliance* (2023), <https://globaldataalliance.org/issues/regulatory-compliance/>.
- 32 Global Data Alliance, *Issues* (2023), <https://globaldataalliance.org/issues/>.
- 33 From 2013 to 2019, data flow regulations across several APAC economies increased by 600%. See Joshua Meltzer, "The Rush to Regulate Data in the Indo-Pacific," in ed. Filippo Fasulo, *The EU Indo-Pacific Bid: Sailing Through Economic and Security Competition* (2023), <https://www.ispionline.it/wp-content/uploads/2023/05/ISPI-Report2023-EUs-Indo-Pacific-Bid-web.pdf>.
- 34 The average cumulative increase in cross-border services trade restrictiveness was five times higher in 2022 than in the year before. OECD, *OECD Services Trade Restrictiveness Index: Policy Trends up to 2023* (2023), https://issuu.com/oecd-publishing/docs/stri_policy_trends_up_to_2023_final. These cross-cutting trends are illustrated well by recent developments in the Asia-Pacific region.

- On the positive side, a recent APEC report indicated that, “APEC intra-regional digital trade and associated activity supported more than 60 million jobs in the APEC region. Intra-regional digital trade contributed USD 2.1 trillion to APEC economies, with \$690 billion from the direct effects of goods/services production; \$790 billion from the indirect effects; and \$650 billion from consumption-induced effects from workers that increased spending as incomes rose. Digitally deliverable services comprised 33% of intra-regional digital trade, while digitally ordered goods and services (e.g., cross-border e-commerce) comprised 67%.” APEC, *Economic Impact of Adopting Digital Trade Rules* (2023), <https://www.apec.org/publications/2023/04/economic-impact-of-adopting-digital-trade-rules-evidence-from-apec-member-economies>. Furthermore, many digital trade agreements among APEC economies—especially, Australia, Canada, Japan, Mexico, Singapore, and the US—contain digital trade provisions. Specific digital trade provisions increased the flows of digitally ordered and digitally deliverable trade by between 11% and 44%. The four most common digital trade provisions in APEC trading partner agreements are (1) prohibition of data localization, found in 66% of agreements; (2) cross-border information transfer, 76%; (3) non-imposition of customs duties on electronic transmissions, 100%; and (4) market access and national treatment for ICT service, 100%. APEC, *Economic Impact of Adopting Digital Trade Rules*. Another report indicates that from 2013 to 2019, “data flow regulations [across several APEC economies] increased [by]...600%. Privacy is by far the main reason for data flow restrictions, accounting for over 34% of regulation. Financial regulation is the second most salient reason for restricting data flows, accounting for 24%, followed closely by internet access and control at 23%, then security at 17% and competition at 2%.” Joshua Meltzer, “The Rush to Regulate Data in the Indo-Pacific,” in ed. Filippo Fasulo, *The EU Indo-Pacific Bid: Sailing Through Economic and Security Competition* (2023), <https://www.ispionline.it/wp-content/uploads/2023/05/ISPI-Report2023-EUs-Indo-Pacific-Bid-web.pdf>.
- ³⁵ Global Industry Statement on an Institutional Arrangement for Partnership on Data Free Flow with Trust (April 2023), <https://globaldataalliance.org/wp-content/uploads/2023/04/04182023g7dfttindustry.pdf>.
- ³⁶ UN High Level Advisory Board on Effective Multilateralism, Effective and Inclusive Global Governance for Today and the Future (April 2023), <https://highleveladvisoryboard.org/breakthrough/>.
- ³⁷ For example, since the latter half of 2020, the EU has experienced a sharp increase in cross-border data restrictiveness based in part on proposals to limit the cross-border movement of information across new and expanded data types, sectors, and functionalities. These include the [EU Data Act](#) proposal (introduced in Feb. 2022), the proposal for a [European Health Data Space](#) (introduced in May 2022), the [EU Cybersecurity Certification Scheme for Cloud Services](#) (introduced in Dec. 2020), and the [EU Data Governance Act](#) (introduced Nov. 2020 and promulgated in June 2022). The EU and its Member States have also experienced the imposition of unprecedented new cross-border data restrictions through judicial and administrative bodies (e.g., the CJEU’s [Schrems II decision](#) of July 2020 and over a dozen DPA opinions on cross-border data restrictions in Austria, Denmark, Finland, France, Germany, Italy, Netherlands, Spain, Sweden, and elsewhere). These developments contribute to a relatively unstable and unpredictable cross-border data policy environment, as reflected in various corporate securities filings highlighting material cross-border data policy risks associated with EU-focused investments, operations, and sales. See IAPP analysis of SEC filings for GSK, Telefonica Deutschland, Alphabet, and others (May 15, 2023), https://www.linkedin.com/posts/joe-jones-b1793bb6_datatransfers-gdpr-activity-7062799650386255872-A2wq/?utm_source=share&utm_medium=member_ios. The Member States of the European Free Trade Association (Iceland, Lichtenstein, Norway, and Switzerland) have not yet proposed or adopted provisions that replicate the EU Data Act, EUCS, or EHDS. For this reason, these countries currently have a lower restrictiveness score than the EU Member States.
- ³⁸ See e.g., Global Industry Statement in Support of a New Trans-Atlantic Data Privacy Framework (2022), <https://globaldataalliance.org/wp-content/uploads/2022/04/04072022gdagltr.pdf> (highlighting the costs to the EU from an interruption in the ability to transfer data across borders. The Statement analyzes costs from the perspective of (1) EU economic growth, employment, and exports; (2) EU enterprise operations; (3) EU innovation and technology leadership; (4) EU small- and medium-sized enterprises; and (5) transatlantic data privacy standards.
- ³⁹ UNCTAD, *Digital Economy Report* (2021), https://unctad.org/system/files/official-document/der2021_en.pdf.
- ⁴⁰ Global Data Alliance, *Selected Cross-Border Data Measures of Concern* (2023), <https://globaldataalliance.org/wp-content/uploads/2023/02/0210212023gdajpmeti.pdf>; Global Data Alliance, *Global Inventory of Domestic Rules on Data Localization and Data Transfers* (2023), https://globaldataalliance.org/resources-results/?pub_type=legal-texts&posts_filtered=1.
- ⁴¹ BSA, *Global Cloud Computing Scorecard* (2018), <https://www.bsa.org/reports/2018-bsa-global-cloud-computing-scorecard>. The BSA Global Cloud Computing Scorecard examines the legal and regulatory framework of 24 countries around the world, identifying 72 questions that are relevant to determining readiness for cloud computing. The questions are categorized under the following policy categories: Data Privacy, Security, Cybercrime, Intellectual Property Rights, Support for International Standards, Promoting Free Trade, IT Readiness, and Broadband Deployment.
- ⁴² European Centre for International Political Economy, *Restrictions on Cross-Border Data Flows: A Taxonomy*, ECIPE Working Paper 1/2017 (2017), <https://ecipe.org/wp-content/uploads/2017/11/Restrictions-on-cross-border-data-flows-a-taxonomy-final1.pdf>. See also European University Institute, *Digital Trade Integration Database* (2022), <https://dti.eui.eu/>.
- ⁴³ Information Technology Industry Foundation, *A Global View of Barriers to Cross-Border Data Flows* (2021), <https://itif.org/publications/2021/07/19/global-view-barriers-cross-border-data-flows/>. This report “uses sub-indicators from the OECD PMR Indicators database to develop a proxy measurement of how restrictive a nation’s rules are for cross-border data transfers. Pre-2018, DRI is calculated using the two medium-level indicators ‘Administrative Barriers to Startups’ and ‘Administrative and Regulatory Opacity.’”
- ⁴⁴ OECD, *Digital Services Trade Restrictiveness Index* (2019), <https://goingdigital.oecd.org/en/indicator/73>.
- ⁴⁵ OECD, *Services Trade Restrictiveness Index* (2023), https://issuu.com/oecd/publishing/docs/stri_policy_trends_up_to_2023_final.
- ⁴⁶ Salesforce, *Data Beyond Borders 3.0: Bridging the Digital Divide* (2023), https://www.salesforce.com/content/dam/web/en_au/www/documents/pdf/data_beyond_borders.pdf. The Salesforce Data Beyond Borders Report includes economy-level metrics focused on data localization, data classification, consent-based transfers, GDPR-level adequacy, and participation in the APEC Cross-Border Privacy Rules Framework.
- ⁴⁷ Tufts University Fletcher School, *Digital Intelligence Index* (2022), <https://digitalintelligence.fletcher.tufts.edu>. The Digital Intelligence Index “tracks a total of 160 indicators to measure the current state and pace of digitalization in an economy. It is structured at four levels: indicators, clusters, components, and drivers. Indicators are standardized data points that answer a specific question. Indicators are aggregated up into clusters, which illuminate 35 aspects of digitalization, which are then rolled into 13 higher-order components, which ultimately feed into the four drivers.”
- ⁴⁸ UK Department of Culture, Media, and Sports, *The Extent and Impact of Data Localisation* (2022), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1125805/Frontier_Economics_-_data_localisation_report_-_June_2022.pdf.
- ⁴⁹ G7 Hiroshima Leaders’ Communiqué (May 2023), <https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/g7-hiroshima-leaders-communicue/>.
- ⁵⁰ WEF, *A Roadmap for Cross-Border Data Flows* (2020), http://www3.weforum.org/docs/WEF_A_Roadmap_for_Cross_Border_Data_Flows_2020.pdf.

EXHIBIT 17

United States Senate

WASHINGTON, DC 20510

November 30, 2023

The Honorable Joseph R. Biden, Jr.
President of the United States
The White House
1600 Pennsylvania Avenue NW
Washington, D.C. 20500

Dear President Biden:

We write to express our concerns with the decision of the United States Trade Representative (USTR) to stop supporting key commitments in the e-commerce negotiations at the World Trade Organization (WTO)—and potentially in other negotiations. These commitments reflect bipartisan principles that, until now, the United States has strongly supported across political parties, administrations, and the federal government: an open internet that promotes the flow of information across borders to support American exports and American values. USTR's decision to abandon these commitments at the WTO creates a policy vacuum that China and Russia will fill. Accordingly, before changing the longstanding U.S. position, we request that you work with Congress and run a comprehensive consultation process—with other federal agencies, with the public, and with us—to reach a consensus U.S. position on these issues that promotes U.S. competitiveness, innovation, and jobs.

For decades, the United States has been at the helm of global leadership on protecting, promoting, and expanding the open internet as both a means of worldwide connectivity and an engine of U.S. economic growth and opportunity. This effort has long been a feature of U.S. trade policy: the United States advocated for commitments to ensure the free flow of information in WTO rules agreed to almost 30 years ago, and our trade agreements with Korea, Mexico, Canada, and Japan include strong digital trade rules guaranteeing the right to move data across borders. In this vein, the United States joined negotiations on e-commerce at the WTO, working with like-minded democratic allies to create rules for a digital economy that is open, fair, and competitive for all. The United States has supported proposals to spur economic growth, encourage free expression and access to information, and promote consumer protections online, while also allowing countries to address concerns regarding security, privacy, surveillance, and competition. These negotiations are crucial to our strategic approach to outcompeting our adversaries: both China and Russia are at the negotiating table, actively pushing their cyber-agenda of censorship, repression, and surveillance that not only hurts their own citizens but also undercuts U.S. competitiveness. Indeed, China is actively seeking to weaken the very principles at issue so it can promote its own version of internet governance.

In spite of this, on October 25, 2023, USTR reversed course and announced that it was walking away from the negotiating table on several core commitments in the e-commerce negotiations. These commitments, which again have broad bipartisan support, are fundamental to the modern economy, supporting U.S. businesses of all sizes across all sectors. Specifically, USTR abandoned the following commitments:

- *Promoting the free flow of data.* Almost every sector of the U.S. economy requires cross-border data flows, from manufacturers sharing product specifications, to airlines diagnosing problems mid-flight, to farmers leveraging precision agriculture to maximize crop yield. Arbitrary and trade-distorting restrictions on cross-border data flows that serve no legitimate public policy purpose can prevent American firms from doing business abroad, stifle economic growth here at home, and trample on human rights in authoritarian countries. Russia, for example, has weaponized data-restrictive laws to crack down on dissent, control information, and expel civil society organizations amidst its ongoing invasion of Ukraine.¹ Recognizing the importance of data flows to U.S. economic and foreign policy goals, the United States' original proposal at the WTO sought to ensure that consumers, companies, and non-governmental organizations could move data across international borders, while recognizing that countries must be able to act in the public interest, such as to protect personal data from abuse and foreign surveillance.
- *Combating forced data localization.* China and Russia, as well as other countries emboldened by their actions, have increasingly pursued data localization measures that require certain domestic data to be stored or processed within their borders. These policies require companies to build or maintain capital- and energy-intensive infrastructure in every market they enter, a major expense for large businesses, but an insurmountable hurdle for small and medium-sized enterprises. Small and medium-sized businesses are then left with an impossible choice: enter a risky joint venture with a foreign enterprise or get shut out of the market entirely. In this way, authoritarian governments leverage data localization measures to discourage competition and facilitate governmental access to data within their borders, helping them access trade secrets, censor and surveil their citizens, and hide human rights abuses, including forced labor.² The United States' proposal sought to limit data localization, while acknowledging that in certain circumstances, data localization may be appropriate to address national security, law enforcement, and privacy concerns.
- *Preventing forced tech transfer.* The U.S. government opposes the Chinese government's practice of conditioning market access on the sharing of proprietary information belonging to U.S. innovators, creators, and start-ups—a threat to both our economic and national security.³ The United States' proposal sought to ensure that countries could not

¹ Justin Sherman, The Brookings Institution, *Russia is Weaponizing Its Data Laws Against Foreign Organizations* (Sept. 27, 2022), <https://www.brookings.edu/articles/russia-is-weaponizing-its-data-laws-against-foreign-organizations/>.

² Freedom House, *User Privacy or Cyber Sovereignty?* (2020), <https://freedomhouse.org/report/special-report/2020/user-privacy-or-cyber-sovereignty>.

³ Daniel Wagner, *The Global Implications of China's National and Cyber Security Laws*, International Policy Digest (Aug. 10, 2020), <https://intpolicydigest.org/the-global-implications-of-china-s-national-and-cyber-security->

force businesses to surrender their source code or share it with domestic competitors as a condition of doing business, while preserving the ability of governments to access source code to achieve legitimate public policy objectives, such as conducting investigations and examinations and promoting consumer health and safety.

- *Open, competitive markets for digital goods and services.* The principle of non-discrimination has been a central component of U.S. trade policy for decades and underlies the international trading system that the United States helped create. It has opened markets for American exporters across industries, from farmers to filmmakers. At its core, non-discrimination ensures that foreign governments treat U.S. companies fairly. It ensures that countries cannot gain a competitive edge by targeting their regulations on imports from one or multiple countries without regulating similarly situated domestic businesses. China, in particular, has leveraged discriminatory policies to handicap international competitors and nurture its domestic companies, many of which are state-owned enterprises that operate at the behest of the Chinese government.⁴ Not only do these homegrown giants facilitate human and worker rights abuses, particularly in the Uyghur community in Xinjiang, but they have the ability to grow without competition and then undercut American competitors in international markets. Recognizing this, the U.S. WTO proposal sought to ensure that protections against discrimination would apply to digital products (e.g., apps, music, games, and movies), ensuring that American creators, innovators, and businesses could operate on a level playing field around the world.

As indicated above, each of these commitments maintained flexibility to regulate for legitimate public policy reasons.

USTR provided no policy alternatives to these longstanding and bipartisan U.S. positions, nor a timeline for providing them. We are concerned that USTR's retreat will hurt workers and employers across all sectors of the U.S. economy, with disproportionate effects on small and medium-sized businesses in creative industries like film, music, and book publishing; innovative industries like software, medical devices, and precision agriculture; travel, tourism, and transportation; logistics, shipping, and supply chain management; and manufacturing, including the critical automotive and semiconductor sectors. Moreover, with this abrupt change in policy, USTR has not only turned its back on our democratic allies and undermined U.S. credibility in other negotiations and fora around the world, but it has also empowered authoritarian regimes like China and Russia, who are eager to fill the void and regulate U.S. jobs out of existence.

We recognize that there is much interest in the digital regulation space, particularly with the rapid adoption of artificial intelligence technology. We welcome discussions and debate on the best way to protect consumers, promote privacy, and ensure a competitive marketplace. However, these efforts do not require the United States to walk away from negotiating strong rules at the WTO that support U.S. businesses and workers—nor would these rules constrain the

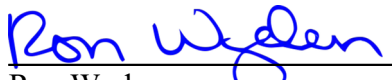
[laws](#).


⁴ U.S.-China Economic and Security Review Commission, *2021 Annual Report to Congress* at p. 165, <https://www.uscc.gov/annual-report/2021-annual-report-congress> (“The Chinese Communist Party (CCP) views achieving technological self-sufficiency as essential for both economic growth and political survival.”).


ability of the United States to regulate. In fact, the commitments under discussion have built-in exceptions that ensure countries can legislate in the public interest. Retreating from our longstanding principles without offering a viable alternative does not help U.S. workers, it does not help U.S. consumers, it does not help U.S. businesses, and it does not help U.S. allies; it only helps our adversaries.

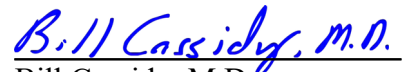
We continue to support the core commitments that USTR has distanced itself from in the WTO e-commerce negotiations. We request that you run a consultation process before changing the historical, consensus U.S. position on these important issues. We look forward to working with you to address this and other bipartisan Member concerns.


Sincerely,



Ron Wyden
United States Senator



Mike Crapo
United States Senator



Thomas R. Carper
United States Senator



Bill Cassidy, M.D.
United States Senator


Chris Van Hollen
United States Senator


Thom Tillis
United States Senator


Christopher A. Coons
United States Senator

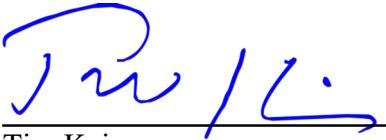

John Barrasso, M.D.
United States Senator



Catherine Cortez Masto
United States Senator



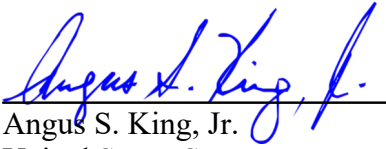
Charles E. Grassley
United States Senator



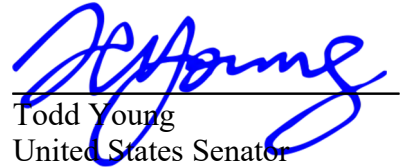
Tim Kaine
United States Senator



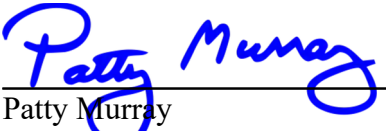
Ted Budd
United States Senator



Angus S. King, Jr.
United States Senator



Todd Young
United States Senator



Patty Murray
United States Senator



Shelley Moore Capito
United States Senator



Kirsten Gillibrand
United States Senator



Steve Daines
United States Senator



Maria Cantwell
United States Senator



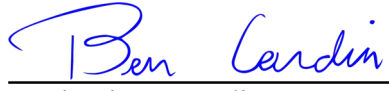
Kevin Cramer
United States Senator



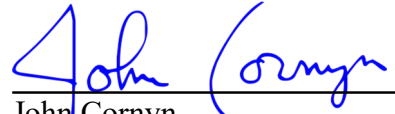
Kyrsten Sinema
United States Senator



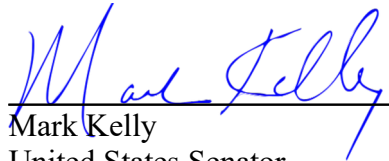
Cynthia M. Lummis
United States Senator



Benjamin L. Cardin
United States Senator



John Cornyn
United States Senator



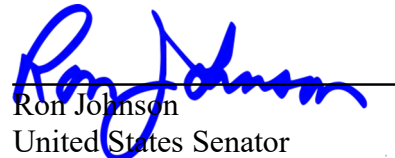
Mark Kelly
United States Senator



James E. Risch
United States Senator



Ted Cruz
United States Senator



Ron Johnson
United States Senator



Jacky Rosen
United States Senator



Alex Padilla
United States Senator



Tim Scott
United States Senator



James Lankford
United States Senator

EXHIBIT 18A



中华人民共和国商务部

MINISTRY OF COMMERCE OF THE PEOPLE'S REPUBLIC OF CHINA

Quotation marks | 000013223/2024-76421

The affiliation of the information | Electronic Commerce Division

The name of the document | Notice of the Ministry of Commerce on Printing and Distributing the Three-Year Action Plan for Digital Commerce (2024-2026).

Symbol | Commercial Telephone Letter [2024] No. 77 | Effective Date | 2024-04-26 | Release date | 2024-04-28

Topic categorization | Theme | Digital commerce

Notice of the Ministry of Commerce on Printing and Distributing the Three-Year Action Plan for Digital Commerce (2024-2026).

The competent departments of commerce of all provinces, autonomous regions, municipalities directly under the Central Government and the Xinjiang Production and Construction Corps:

In order to implement the decisions and arrangements of the CPC Central Committee and the State Council on the development of the digital economy, and better promote the digital development of all fields of commerce, our ministry has researched and formulated the "Three-Year Action Plan for Digital Commerce (2024-2026)", which is hereby issued to you, please implement it in light of the actual situation.

Commerce
April 26, 2024

Three-Year Action Plan for Digital Commerce (2024-2026)

Digital commerce is an important component of the most rapid development, the most active innovation and the most abundant application of the digital economy, the specific practice of the digital economy in the business field, and the implementation path of digital development in various fields of business. This action plan is formulated so as to implement the decisions and deployments of the Party Central Committee and the State Council on the development of the digital economy, to better promote the digital transformation of all areas of commerce, to empower economic and social development, and to serve the construction of a new development pattern.

1. General requirements

Guided by Xi Jinping Thought on Socialism with Chinese Characteristics for a New Era, thoroughly implement the spirit of the 20th National Congress of the Communist Party of China, completely, accurately and comprehensively implement the new development concept, follow the laws of digital economy development, based on the "three important" positioning of business work, and take the development of new

quality productivity as the starting point, innovate the path of digital transformation, improve the effect of digital empowerment, do a good job in digital support services, build a digital business ecosystem, comprehensively improve the digital, networked and intelligent level of business development, and help China's digital economy continue to become stronger, better and bigger.

—Adhere to innovation-driven. Strengthen the in-depth application of advanced information technology in the whole chain in various fields of business, and promote the innovation of models, formats, products and services. With the advantages of rich application scenarios in the business field, we will drive the implementation of advanced technologies and product and service innovation, and form a high-level development situation in which demand drives supply and supply creates demand.

—Adhere to data empowerment. Deeply explore the value of data elements in the business field, strengthen the in-depth empowerment of data in the fields of circulation, consumption, foreign trade, foreign investment, foreign investment, and international cooperation, and effectively give full play to the supporting role of data elements in improving quality, reducing costs, and increasing efficiency in the business field, so as to create a new digital engine for high-quality business development.

-- Adhere to integrated development. With data and scenarios as the link, we will promote the integration of online and offline, urban and rural, and domestic and international in the business field, break down industry barriers, encourage cross-border development, and effectively promote the integration of domestic and foreign trade.

-- Persist in opening wider to the outside world. Deepen international cooperation in digital commerce, further enrich the level of cooperation, expand cooperation channels, build cooperation carriers, carry out pilot trials in line with international high-standard economic and trade rules, and lead new advantages in international cooperation with digitalization in the business field.

By the end of 2026, the level of digitalization, networking, intelligence, and integration in all fields of commerce will be significantly improved, the scale and efficiency of digital commerce will grow steadily, the industrial ecology will be more perfect, the application scenarios will be continuously enriched, international cooperation will continue to expand, and the support system will become increasingly sound. The scale of the digital economy in the business sector continues to grow, the scale of online retail remains the largest in the world, the growth rate of cross-border e-commerce is faster than the growth rate of trade in goods, the use of trade electronic documents has reached the international average, and the overall scale of digital trade continues to expand.

2. Key actions

(1) The action of "strengthening the foundation of digital business".

The first is to cultivate the main body of innovation. Create a group of digital business enterprises and industrial clusters that lead innovation. Select a number of excellent cases of commercial science and technology innovation and application, and guide enterprises to increase the innovation and application of advanced information technology. Cultivate a group of data service providers in the business field to release the value of data elements in multiple scenarios.

The second is to build a monitoring and evaluation system. Establish and improve the monitoring and evaluation system for digital commerce, and scientifically measure and reflect the level of development of digital commerce. Carry out full-caliber monitoring of digital commerce, and strengthen the coordination and data sharing of central and local work. Deepen the application of monitoring data, form dynamic indicators of digital commerce, and formulate digital business development indexes. Establish a digital business evaluation system, scientifically select indicators and formulate evaluation methods according to the basic conditions, development directions and work objectives of different regions, so as to provide a basis for evaluating effectiveness and improving work.

The third is to improve the level of governance. Accelerate the application of commercial big data, improve the early warning and disposal mechanism of central and local coordination, and improve the monitoring, forecasting and early warning capabilities in the fields of domestic and foreign trade and foreign investment. Encourage the coordination and linkage of local monitoring platforms and commercial big data platforms to improve the quality and expand the scope of the big data system. Establish a system for categorical and hierarchical protection of data in the commercial field, form a catalog of important data, and increase the security awareness and protection capabilities of data processors. Expand the supply of public data resources in the commercial sector, strengthen the construction of mobile terminals, and encourage all regions to explore the authorized operation of public data.

Fourth, strengthen intellectual support. Give full play to the supporting role of think tank alliances, research institutions, and industry organizations, and strengthen communication and contact with experts and scholars in the field of digital commerce. Support the cultivation of professionals in digital business-related disciplines, promote the collaboration between government, industry, academia, research and application, and carry out multi-level and practical digital business talent training. Give full play to the role of industry associations and industry alliances in the field of digital commerce, create a number of public service platforms for digital business talents, and promote the docking of supply and demand and resource sharing.

Fifth, promote the development of norms. Establish and improve the digital commerce standard system, make good use of the technical committee for the standardization of the digital commerce industry, issue guidelines for the standardization of the digital commerce industry, accelerate the construction of standards in key areas of business digitalization, promote the implementation and application of standards, and improve industry management and service quality. Strengthen the business credit system and brand building, and promote the improvement of the quality of digital commerce. Compile compliance guidelines for e-commerce enterprises, guide enterprises to operate in accordance with laws and regulations, and promote the standardized and healthy development of the industry.

(2) "Digital business expansion and elimination" action.

The first is to cultivate and expand new consumption. Implement digital consumption promotion actions, create a "4+N" online consumption matrix, and carry out four national online promotional activities: "National Online New Year Goods Festival", "Double Product Online Shopping Festival", "Digital Business Rejuvenation of Agriculture and Harvest Festival" and "Silk Road Cloud Product E-commerce Festival", and support all localities to carry out a series of supporting activities according to local conditions. Encourage the development of digital, green, health and other consumption, carry out online theme promotions such as home renovation, national tide renewal, scene renewal, etc., create a number of new scenarios for digital-real integrated consumption around new product experiences, cultural and entertainment tourism, sports events, medical and health care, etc., and cultivate a number of digital consumer brands.

The second is to promote online and offline integration. Encourage the digital development of the business and trade service industry. Confirm a number of smart business districts and smart stores, guide the commodity market to carry out digital transformation and intelligent upgrading, and promote the improvement of the coverage of smart service platforms in the convenient life circle within a quarter of an hour. Accelerate the digital empowerment of life services, and promote the digital and intelligent transformation and upgrading of life services. Improve the "Time-honored Brand Digital Museum" and stimulate the innovation vitality of time-honored brands.

The third is to stimulate the potential of rural consumption. Implement the high-quality development project of rural e-commerce, cultivate a number of rural e-commerce live broadcast bases and county-level digital circulation leading enterprises, organize and carry out rural live broadcast e-commerce related activities, and promote the digital transformation of the agricultural product industry chain. Implement "digital business to rejuvenate agriculture", organize the implementation of high-quality agricultural products "three products and one standard" certification assistance, and cultivate a number of regional characteristic network brands. Improve the rural mail and logistics system, and promote the coordinated development of rural e-commerce and express delivery.

Fourth, promote the docking of domestic and foreign trade markets. Promote the standardized and healthy development of the cross-border e-commerce retail import industry, and provide diversified choices for Chinese consumers with global good products. Encourage "Silk Road E-commerce" partner countries to set up exhibition and sales columns on China's e-commerce platforms, and support local governments to hold special activities such as national e-commerce theme weeks and live broadcasts of ambassadors to China, so as to drive the world to share China's e-commerce market. Guide e-commerce platforms to set up special areas and special sessions for domestic sales of foreign trade products to help foreign trade enterprises expand the domestic market and meet the diversified needs of consumers.

Fifth, promote the digital development of logistics in the field of trade circulation. Build a number of digital service platforms, strengthen the integration of logistics information in the whole link, promote the use of intelligent warehousing and distribution, unmanned logistics equipment, accelerate the use of standard pallets, turnover boxes (baskets), etc., improve distribution efficiency, and reduce logistics costs. Promote the coordinated development of e-commerce and express logistics, guide e-commerce platforms and express delivery companies to strengthen business docking and data sharing, carry out leading actions for e-commerce platform original packaging, and accelerate the green transformation of express packaging in the e-commerce field.

(3) "Digital Commerce and Trade" action.

The first is to improve the level of trade digitalization. Promote the digital development of the whole trade chain, rely on the Guangdong-Hong Kong-Macao Greater Bay Area Global Trade Digitalization Pilot Zone, the Pilot Free Trade Zone, and the Shanghai "Silk Road E-commerce" Cooperation Pilot Zone, etc., to accelerate the application of electronic trade documents and cross-border interoperability, and cultivate new momentum for foreign trade.

The second is to promote cross-border e-commerce exports. Optimize the way of cross-border e-commerce export supervision. Organize cross-border e-commerce comprehensive pilot zones to carry out special actions such as platforms and sellers going overseas. Support cross-border e-commerce to empower industrial belts, guide traditional foreign trade enterprises to develop cross-border e-commerce, and establish a marketing service system that integrates online and offline and links domestic and overseas. Improve the professional, large-scale and intelligent level of overseas warehouses.

The third is to expand the digital content of service trade. Implement the "Thousand Sails to the Sea" plan for foreign cultural trade, cultivate a number of brand projects and overseas platforms featuring digital cultural trade, support cultural enterprises to actively expand the international

market, and promote the development of digital cultural trade. Support e-commerce platforms to innovate digital products and services such as cloud computing and mobile payment, strengthen remote delivery capabilities, and develop overseas service markets.

Fourth, vigorously develop digital trade. Promote the reform, innovation and development of digital trade, establish and improve the digital trade governance system, and accelerate the development of new forms and models of digital trade. Actively carry out international cooperation in digital trade with relevant countries and regions. The Global Digital Trade Expo is held every year to strengthen the leading role of innovation and accelerate the implementation of achievements. Improve the digital level of important exhibitions and exhibitions, hold "cloud exhibitions", and carry out "cloud display", "cloud docking", "cloud negotiation" and "cloud signing".

(4) The action of "digital business and industry".

The first is to build a strong digital industrial chain and supply chain. Cultivate a number of B2B platforms that are deeply engaged in vertical industries. Relying on the e-commerce industry agglomeration area, we will create a number of characteristic digital and intelligent industrial belts to drive the transformation and upgrading of traditional industries. Carry out supply chain innovation and application, and introduce a special action plan for the development of digital supply chain. Build a number of digital international supply chain platforms, and improve the platform's comprehensive supply chain service functions such as credit evaluation, international logistics, payment and settlement, information services, and cross-border data flow.

The second is to optimize the environment for attracting foreign investment in the digital sector. We will continue to promote the relaxation of access to telecommunications and other industries, and attract more foreign-funded enterprises to invest in the digital industry. A negative list for cross-border trade in services has been introduced, and targeted opening-up measures have been put forward in the digital sector. Enhance the convenience of cross-border data flow for qualified foreign-funded enterprises. Support Beijing, Shanghai, Tianjin, and other pilot free trade zones in implementing systems for categorical and hierarchical protection of data, formulate important data catalogs and other institutional norms, and explore the establishment of legal, secure, and convenient mechanisms for cross-border data flows.

The third is to expand foreign investment and cooperation in the digital field. Actively negotiate and implement multilateral and bilateral memorandums of understanding on digital economy investment cooperation, and guide the rational and orderly cross-border layout of the digital economy industry chain. Promote the synergy between the overseas consumer platform and the domestic industrial platform, and encourage the e-commerce platform to drive the upstream and downstream of the industrial chain such as smart logistics and mobile payment to go overseas. We will do a good job in ensuring the service of digital enterprises going global, compile the annual "Guidelines for Countries (Regions) for Foreign Investment and Cooperation" and other public service products, actively respond to trade frictions in the digital field, and safeguard the legitimate rights and interests of our enterprises. Promote the facilitation and digitization of outbound investment, and promote the use of electronic certificates for outbound investment throughout the country.

(5) "Digital Business Opening" action.

The first is to expand the cooperation space of "Silk Road e-commerce". Broaden the circle of friends of "Silk Road e-commerce" and promote the establishment of new bilateral cooperation mechanisms for e-commerce with more countries. Promote the implementation of existing mechanisms, carry out policy coordination, industrial docking, local cooperation, and capacity building, and tighten trade ties with co-construction countries. Explore the establishment of a global e-commerce cooperation alliance. Create a number of "Silk Road e-commerce" local cooperative brands, encourage local governments to give full play to their resource endowments and industrial characteristics, and carry out cooperation and docking with relevant countries and regions.

The second is to carry out the first trial of digital rules. Based on its own institutional framework, it will align with international high-standard economic and trade rules, guide pilot free trade zones and free trade ports to carry out pilot trials and stress tests in the digital field, and accelerate the formation of a number of institutional opening-up achievements with leading roles. Implement the work plan of the "Silk Road E-commerce" Cooperation Pilot Zone, promote institutional innovation, expand institutional opening-up, cultivate functional service entities, promote the implementation and effectiveness of 38 pilot measures, and promote mature experience in a timely manner.

Third, we should actively participate in the governance of the global digital economy. Voice China's voice, contribute China's wisdom, and promote the achievement of a number of consensus on digital economy cooperation. Actively promote the process of joining the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the Digital Economy Partnership Agreement (DEPA). Actively participate in the WTO e-commerce negotiations. Strengthen regional, multilateral and bilateral dialogue and cooperation in the digital field such as the Shanghai Cooperation Organization, BRICS, G20 and APEC, and expand new space for mutually beneficial and win-win international cooperation in the digital economy. Implement and promote the Framework Agreement on International Economic and Trade Cooperation on Digital Economy and Green Development, and launch a number of cooperation projects focusing on trade and investment promotion, policy exchanges, and skills training.

3. Safeguard measures

Local competent departments of commerce should strengthen organizational leadership, strengthen digital thinking and innovation awareness, base themselves on regional endowments, make good use of existing working mechanisms, and actively coordinate supporting resources in the fields of data, talent, finance, logistics, and infrastructure. Coordinate and make good use of existing fiscal and capital policies, support digital business entities and key projects, promote the connection between financial enterprises and digital business enterprises, and actively support the financing needs of digital business small and medium-sized enterprises. Promptly summarize phased results, good experiences, and good practices, and conduct publicity and reporting through various channels and methods such as local media and government websites. Adhere to the bottom line of security, ensure data security and network security in the commercial field, resolutely safeguard national sovereignty, security and development interests, strictly implement the responsibility of "three controls and three musts", and prevent safety production risks in the field of digital commerce.

Scan to open the current page on your phone



[Export PDF files](#)

Link: [Chinese government website](#) [Local commerce authorities](#) [Related Societies](#)

Organizer: Ministry of Commerce of the People's Republic of China Website identification code bm22000001 Beijing ICP No. 05004093-1 

Beijing Public Network Security No. 11040102700091

Website management: Department of E-commerce and Information Technology of the Ministry of Commerce Technical Support: China

International Electronic Commerce Center Technical Support Tel: 010-85093026

Website service telephone: 010-85093020 Unified platform technical support telephone: 010-67870108 E-mail: E-mail of the Ministry of Commerce

[English](#)
[Français](#)
[Русский](#)
[Español](#)
[Deutsch](#)

[Weibo,](#)
[WeChat public](#)
[account](#)
[, mobile client](#)
[, intelligent](#)
[Q&A](#)



[Nostalgia](#)

[for the](#)

[Website](#)

[Site](#)

[Information](#)

[staff](#)

[old](#)

[Contact](#)

[Internal](#)

[Administration](#)

[Site Map](#)

[Statement](#)

[statistics](#)

[member](#)

[station](#)

[us](#)

[mailbox](#)

EXHIBIT 18B

COMMENTARY ([HTTPS://MACROPOLO.ORG/COMMENTARY/](https://macropolo.org/commentary/))



DIGITAL PROJECTS ([HTTPS://MACROPOLO.ORG/DIGITAL-PROJECTS/](https://macropolo.org/digital-projects/))

(<https://macropolo.org>)

ANALYSIS ([HTTPS://MACROPOLO.ORG/ANALYSIS/](https://macropolo.org/analysis/))

July 16, 2019 ECONOMY (<https://macropolo.org/category/economy/>), POLITICS (<https://macropolo.org/category/politics/>),

TECHNOLOGY (<https://macropolo.org/category/technology/>)
MULTIMEDIA ([HTTPS://MACROPOLO.ORG/MULTIMEDIA/](https://macropolo.org/multimedia/))

ABOUT ([HTTPS://MACROPOLO.ORG/ABOUT/](https://macropolo.org/about/))

Much Ado About Data: How America and China Stack Up

Matt Sheehan (<https://macropolo.org/author/mattsheehan/>)

(<https://macropolo.org/ai-data-us-china/>)

Analysts often cite the amount of data in China as a core advantage of its artificial intelligence (AI) ecosystem compared to the United States. That's true to a certain extent: 1.4 billion people + deep smartphone penetration + 24/7 online and offline data collection = staggering amount of data.

But the reality is far more complex, because data is not a single-dimensional input into AI, something that China simply has "more" of. The relationship between data and AI prowess is analogous to the relationship between labor and the economy. China may have an abundance of workers, but the quality, structure, and mobility of that labor force is just as important to economic development.

Likewise, data is better understood as a key input with five different dimensions—quantity, depth, quality, diversity, and access—all of which affect what data can do for AI systems.

What follows is a framework for analyzing the comparative advantages of countries and companies across the five dimensions, with the aim of bringing more precision to comparisons of how America and China stack up. This is, however, just one framework, and I welcome critiques and suggestions on how to quantitatively measure each of these dimensions.
Your access to, and use of this website, is subject to the [Terms of Use](#), which can be read in its entirety [here](#) ([terms-of-use](#)).

Why Does Data Matter To AI Systems?

Before getting to the five dimensions, a detour into data's role in AI systems is in order.

Advances in AI have given computers superhuman pattern-recognition skills: the ability to wade through oceans of digital data, spotting thousands of hidden patterns or correlations between inputs and outcomes. AI systems then use those correlations to make inferences or predictions, "learning" how to perform a task based on the examples it has seen in the data.





No single correlation can correctly predict an outcome on its own. But increases in computing power now allow AI algorithms to examine correlations across millions or even billions of examples. As more or better data is fed into the system, the accuracy of these predictions can improve dramatically.

That is why data is crucial to machine learning today. It is the fuel that most AI applications today—online shopping recommendations, facial recognition, autonomous vehicles, and machine translation—run on and what allows them to learn and master a specific task.

Breaking Down the Five Dimensions

The following section provides an overview of the five dimensions (see Table), followed by analysis of each one, and concludes with a brief look at how the balance of capabilities could change over time.

Table. The 5 Dimensions of Data in China and the US

Dimension	Description	Examples	Advantage	Notes
Quantity	# of users or events.	# of active Facebook users; # of trips made on shared bikes.	Even	US = higher ceiling; China = faster scaling.
Depth	Different aspects of user behavior or events captured in digital form.	% of daily trips, transactions, meals, etc. done using a smartphone.		Greater % of urban activities done via smartphones.
Quality	Accuracy of data used for training; how that data is structured and stored.	How corporate financial records are created and stored.		US private sector far ahead; potential for China to catch up in public sector data.
Diversity	Heterogeneity of users or events studied.	# of different ethnicities used to train a facial recognition model		US = diverse domestic + global user base; China = more economically diverse domestic users.
Access	Availability of data to relevant actors.	How is surveillance footage gathered and who can access it?		Gov + private access to massive scope of surveillance + traffic cameras.

Note: The term "advantage" simply connotes the respective capability in each dimension and is not meant to render a value judgment on how the capability is deployed and to what end. Data can be used for everything from improving cancer diagnoses to expanding a surveillance state (<https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html>).

Quantity

Your access to, and use of this website, is subject to the Terms of Use, which can be read in its entirety here (/terms-of-use).

Many assume the size of China's population gives it an advantage in the volume of data, but this is actually misleading. Chinese tech companies can tap the world's largest domestic population, but very few of them have succeeded in reaching global users. In contrast, American tech giants make up for their far smaller pool of domestic users by drawing the majority of their users (and data) from global markets.

WeChat and Facebook make for a clear contrast. WeChat has leveraged China's 800 million internet users to rapidly scale up, but it has weak global penetration, capping out at 1.1 billion users (<https://www.statista.com/statistics/255778/number-of-active-wechat-messenger-accounts/>) today. Facebook, however, has long outgrown its US home market and now reaches 2.3 billion users (<https://www.nbcnews.com/tech/tech-news/facebook-hits-2-27-billion-monthly-active-users-earnings-stabilize-n926391>) globally.

This means that—for now, at least—Chinese tech companies can scale up faster by relying on only domestic users, while US (and European) companies tend to have a higher ceiling for total users given their global reach.

Depth

Depth of data refers to *different aspects* of user behavior captured in digital form. The more an algorithm is trained on different types of user behavior, the more sophisticated its recommendations or predictions can be for that user.

China's advantage mainly lies in the fact that its leading tech companies have many more windows into a user's online and offline behaviors. This is a result of the fact that a far larger portion of an urban Chinese citizen's real-world activities are funneled through smartphones (see ChinAI (<https://macropolo.org/digital-projects/chinai/the-data/>) for an interactive demonstration).

Each of those real-world activities—bikeshare trips, meals ordered, appointments booked—is a small window into user habits, which can be used to more accurately tailor recommendations for that user. While US tech giants often know a lot about their users’ online habits (search history, pages “liked”, etc.), they have more limited insight into users’ real-world activities compared with Chinese counterparts like Tencent, Alibaba, and Meituan.

Quality

Quality refers to both the *accuracy*, and the *structure* and *storage* of the training data. The United States has an edge on both because its data tend to be more reliable, and much more of its data have been digitized and stored in easily retrievable formats.

RELATED

Eye on Indonesian Tech: Where US and Chinese Companies Vie for Market Power and Soft Power (<https://macropolo.org/analysis/indonesian-tech-us-chinese-companies-market-power-soft-power/>)

Matt Sheehan (<https://macropolo.org/author/mattsheehan/>) and Anarkalee Perera (<https://macropolo.org/author/anarkaleeperera/>)
Your access to, and use of this website, is subject to the Terms of Use, which can be read in its entirety here ([terms-of-use](#)).

(<https://macropolo.org/analysis/indonesian-tech-us-chinese-companies-market-power-soft-power/>)

Beijing's Approach to Trustworthy AI Isn't So Dissimilar from the World's (<https://macropolo.org/beijing-approach-trustworthy-ai/>)

Matt Sheehan (<https://macropolo.org/author/mattsheehan/>)

(<https://macropolo.org/beijing-approach-trustworthy-ai/>)

First, on accuracy. When machine learning applications rely on training data, they are subject to a longstanding rule of computer science: “garbage in, garbage out.” If an AI algorithm is fed inaccurate data, it will produce inaccurate outputs.

For example, if the Chinese government wanted an early warning system for “airpocalypse” days, it might train an algorithm using historical data to find correlations between pollution and hundreds of variables. But if the historical data is inaccurate, the algorithm will learn faulty correlations and produce inaccurate predictions. That kind of inaccuracy is common across many public and private sector datasets in China, giving the US an advantage from its (relatively) reliable data.

Second, on structure and storage. Data is useful to AI algorithms when it is stored in a computer-readable format and structured consistently. A consistent digital database of medical symptoms and their corresponding diagnoses can be used to train an AI doctor, whereas thousands of handwritten slips of diagnoses cannot.

On this front, American hospitals, companies, and bureaucracies have an enormous head start on their Chinese peers, which have not invested as much in enterprise software or digitizing data. That may change over time, however, as Beijing is investing heavily and incentivizing localities to digitize records and adopt AI-powered analytical tools.

Diversity

Data heterogeneity is important to train AI algorithms on diverse skills related to a given task.

America holds a clear advantage in this dimension because of its diverse domestic population and the global user base of many Silicon Valley companies. Users of Google and Facebook represent a far greater range of languages, ethnicities, and nationalities than users of WeChat or Baidu.

Your access to, and use of this website, is subject to the Terms of Use, which can be read in its entirety here (</terms-of-use>).

In contrast, a facial recognition algorithm trained on one billion Chinese faces will be excellent at identifying another Chinese face, but it may struggle when deployed in Ethiopia or Norway. The same challenge applies to machine translation and speech recognition with different accents.

One potential advantage for China is the economic diversity of users on which it has deep consumer data. While US companies reach users across the globe, they don't often draw the same depth of data from those populations.

Chinese companies may have limited global reach, but their insights on the consumption habits of an economically diverse population at home run the gamut: from the global elite of Shanghai (comparable to rich Singaporeans) to poor Guizhou farmers (comparable to parts of Indonesia or India). Such rich data on an economically diverse population may give Chinese AI companies crossover potential in other emerging markets.

Access

China holds a distinct advantage in accessing data from public spaces. That data is gathered through the country's sprawling network of surveillance, security, and traffic cameras—tools that can “datatize” public spaces by identifying and analyzing the movement of each car, bike, bus, and pedestrian.

Chinese city governments have initiated dozens of partnerships with private firms like Alibaba on “smart city” projects, granting them access to these data streams in a bid to optimize everything from big brother surveillance to traffic management. Partnerships between China's leading facial recognition startups and law enforcement are similarly vacuuming up hundreds of millions of face scans, using them to stitch together a national surveillance system and track the country's (<https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html>) Uighur minority.

Source: Alibaba Cloud.

Even with that access, perception often outstrips the reality of Chinese capabilities. Many installed surveillance cameras are not currently equipped with AI technology, and even those that are often cannot effectively store or integrate data into larger systems.

Your access to, and use of this website, is subject to the Terms of Use, which can be read in its entirety here (</terms-of-use>).

Still, the growing access of Chinese government and private actors to this data marks a major departure from the United States, where municipalities have proactively banned facial recognition (<https://www.nytimes.com/2019/07/01/us/facial-recognition-san-francisco.html>) technology due to concerns over privacy, personal freedoms, and racial profiling.

Where Things Are Headed

The above assessments represent a snapshot—and a relatively subjective one—of where the two countries stand today. So which of these dimensions might see significant shifts in coming years?

Chinese apps such as Tik Tok have recently met with major success outside of China, and if that trend continues it will increase the quantity and diversity of users for Chinese companies. Chinese government incentives for applying AI in the public sector (<https://macropolo.org/analysis/how-chinas-massive-ai-plan-actually-works/>) are also likely to raise the quality of data through better structuring and storage.

American tech companies are increasing the depth of their data, with Apple pushing mobile payments and smart home technologies like Amazon's Alexa capturing more offline activities in digital data.

But perhaps bigger than any relative gains across these dimensions would be advances in the field of AI that dramatically reduce the need for large amounts of user-generated training data. Cutting-edge AI systems like DeepMind's AlphaGo Zero have already demonstrated the power of approaches like reinforcement learning, which generates its own data through simulations.

If those approaches prove widely applicable, they could devalue the relative importance of data while increasing the value of advanced semiconductors or research talent (</china-ai-research-talent-data>).

GET OUR STUFF

Get on our mailing list to keep up with our analysis and new products.

SUBSCRIBE

(<http://eepurl.com/h3l8Yj>)

SHARE THIS ARTICLE



Your access to, and use of this website, is subject to the Terms of Use, which can be read in its entirety here (</terms-of-use>).

ACCEPT

EXHIBIT 18C

Assessing U.S. Data Policy Toward China: A Proposed Framework

Samm Sacks, Peter Swire

Friday, July 14, 2023, 10:40 AM



Addressing risks posed by Beijing's accessing Americans' data requires first conceptualizing the trade offs in current U.S. policy approaches.

Access to and use of personal data is at the forefront of the U.S.-China technology conflict. Republicans and Democrats have found common ground in the concern that unacceptable national security and privacy risks arise from Beijing's access to U.S. persons' data through open commercial channels. Over the past several years, U.S. policymakers have expanded their earlier focus on cyber theft and industrial espionage to grapple with new risks posed by Chinese firms handling U.S. persons' data or data flowing to China by data brokers or other means.

According to Director of National Intelligence Avril Haines (as cited in support of [a bill requiring licenses to export certain personal data to China and other countries](#)): "There's a concern about foreign adversaries getting commercially-acquired information as well, [I] am absolutely committed to trying to do everything we can to reduce that possibility."

The [Biden administration](#) and Congress are building on the effort (which started in the [Trump administration](#)) by putting forward a range of measures that aim to create new guardrails for data flows to China. These include [executive orders](#) and [rules](#) for reviewing transactions involving foreign adversaries' access to U.S. persons' sensitive data, bans on Chinese software applications, and creating blacklists of countries approved to receive U.S. persons' data as an export-controlled item, [among other actions](#). Many proposals remain in draft form, unresolved amid debate that does not map onto political party lines.

To date, we have not seen any systematic approach to address what limits on data flows should apply and for what reasons. [In a new report](#), published with the Cross Border Data Forum, we offer a framework to conceptualize current U.S. data policy toward China, identifying four distinct policy models and analyzing the costs and benefits of each, drawing on the perspectives of trade and economics, national security, and privacy. Rather than advocate for a particular policy solution, our aim is to inform policymaking by discussing the ripple effects of different options.

Four Models

First, the Digital Free Trade model emphasizes the benefits to the United States of having robust trade in goods and services in general, and with China more specifically. This model would place no limits on China or other countries simply because they have authoritarian political systems. This model has largely described the status quo in the U.S. The free trade perspective contributed to U.S. support for [China to enter the World Trade Organization](#) in 2001. Under the Digital Free Trade model, the main issue to address is what presumptions and showing of risk would need to be established as a basis for limiting trade.

Second, the Blocking Adversaries model seeks to restrict data from flowing to certain countries, such as China, that are deemed foreign adversaries by the U.S. government. The stated goal is to eliminate national security harms that could result if authoritarian governments were to gain access to information about either specific U.S. persons or population-level insights. The U.S. government has sought to use the Committee on Foreign Investment in the United States process to restrict TikTok's data flows from the U.S. to China and earlier blocked acquisition of the dating app Grindr. President Biden explained this rationale for action in the 2021 executive order entitled "Protecting Americans' Sensitive Data from Foreign Adversaries." Sen. Ron Wyden's (D-Ore.) Protecting Americans' Data From Foreign Surveillance Act would create an export control regime for bulk exports of U.S. persons' data to certain high-risk countries such as China.

Third, the Privacy Law model builds on the growing bipartisan consensus that the U.S. should enact comprehensive privacy legislation with the goal of addressing data processing by both domestic and foreign companies. This model is distinct from national security, because the focus is on overall protection of individuals' data, rather than on an assessment of the risk of the data in the hands of a particular adversary. More recently, however, lawmakers have emphasized that privacy legislation can also address trans-border privacy risks, with disclosure requirements or restrictions specifically applying to China and other adversaries.

Fourth, the Data Allies model provides a way to address specific national security and privacy risks posed by non-democracies, while retaining a willingness to engage in global trade when such risks are manageable. The Data Allies approach broadly describes the Biden administration's current approach, as shown in the 2022 Declaration for the Future of the Internet, which the U.S. launched with 60 partnering countries and aims to "realize the benefits of data free flows with trust based on our shared values as like-minded, democratic, open and outward looking partners." This model uses a principled basis to facilitate more data sharing with each other, while also using a stricter standard for "adversary" countries like Russia and China to access U.S. persons' data. As discussed in more detail in our report, and in other recent writing, data ally initiatives are proceeding on a multilateral basis, at the G-7 and the Organization for Economic Cooperation and Development, and as part of the initiatives for "data free flow with trust" and the Global Cross-Border Privacy Rules. The Data Allies model has also been incorporated more formally, such as in the 2015 Judicial Redress Act, the 2018 CLOUD Act, and the current EU/U.S. Data Privacy Framework.

Trade-Offs

The four models highlight areas of tension and overlap among the three goals of national security, free trade, and privacy. Recent U.S. policy debates have highlighted ways that national security can come into conflict with the Digital Free

Trade model. Both the Trump and Biden administrations have emphasized risks to national security, and personal data held by companies in China lacks rule-of-law safeguards against excessive surveillance. Our report identifies how U.S. policymakers perceive the nature of the national security risk, including combining data sets to target Americans in national security positions or with access to critical infrastructure, enabling bulk or targeted electronic surveillance, pushing out targeted misinformation, strengthening economic competitiveness of Chinese firms, and launching more effective cyberattacks.

These are legitimate national security concerns. Policy analysis should, however, recognize the ways that global trade may also advance national security and cybersecurity. Free trade can create stronger ties with potential adversaries such as China, and possibly reduce the likelihood and magnitude of conflict. Joseph Nye writes that entanglement can have a deterrent effect. He argues that the exponential increase in cross-border data flows underpinning global commerce can be a factor in cybersecurity and other forms of deterrence. For those inclined to cut ties with China, it is worth considering what conflict would look like if the U.S. were to block trade and create sanctions at the level now applying to North Korea. Some degree of trade and entanglement with China, therefore, likely supports U.S. national security.

A stronger U.S. economy can also benefit U.S. national security in ways that extend beyond the borders of both the U.S. and China. New limits on outbound data transfers from the U.S. make it more challenging for U.S. firms to push back against rising digital sovereignty in the EU, India, and globally. It also weakens cooperation with allies by making it more difficult to effectively share data for law enforcement, intelligence, cybersecurity, health research, and other common purposes. Restrictions on data flows imposed on U.S. firms by countries beyond China undermine the competitiveness of U.S. digital industries, reducing leadership in artificial intelligence and cybersecurity-related capabilities. Limits on exports of personal data, such as the telemetry used in cybersecurity, could reduce the ability of U.S. cybersecurity companies to service the global market.

As scholars have noted, trade and privacy often seem locked “in a mortal contest” between trade-based cross-border flows and privacy-based skepticism of such flows. Historically, the U.S. has generally favored a relatively free flow of data across borders, not least in order to support U.S.-based technology companies. More recently, the Data Allies model seems a more accurate description of U.S. policy, with initiatives such as the EU/U.S. Data Privacy Framework seeking to retain robust data flows with allied nations that offer privacy protections.

As for national security and privacy, congressional privacy debates in recent years have emphasized privacy rules across the board, rather than remaining focused only on data flows to adversary countries. The 2022 privacy legislation, which

passed the House Energy and Commerce Committee with a 53-2 bipartisan vote, had only modest notice requirements about transfers to China and a few other countries. More recently, there have been hearings in Congress that emphasized the specific privacy risks of data flows to China, showing more convergence between the national security and privacy goals. Nonetheless, effective overall protection of privacy would address the vast majority of data collection and use, which does not involve China or other adversaries.

Conclusion

Each of the four models clarifies what is at stake for the possible limits on transfers of U.S. persons' data to China in pursuit of the goals of economic growth, national security, and privacy protections.

Going forward, analysis should realistically examine the effects of a proposal on each of these important policy goals. Such analysis is consistent with the 2021 executive order, which called for a "through rigorous, evidence-based analysis." With respect to economic growth and international trade with China, these goals likely remain in effect for many exports, imports, and across many sectors. Therefore, a blanket ban on digital trade with China would be an overreaction to concerns about national security and privacy. Further, the Data Allies model can be used as a way to conceptualize the emerging U.S. approach for international data transfers.

With the current attention to data access by Chinese-based companies, there is a risk that ill-considered limits will have harmful spillover effects on U.S. national interests. Privacy and national security arguments to wall off U.S. persons' data or ban platforms entirely should take into consideration the consequences of doing so—both for stated national security objectives as well as those for that go beyond a national security rationale.

While we provide a framework for analyzing these important issues, we do not presume to have all the facts needed to make comprehensive policy recommendations. One path worthy of consideration for those who do have such insight is to enact the sort of comprehensive privacy legislation that Congress has considered, perhaps with targeted provisions limiting data flows in certain circumstances and addressing the most serious risks from data brokers. Greater attention to the details of such an approach is beyond the scope of this article. Our hope is that this framework can serve as a foundation, useful to those across the political spectrum, that can help determine the most effective approach for meeting the multiple goals of U.S. policy.

EXHIBIT 19A



Memorandum

Impact of USTR’s Digital Trade Policy Reversal on Supply Chain Resilience and Other US Government Priorities

Updated May 2024

The Global Data Alliance¹ has generated this memorandum to provide an overview of the impact on US interests caused by the reversal of longstanding US cross-border data policy effectuated by the Office of the US Trade Representative (“USTR”) over the past six months.

Executive Summary

Since late 2023, USTR has successively reversed and dismantled longstanding US trade policy positions on cross-border data and digital trade. This includes: (1) the October 25, 2023 withdrawal of US government support for core digital trade norms at the World Trade Organization (WTO); (2) USTR withdrawal of support for similar norms in the Indo-Pacific Economic Framework (IPEF) and the Americas Partnership for Economic Prosperity (APEP); (3) USTR’s failure to identify and analyze digital trade barriers in the National Trade Estimate Report – including a 70% reduction in focus on data localization mandates – all in contravention of section 181 of the Trade Act of 1974; and (4) USTR’s failure to address cross-border data barriers that impact US persons who rely on intellectual property in the Special 301 Report – in contravention of section 182 of the Trade Act.

USTR’s systematic reversal of longstanding US digital trade policy officially withdraws US support for international trade law disciplines that promote: (1) US cross-border access to knowledge, ideas, and information from trading partners; and (2) safeguards for Americans from arbitrary, disguised, discriminatory, or unnecessary cross-border data barriers and other digital barriers adopted by foreign governments.

USTR’s effort to dismantle longstanding US digital trade policy has far-reaching implications. It:

- Undermines the [Biden-Harris Executive Order on Artificial Intelligence \(AI\)](#) and US leadership in AI, which require reliable cross-border access to information from abroad.
- Undermines other US priorities that depend upon cross-border access to information from abroad – whether to protect America’s [environment](#), [health](#), [innovation](#), [security](#), or [jobs](#).
- Contradicts White House commitments to engage in international negotiations involving “high-standard rules of the road in the digital economy, including [standards on cross-border data flows and data localization](#).”

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. GDA member companies are active in the accounting, agriculture, automotive, aerospace and aviation, biopharmaceutical, consumer goods, energy, film and television, finance, healthcare, hospitality, insurance, manufacturing, medical device, natural resources, publishing, semiconductor, software, supply chain, telecommunications, and transportation sectors. GDA member companies collectively employ millions of American workers across all 50 states. For more information, see <https://www.globaldataalliance.org>

- Contradicts the [National Security Strategy](#) call to “to promote the free flow of data and ideas with trust, while protecting our security, privacy, and human rights, and enhancing our competitiveness.”
- Contradicts the [National Cybersecurity Strategy](#) call to “rally like-minded countries, the international business community, and other stakeholders to advance our vision for the future of the Internet that promotes secure and trusted data flows, respects privacy, promotes human rights, and enables progress on broader challenges.”
- Contradicts the [International Cyberspace and Digital Policy Strategy](#), which supports the “trusted free flow of data and an open Internet with strong and effective protections for individuals’ human rights and privacy and measures to preserve governments’ abilities to enforce laws and advance policies in the public interest,” and which champions “trusted cross-border data flows by promoting data transfer mechanisms that improve interoperability between different data privacy regimes.”
- Isolates the United States from its allies and produces a (wholly avoidable and unnecessary) appearance of US alignment with [Chinese WTO negotiating positions designed to shield China’s digitally authoritarian policies from scrutiny](#). Indeed, China has for years opposed the very same digital trade disciplines that USTR has now abandoned – disciplines that the United States had drafted, in part, specifically to counteract digitally authoritarian policies. Even worse, while USTR refuses to act, [China is now working to bring US allies into its cross-border data policy orbit](#), securing China’s own cross-border data access – potentially on terms unfavorable to the United States.

Absent binding rules with allies on cross-border data, the US will face challenges protecting future:

- US cross-border access to information from abroad, as foreign governments will not be required to provide any assurances regarding future cross-border data transfers, and will face few (if any) international trade penalties for unreasonably blocking such transfers; and
- US interests from discriminatory or unfair data access conditions, as foreign governments will be free to restrict US access to information in ways that are discriminatory, unduly restrictive, or disguised barriers to trade.

USTR’s unilateral relinquishment of the opportunity to set such rules – and to advance the White House AI Executive Order’s goals – is a particularly damaging aspect of USTR’s actions.

The United States must reengage. In the Indo-Pacific Economic Framework (IPEF), the Americas Partnership for Economic Prosperity (APEP), and trade negotiations with other economies, the United States must do everything possible to reengage with its allies so as to promote the cross-border exchange of information, protect democracy and human rights, safeguard its alliances, and address tomorrow’s challenges. In the sections that follow, this memorandum offers the following observations:

1. USTR’s Actions Undermine a US-Led Coalition of Democracies that Have Sought to Oppose Digital Authoritarianism and Protectionism
2. USTR’s Actions Jeopardize US National Interests
3. USTR’s Actions Prejudice the Interests of US Enterprises and Workers
4. USTR’s Actions Do Not Appear to Meet Procedural Requirements

I. USTR's Actions Undermine a US-Led Coalition of Democracies that Have Sought to Oppose Digital Authoritarianism and Protectionism

The United States is strongest when it works with its allies. The United States must not abandon the pro-democracy, pro-economic opportunity, and pro-science digital trade disciplines that have helped it assemble a coalition of democracies across APAC, EMEA, and the Western Hemisphere to resist the challenge of digitally authoritarian policies. US government efforts included the [Department of State](#), [Department of Commerce](#), and [USTR](#) and have spanned the Bush II, Obama, Trump, and Biden-Harris Administrations, have included the following dimensions:

1. **Geopolitical.** The United States and its allies have spent decades building support for trade law disciplines that promote the cross-border exchange of ideas, knowledge, and information, while also promoting US-based norms of transparency, due process, and procedural fairness.
2. **Economic.** The United States has been a pioneer in developing these disciplines. The United States was the first country to develop binding trade disciplines that promoted the cross-border exchange of information within widely understood trade law frameworks. Subsequently, US allies negotiated their own digital economy agreements based on US model agreements.
3. **Legal.** The United States has drafted these disciplines based on US legal principles – helping ensure that US values and legal norms remain at the foundation of international economic law.
4. **Democratic.** The United States has always understood that access to knowledge and information is critical to civil and economic freedoms. The disciplines at issue serve to [protect human rights](#) and [counter digital authoritarianism](#). Consistent with the [Presidential Initiative for Democratic Renewal](#), and the [National Cybersecurity Strategy](#), and as stated in the [Declaration on the Future of the Internet](#), the US and its partners must work “to realize the benefits of data free flows with trust based on our shared values as like-minded, democratic, open and outward looking partners.”

USTR's actions – which reversed these efforts – has had the unfortunate effect of isolating the United States from its allies. It set aside a body of work developed by the United States and its allies over many years to bring greater predictability to cross-border data access and data transfers. It also produced an unfortunate appearance of US alignment with [Chinese WTO negotiating positions designed to shield China's digitally authoritarian policies from scrutiny](#).

II. USTR's Actions Jeopardize US Interests

The US national interest is harmed when foreign governments interfere with the ability of the US government to maintain reliable cross-border access to data from around the world. Because USTR's actions abandoned trade-related rules designed to promote cross-border data transfers, it makes it easier for foreign governments to impede US access to such data, which is critical to supply chain resilience, as well as US government priorities on AI, cybersecurity, health, safety, and small business.

A. USTR's Actions Undermine the Biden-Harris Executive Order on AI

The United States needs access to data from overseas to fulfill the [Executive Order](#) goal of “[lead\[ing\] the way in \[AI\] innovation and competition](#).” US leadership in AI requires deliberate policy choices that properly manage risks – including the risk that foreign governments will block US access to data needed to fulfill the Executive Order's goals.

Data lies at the core of these national interests. A lack of predictable and reliable cross-border access to data will frustrate many of the Administration's efforts on AI.

This is why USTR's actions raise such concerns: It threatens to vitiate a core foundational premise of the Executive Order – namely that the United States can count on reliable and predictable cross-border access to data that is critical to continued US leadership in AI. Without the legal certainty and due process that these trade rules on cross-border data can provide, foreign governments may now deny the United States cross-border access to data for any reason or no reason at all.

Please see the third memorandum in this series for more information.

B. USTR's Actions Undermine Other US Public Policy Priorities

US government access to cross-border data is also critical to [foreign development assistance](#); [small business promotion](#); [financial equity and inclusion](#); [cybersecurity](#); [human rights](#); [science, innovation and IP](#); [health and safety](#); [environmental protection](#); and many other [regulatory compliance](#) priorities. Many US government agencies have contended with arbitrary or unwarranted foreign government restrictions on cross-border data transfers to the United States. It is important to fully understand how US public policy priorities will be [directly undermined](#) if other countries can readily impede US cross-border access to data for reasons that are arbitrary, disguised, discriminatory, or unnecessary. Foreign cross-border data barriers have increased by [600%](#) in some regions. This is a [longstanding and growing problem that USTR's actions are likely to aggravate](#).

Please see the fourth memorandum in this series for more information.

III. USTR's Actions Prejudice the Interests of US Enterprises and Workers

USTR's actions also prejudices private sector interests. US government agencies and independent economists agree: Restrictions on cross-border access to information harm the economy, productivity, and investment – all of which threatens the [40 million American jobs supported by international trade](#). US digitally enabled services exports [exceed \\$650 billion](#) and digitally enabled goods exports are even higher. So, when foreign governments erect barriers to US digitally enabled goods and services – such as aircraft, vehicles, semiconductors, creative content, and financial and other services – they [hurt the millions of American workers who design, produce, and deliver them](#).

America's trade rules on [cross-border data are particularly important for small- and medium-sized businesses](#) (SMEs). US workers and companies of all sizes and [across sectors](#) – not “Big Tech” firms – are most vulnerable to foreign cross-border data restrictions. For example, in one recent study, 30-40% percent of SMEs surveyed said that [data localization barriers were a top challenge](#), and that with more digital connectivity, they could increase sales by 15-40% and hire 10-50 new employees each. [33.2 million](#) US SMEs employ [62 million US workers](#), accounting for [99.9%](#) of all US businesses and [63% of new jobs](#).

IV. USTR's Actions Do Not Appear to Meet Applicable Legal Requirements

Congress has [legislated safeguards](#) to ensure that USTR consults adequately with the public and all parts of the US government. USTR is obligated to consult with [the public](#), [Congress](#), [other Executive Branch agencies](#), and the [50 US states, territories and possessions](#). USTR has not met those legal requirements, and the reaction has been strong following USTR's October 25 action, its refusal to

negotiate on digital trade in IPEF and APEP, and its disregard for digital barriers in the NTE and Special 301 Reports.

V. Conclusion

Cross-border access to information is critical to advancing the shared public policy goals of the United States and its allies. Their interests are harmed when discriminatory or unnecessary barriers are erected against reliable cross-border access to information. USTR's actions make it easier for others to do so.

In the Indo-Pacific Economic Framework (IPEF), the Americas Partnership for Economic Prosperity (APEP), and trade negotiations with other economies, the United States must do everything possible to reengage with its allies so as to promote the cross-border exchange of information, protect democracy and human rights, safeguard its alliances, and address tomorrow's challenges.

EXHIBIT 19B



MEMORANDUM

Impact of USTR Digital Trade Policy Reversals on Other US Government Agency Interests

Updated May 2024

This memorandum is the fourth in a series dealing with the legal and policy implications of actions taken in 2023 and 2024 by the Office of the US Trade Representative (USTR) to [reverse longstanding US trade policy](#) positions on the cross-border movement of data and digital trade. This memorandum addresses impacts on the policy and legal interests of other US governmental agencies.

US government access to cross-border data is critical to [foreign development assistance](#), [small business promotion](#), [financial equity and inclusion](#); [cybersecurity](#), [human rights](#), [science, innovation and IP](#); [health and safety](#), [environmental protection](#), and many other [regulatory compliance](#) priorities. Many US government agencies have contended with arbitrary or unwarranted foreign government restrictions on cross-border data transfers to the United States. Allowing US allies to restrict or block US cross-border access to information on any ground – even arbitrary, discriminatory, disguised, or unnecessary grounds – hams US government interests.

For example, cross-border data transfers are important to US government priorities in contexts including:

1. **Artificial Intelligence:** Meeting the goals of the [White House](#)'s October 30 [Executive Order on Artificial Intelligence](#) (AI) for "AI research in vital areas like healthcare and climate change" depends upon securing reliable US cross-border access to high quality data in large quantities from around the world.
2. **Cyber- and Homeland Security:** Cyber-defenders at the [Department of Homeland Security](#) (DHS) and other agencies cannot protect US networks without cross-border access to global cyberthreat intelligence. Likewise, [CBP](#) depends upon cross-border digital access to international supply chain threat intelligence to interdict dangerous imports under [CTPAT](#), [IPR](#), [narcotics](#), and other border enforcement programs.
3. **Economy:** The [Department of Commerce](#), the [International Trade Administration](#), the [US Commercial Service](#), the [Small Business Administration](#), and the economic branch of the [Department of State](#) depend upon cross-border access to information regarding business, sales, and export opportunities available to US citizens. It is estimated that [40 million American jobs \(or 1 in 5 jobs\)](#) depend on international trade.
4. **Environment:** The [Department of Energy](#) and the [Environmental Protection Agency](#) (EPA) each depend upon cross-border access to satellite, meteorological, emissions, and other data from across the globe to combat climate change.
5. **Finance:** The [Department of Treasury Financial Crimes Enforcement Network](#) depends on cross-border access to financial information flows to combat terrorist financing, money laundering, corruption and fraud. The [Securities and Exchange Commission](#) and [Internal Revenue Service](#) (and other agencies) require ready cross-border access to financial information to fulfill their respective statutory functions.

6. **Foreign Policy:** The [Department of State](#) relies on cross-border data transfers for every aspect of its work in advancing US foreign policy, interests, and security abroad. This extends to the [Presidential Initiative for Democratic Renewal](#), and efforts to advance [US cyber policy](#), [human rights](#), and [foreign development assistance by USAID](#), as well as related efforts by the [US Agency for Global Media](#), [US Trade & Development Agency](#), [US Development Finance Corporation](#), and [US Export-Import Bank](#).
7. **Health & Safety:** The [Department of Health & Human Services](#) depends upon reliable cross-border access to health data in many contexts. The [Food & Drug Administration](#) needs cross-border access to pre-clinical and clinical trial data from around the world to evaluate new treatments. The [Centers for Disease Control & Prevention](#) depends upon real-time access to global epidemiological statistics and pandemic-related indicators. [National Institutes of Health](#) researchers depend on cross-border access to scientific publications and laboratory results from around the world. The [Centers for Medicare & Medicaid Services](#) depend on cross-border access to pricing data to administer Medicare and Medicaid.
8. **Innovation & IP:** The [US Patent & Trademark Office](#), [US Copyright Office](#), and [National Science Foundation](#) and other innovation and IP-focused agencies depend on cross-border access to data on inventions, creations, and R&D from abroad, including to assess prior art, registrability, and ownership of IP, as well as foundational research across the sciences.

EXHIBIT 19C



MEMORANDUM

Impact of USTR Digital Trade Policy Reversals on US Artificial Intelligence Policy

Updated May 2024

This memorandum is the third in a series dealing with the legal and policy implications of actions taken in 2023 and 2024 by the Office of the US Trade Representative (USTR) to [reverse longstanding US trade policy](#) positions on the cross-border movement of data and digital trade. This memorandum addresses impacts on US AI policy broadly, and the October 30 [White House Executive Order on Artificial Intelligence](#) specifically. USTR's action vitiates a foundational premise of the Executive Order – the reliable and predictable cross-border access by the United States to global data sources necessary to realize the benefits of AI and to deter and manage its risks.

Biden-Harris Administration trade policy should support all US government interests, including those outlined in the October 30 [AI Executive Order](#). The Biden-Harris Administration should reverse USTR's actions, or at a minimum, seek to mitigate their harmful impacts.

I. Artificial Intelligence and Cross-Border Access to Information

We offer below a few examples of the benefits that cross-border access to information offers in insights, predictions, and other outputs produced by AI machine learning:

- [Automated flight management](#) and air traffic control based on computational analysis of cross-border data, including meteorological conditions, real-time fuel consumption, aircraft operational data, nearby air traffic conditions, airport congestion, and numerous other data elements.¹
- Identification of chemical and cellular anomalies found in global data sets for [early diagnosis, prevention, and treatment](#) in the fields of oncology, autoimmune disorders, and Parkinsons and Alzheimers disease.²
- [Predictive climate modeling](#) based on computational analysis of satellite data, weather station data, topographical information, and various IoT and sensor data.³
- [Improved carbon tracking and mitigation](#) based on computational analysis of transportation logs, meter readings, fuel purchase records, atmospheric pollution tracking, and visual monitoring of power plants and other facilities, and other data sources from around the world.⁴
- Computational analysis to map vulnerable seaside areas to produce cyclone risk maps and guide investment plans for cyclone shelters, schools, health facilities, and other infrastructure for [disaster planning and survivability](#) across various countries.⁵

These are just a few of the many use studies for cross-border data in an AI context. USTR's action will better position other governments – whether economic competitors or adversaries – to block the sharing of such cross-border data for arbitrary, discriminatory, disguised, or unnecessary reasons.

II. USTR's Action Undermines the Executive Order on Artificial Intelligence

Data lies at the heart of the [AI Executive Order](#), which was developed over many months through a whole-of-government approach involving the Departments of Agriculture, Commerce, Defense, Education, Energy, Health & Human Services, Housing & Urban Development, Justice, Labor, State, Transportation, Treasury, and Veterans' Affairs, as well as other federal government offices. The [AI Executive Order](#) assigns each of these governmental departments and offices with discrete responsibilities intended to realize AI's benefits while managing its risks.

To fulfill their responsibilities under the [AI Executive Order](#), these departments and offices need cross-border access to data from around the world. This includes cross-border access to health data, climate and emissions data, agricultural and meteorological data, and other data needed – in the words of Secretary of State Antony Blinken and Secretary of Commerce Gina Raimondo – to address “[some of the world's biggest challenges](#), from curing cancer to mitigating the effects of climate change to solving global food insecurity.” It also includes cross-border access to data needed to ensure that AI is “[safe and secure](#),” including overseas data relating to biosecurity, competition, cybersecurity, human rights, labor, privacy, and other AI-related risks.

The United States' access to such data requires a stable and predictable legal framework on the cross-border movement of information – precisely the type of framework that has been under negotiation in the WTO and IPEF which USTR now refuses to negotiate. Such a framework is needed to prevent other governments from imposing cross-border data restrictions that would:

- Frustrate US government efforts to “[catalyze AI research across the United States](#)” in relation to agriculture, climate, health, or the economy.
- Impede the ability to “[test, understand, and mitigate \[AI\] risks](#),” given that large and representative data sets are a prerequisite to “robust, reliable, repeatable, and standardized evaluations of AI systems.”
- Impair the US government's capacity to conduct “[AI-related research](#) in contexts beyond United States borders”; use “AI tools to mitigate [climate change](#) risks;” to assess “AI's [labor-market](#) implications across international contexts”; and to “collect and analyze reports of AI-related [IP theft](#).”
- Undermine US government efforts to promote “[competition in AI and related technologies](#),” given that cross-border data restrictions will increase the dependence on large incumbent firms that have already compiled large AI training data sets – essentially raising barriers to entry for smaller businesses and entrepreneurs.

As noted above, USTR's unilateral withdrawal of support for standards of due process and transparency in relation to measures affecting cross-border data would countenance the imposition by foreign governments of arbitrary, discriminatory, disguised, or unnecessary barriers on US access to data needed to meet the [AI Executive Order](#)'s goals.

Recent events demonstrate that this is no hypothetical concern. For example, in November 2023, the [EU Data Act](#) was finalized. This measure contains unprecedented new restrictions on transfers of [non-personal data](#) from the EU to the United States and other jurisdictions. (See e.g., Art. 32). Then, in April 2024, the European Health Data Space (EHDS) was finalized. EHDS explicitly allows EU Member States to require localization of health data; restricts data transfers to third countries that do not provide “reciprocal” access to health data vis-à-vis the EU; and mandates localization of certain health data in certain processing scenarios, subject to some limited exceptions. The future impact of such EU transfer restrictions on US access to non-personal data could dwarf the impact of restrictions imposed by economies that are less

integrated with the United States. It is expected that the EU will introduce further barriers to transfers of data under “data spaces” involving other sectors.

Such barriers jeopardize US efforts to – in the words of [Vice President Kamala Harris](#) – fulfill AI’s “potential to do profound good”; to “ensure that everyone is able to enjoy its benefits”; and ultimately “create a safer AI future.” USTR’s unilateral withdrawal of support for a common set of international due process safeguards regarding such cross-border data barriers will only complicate the US Government’s efforts to realize the goals of the [AI Executive Order](#).

III. Conclusion

For the sake of the goals outlined of the Executive Order on Artificial Intelligence, and to protect other governmental priorities, we urge the Biden-Harris Administration to do everything possible to promote the cross-border access and exchange of information with our allies and partners around the world. At a minimum, this means preventing USTR from extending its erroneous policy reversal into other contexts, including the IPEF and the APEP.

¹ See e.g., M. Durgut, *Artificial Intelligence and Air Traffic Control*, Aviationfile.com website (Jan. 2023), at: <https://www.aviationfile.com/artificial-intelligence-and-air-traffic-control/#:~:text=One%20of%20the%20primary%20applications%20is%20to%20help,make%20informed%20decisions%20on%20routing%20and%20scheduling%20flights>; Degas et al., *A Survey on Artificial Intelligence and explainable AI in Air Traffic Management*, 12 Applied Sciences 1295 (2022), at: <https://www.mdpi.com/2076-3417/12/3/1295>; Hanneke Weitering, *How Artificial Intelligence is Transforming Aviation*, Futureflight.aero website (2023), <https://www.futureflight.aero/news-article/2023-07-13/beyond-automation-how-artificial-intelligence-transforming-aviation>

² See e.g., Hunter et al., *The Role of Artificial Intelligence in Early Cancer Diagnosis*, 14(6) Cancers 1524 (2022), <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8946688/>; Stafford et al., *A systematic review of the applications of artificial intelligence and machine learning in autoimmune diseases*, 3 NPJ - Digital Medicine 30 (2020), at: <https://www.nature.com/articles/s41746-020-0229-3>; Diogo et al., *Early diagnosis of Alzheimer’s disease using machine learning*, 14 Alzheimers Research and Theory 107 (2022), at: <https://alzres.biomedcentral.com/articles/10.1186/s13195-022-01047-y>; Ahsan et al., *Machine-Learning-Based Disease Diagnosis: A Comprehensive Review*, 10(3) Healthcare Basel 541 (2022), at: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8950225/>; Luchini et al., *Artificial Intelligence in Oncology*, 126 British J. of Cancer 1 (2022), at: <https://www.nature.com/articles/s41416-021-01633-1>; Yumar et al., *Artificial intelligence in Disease Diagnosis*, 14(7) J. Ambient Intell Humaniz Comput. 8459 (2023), at: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8754556/>

³ Schneider et al., *Harnessing AI and computing to advance climate modelling and prediction*, 13 Nature Climate Change 887 (2023), at: <https://www.nature.com/articles/s41558-023-01769-3>; World Economic Forum, *The role of machine learning in helping to save the planet* (2021), at: <https://www.weforum.org/agenda/2021/08/how-is-machine-learning-helping-us-to-create-more-sophisticated-climate-change-models/>; Kaak et al., *Aligning artificial intelligence with climate change mitigation*, 12 Nature Climate Change 518 (2022), at: <https://www.nature.com/articles/s41558-022-01377-7>; Xin et al., *Artificial Intelligence for Climate Change Risk Prediction, Adaptation, & Mitigation*, Ecological Processes (2021), at: <https://www.springeropen.com/collections/AICC>; Chantry et al., *Opportunities and challenges for machine learning in weather and climate modelling*, 379 Phil. Trans. R. Soc. 83 (2020), at: <https://doi.org/10.1098/rsta.2020.0083> (2020).

⁴ See e.g., Global Data Alliance, *Cross-Border Data Transfers & Environmental Sustainability* (2023) (internal citations omitted), at: <https://globaldataalliance.org/wp-content/uploads/2023/04/04192023gdacbdtsustainability.pdf>

⁵ See *id.*

EXHIBIT 19D

Global Data Alliance Recommendations to White House on Cross-Border Data

The Global Data Alliance respectfully offers the following recommendations on digital trade and cross-border access to information. We urge the United States to:

1. **Stand up for US allies.** The US must under no circumstances support digital authoritarianism abroad. The US withdrawal of support for longstanding international rule of law norms – even vis-à-vis our closest allies – appears to have that unfortunate and avoidable effect. This unforced error undermines US leadership of free, transparent, and competitive economies. It must not be repeated.
2. **Refrain from further actions that undermine the Rule of Law in the digital environment.** The US and its allies must refrain from treating each other in ways that are arbitrary, discriminatory, disguised, or unnecessary. These principles, which are integrated into public policy exceptions in US and allied trade agreements,¹ must be safeguarded and protected. Please do not move forward on any other basis.
3. **Decline the invitation to withdraw longstanding US support for the Rule of Law** on the basis of (inaccurate) assertions that such support would “[totally shut down](#)” governmental regulation in the public interest. This flawed argument is based on a misleading analysis of prior cases under the WTO Dispute Settlement (“DS”) System. This analysis:
 - Fails to acknowledge that WTO dispute settlement supports US allies in the face of authoritarian overreach, economic coercion, and nonmarket economy practices. Since 2021, China has faced WTO DS claims at rates that are 500% higher than Australia, Japan, Korea, Singapore, and the UK, and 150% higher than the US.
 - Ignores the precept – enshrined in US law – that WTO recommendations do not bind the US Congress or the US Executive Branch.
 - Disregards that the US is working to reform the WTO DS System. The US has blocked the appointment of new WTO Appellate Body members, given concerns that this Body had exceeded its mandate. The WTO DS system will not be revived except on terms agreed by the US.
 - Overstates the probability that any given regulatory action would be addressed – let alone successfully challenged – in WTO dispute settlement. For example, there are over 3,000 regulatory actions in the [2023 Unified Regulatory Agenda](#). In 2023, only a single (one) request for WTO consultations was filed against the US. This represents a less than 0.0003 probability that any given US regulatory act would be challenged.²
 - Diminishes and misrepresents US successes. The US has an excellent WTO litigation track record. It has historically prevailed in a large majority of the cases that it brought, while also effectively limiting the scope and impact of cases filed against it.
4. **Recognize the critical role that cross-border access to information plays in helping realize the [AI Executive Order](#)'s goals of promoting AI research, safety, and security.** Each of the 14 federal departments and agencies tasked with fulfilling discrete responsibilities under the Executive Order will only be able to do so if they have reliable access to global data sources. It undermines these goals to suggest to US allies and other trading partners that they may freely block the United States' access to cross-border data for reasons that are arbitrary, discriminatory, disguised, or unnecessary.

5. **Acknowledge that cross-border access to information and rule of law are not anticompetitive.** It has been suggested that USTR’s refusal to support rules that benefit the entire economy stems from a concern about “[a] [very small number](#) of extremely powerful and dominant companies.” Yet, there is no conflict between antitrust and rule of law or cross-border data norms. Nothing in these norms impedes new antitrust legislation or enforcement. On the contrary, restricting cross-border access to information and data transfers hurts [small businesses](#), competition and marketplace choice. And by galvanizing cross-industry opposition, this controversial approach distracts from more focused efforts to address competition concerns in the digital economy.
6. **Understand the trade provisions at issue.** Seemingly out of concerns regarding “Big Tech,” USTR abandoned a provision that protects American music, books, film, and software from nationality-based discrimination abroad. Discrimination against US cultural content has a long history, including theatrical or screen quotas, censorship, and discriminatory levies. Relinquishing this chance to tackle such discrimination will undermine the interests of [4.9 million Americans holding arts and cultural jobs](#) and [3.3 million Americans holding software jobs](#). Regrettably, a single-minded focus on a simple “Big Tech” narrative has produced unintended consequences and an appearance of indifference and disregard for other sectors.
7. **Protect all American enterprises and workers**, including those supported by trade and cross-border data. There is no place in US trade policy for the misguided view that US exports are unimportant because they contribute only 9 percent of US GDP. We reject this view. So would the [40 million](#) American workers whose jobs are supported by international trade. A truly worker-centered trade policy must respect and value [all American workers](#).

Cross-border data supports [every sector of the US economy](#), including the sectors in which GDA members are active – accounting, automotive, aerospace, consumer goods, energy, film, finance, healthcare, insurance, manufacturing, medical devices, pharmaceuticals, natural resources, publishing, semiconductor, software, supply chain, telecommunications, and transportation.

We urge you to engage in a careful, thorough, and deliberate process. Whether for purposes of IPEF, APEP, or the US-Taiwan or US-Kenya negotiations, there is no substitute for transparency, legal and procedural rigor, and the development of a substantial evidentiary basis.

¹ See [GDA Model Texts](#); See also, [USMCA](#) Arts. 19.4, 19.11-12, 19.16, [17.18-18](#); [US-Japan DTA](#), Arts. 8, 11-13, 17.

² This probability drops further when data is taken from the past 3+ years: Only one consultation request was filed against the US in 2022; none were filed against the US in 2021. Furthermore, when the entire universe of regulatory actions taken by all 160+ WTO Members since 1995 is considered, the probability falls even further that any given regulatory act would fall within the small group of 46 cases analyzed in the cited article.

EXHIBIT 19E

DIGITAL TRADE

The true cost of USTR's U-turn on data in the WTO e-commerce talks



Joseph Whitlock

SHARE     

Published 21 November 2023

The USTR's withdrawal of support for trade rules that promote cross-border information access could make it easier for others to deprive the United States and its partners of the information they need to make informed decisions and prepare for the future. By closing the door on pro-competition data regulations, USTR's action opens the door to exclusionary digital policies.

The United States Trade Representative's (USTR) October 25 **withdrawal of US support** for provisions promoting cross-border access to information in the World Trade Organization (WTO) e-commerce negotiations is a stunning policy U-turn that reverses core tenets of US foreign economic policy in place for nearly two decades. This action has the unfortunate effect of undermining US support at the WTO for Australia, Japan, Singapore, and other US allies, while also penalizing workers, consumers and businesses engaged in global e-commerce. The ramifications of the October 25 action likely exceed those of the ill-conceived US withdrawal from the Trans-Pacific Partnership.

The USTR's action overturns long-established US policy of advancing pro-democracy, pro-inclusion, and pro-

RELATED ARTICLE

science rules grounded in: (1) the cross-border exchange of knowledge, ideas, and information with US partners; and (2) the international adoption of democratic norms of transparency and due process in relation to measures affecting such cross-border data.

The USTR's action jeopardizes the interests of the United States and its allies in securing reliable cross-border access to information relating to the economy, environment, health, safety, security, science and technology, among other topics. In the absence of such trade rules, which are designed to protect against the imposition of arbitrary, discriminatory, disguised, or unnecessary barriers to information access, it becomes easier for others to deprive the United States and its partners of the information they need to make informed decisions and prepare for the future.

1. What does the October 25 reversal mean for the economies of the United States and its allies?

The USTR's withdrawal of support for trade rules that promote cross-border information access will produce significant economic costs for the United States and its US allies.

Restrictions on cross-border access to information and other digital trade barriers harm GDP (-0.7-1.7%); investment flows (-4%); productivity (4.5% loss); and small business (up to 80% higher trade costs). As the World Bank has noted, "restrictions on data flows have large negative consequences on the productivity of local companies using digital technologies and especially on trade in services." These burdens are borne most heavily by developing and least developed economies . As the United Nations has stated, "regulatory fragmentation in the digital

Integration, interoperability, inclusion: Igniting the e-commerce boom in Asia



Kati Suominen

14 November 2023

landscape...is most likely to adversely impact low-income countries, less well-off individuals, and marginalized communities the world over, as well as worsen structural discrimination against women. A future of exclusionary digital development must be avoided at all costs.”

Despite their heavy economic costs, **cross-border data restrictiveness** continues to increase. It is estimated that these restrictions increased by **600%** between 2013 and 2019 in the Asia-Pacific, and increased at a rate **five times** higher in 2022 than in 2021.

Conversely, studies also show that removing cross-border data restrictions benefits workers, consumers, and enterprises across the economy. According to the **World Bank**, “studies show that countries would gain on average about 4.5 percent in productivity if they removed their restrictive data policies.” The **Organisation for Economic Co-operation and Development** has found that a 0.1 point reduction in a country’s level of digital services trade restrictiveness is associated with a 145% increase in overall exports.

2. What does the October 25 reversal mean for digital inclusion, worker and consumer welfare, and marketplace competition?

Cross-border access to information is necessary to promote digital transformation and digital inclusion for consumers, **workers**, and enterprises of **all sizes**, at **every stage of the value chain**, and across **every sector**, including the **agriculture, automotive, clean energy, finance and insurance, healthcare and medical technology, logistics, media, pharmaceutical, and telecommunications** sectors. Digital barriers to the exchange of connected goods and services including aircraft, vehicles, semiconductors, creative content, and financial and other services also hurt the workers who **design, produce, and deliver** them, and the consumers who purchase them. In the United States, 1 in 5 jobs (**40 million jobs**) is supported by international trade, a proportion that is even higher among many of America’s closest allies.

Small businesses across all sectors are particularly vulnerable to restrictions on the cross-border access to information. For example, in one recent study conducted across markets in the 12 member states of the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP), the TPP’s successor, roughly 70% of small businesses surveyed stated that the CPTPP’s rules on data transfers and data localization were **somewhat or very beneficial** to their ability to engage in online commerce. At the same time, 30% to 40% percent of small businesses surveyed

said that fragmented and inconsistent digital policies and **data localization barriers were top challenges.**

The historical support of the United States and its allies for trade rules on cross-border access to information has helped protect the interests of those countries' consumers, workers, small businesses, and other enterprises. Digital access to market information and to new export opportunities promotes marketplace competition. Lowering barriers to knowledge and eliminating other information blind spots also reduces barriers to entry, opportunities for unfair discrimination, and undue or disguised restrictions on trade. Better information also tends to limit the risk of abusive pricing or market arbitrage practices. Ultimately, the pro-competition nature of cross-border data rules has translated into more agile and resilient supply chains, greater consumer choice, and overall increases in consumer welfare among the US and allied economies that have historically supported these rules.

USTR's policy reversal closes the door on these pro-competition and pro-inclusion digital trade rules, while opening the door to anti-competitive and exclusionary digital policies.

3. What does the USTR reversal mean for the strategic interests of the United States and its allies?

The United States is strongest when it works with its allies. The United States and its allies worked for years to develop the pro-democracy, pro-inclusion, and pro-science trade rules on cross-border data at issue here. That collaborative effort

RELATED ARTICLE

Geopolitics and the race for data supremacy



Alex Capri
05 October 2022

brought together a coalition of like-minded Pacific Rim democracies, including Australia, Canada, Chile, Japan, Mexico, Peru, Singapore, South Korea, and New Zealand – economies that recognize the role of cross-border access to information in supporting the well-being of their consumers, workers, and enterprises.

The United States and its allies have understood that access to knowledge and information is integral to civic and economic freedoms, and particularly the protection of **human rights**. The Biden-Harris administration has consistently supported this view, as reflected in the **Presidential Initiative for Democratic Renewal** and the **Declaration on the Future of the Internet** , which reflect a shared commitment among 60 economies to work “to realize the benefits of data free flows with trust based on our shared values as like-minded, democratic, open and outward looking partners.”

In this respect, US and allied support for trade rules on cross-border access to information has served as a bulwark against a rising tide of **digital authoritarianism** , which has been associated with a dizzying array of new cross-border data restrictions and localization mandates affecting not only **personal data**, but also “**important data**,” deemed to include **automotive, cultural, environmental, financial, geographic, health, business, statistical, and production process data**, and information on **scientific and technological achievements**. Similar cross-border data restrictions apply to “**core data**”, which covers data relating to the “life of the **national economy**, people’s important **livelihoods**, [and] important **public interests**”, a second broad category of “**critical infrastructure information**”, and a third category called “**key data**.”

Fortunately, longstanding allied support for trade rules on cross-border access to information has helped slow the global spread of digital authoritarianism.

Unfortunately, USTR’s action would dictate a very different policy direction. USTR’s action undermines a pillar of an Asia-Pacific digital governance strategy that the United States has invested political capital and years of effort in developing. This issue was highlighted in a November 15 **US Senate Foreign Relations Committee Hearing**, at which Senator Van Hollen (D. MD) stated:

RELATED ARTICLE

“What the USTR did at the WTO totally ... undermines the principles... of free flow of information and [of] ... resistance to data localization, which empowers authoritarian regimes.” Over 50 **Senators** and **House representatives** have raised their own concerns, as have commentators from **academia**, **civil society**, **think-tanks**, **small businesses** , **individual companies**, and some **50 international business groups** that represent thousands of companies and millions of workers worldwide.

Regulating artificial intelligence through digital trade agreements



Neha Mishra
30 August 2022

By closing the door on pro-democracy digital trade rules, USTR’s decision has opened the door to pro-authoritarian digital trade rules.

4. What does the October 25 reversal mean for the Biden-Harris administration’s priorities?

Cross-border access to information and data transfers are important to many **governmental policy objectives**. Conversely, restrictive cross-border policies hurt **developing countries** and **small businesses**; impede **financial equity and inclusion**; undermine **national security** and **cybersecurity**; threaten **human rights**; slow science and **innovation**; and impair various **health and safety**, **environmental**, and other **regulatory compliance** priorities.

For many years, the United States made support for cross-border data transfers and access to information a pillar of US government policy. With the October 25 action, the landscape has now changed – not just for USTR, but also for many other departments and agencies whose work and goals are prejudiced by its October 25 action.

The October 25 action creates new challenges for:

- US international relations, given that the October 25 action isolates the United States from its allies and produces an avoidable and unnecessary **appearance** of USTR alignment with **China’s** WTO negotiating positions – **positions intended to**

shield China's digitally authoritarian policies from WTO scrutiny. Indeed, China has for years opposed the very same digital trade disciplines that USTR abandoned on October 25, disciplines that the United States had drafted, in part, specifically to counteract the rise of digital authoritarianism.

- The White House's commitment to pursue "high-standard rules of the road in the digital economy, including standards on cross-border data flows and data localization" and similar calls in the Declaration for the Future of the Internet . It also works at cross purposes with the US-EU Data Privacy Framework and the Global Cross-Border Privacy Rules Forum, both of which are designed to promote trusted cross-border data transfers.
- The 2023 National Security Strategy and the 2023 National Cybersecurity Strategy , which recognize that cybersecurity depends on real-time cross-border access to cyberthreat indicators to identify risks and divert threats. The National Security Strategy calls on the United States "to promote the free flow of data and ideas with trust, while protecting our security, privacy, and human rights, and enhancing our competitiveness."
- Cybersecurity priorities at the Department of Homeland Security, economic priorities at the Department of Commerce, environmental priorities at the Department of Energy and Environmental Protection Agency (EPA), finance priorities at the Department of the Treasury, foreign policy priorities at the Department of State, health and safety priorities at the Department of Health & Human Services, Food and Drug Administration (FDA), and National Institute of Health (NIH); and innovation and IP priorities at the US Patent & Trademark Office and the National Science Foundation. All of these government functions depend

RELATED ARTICLE

China's quest to shape the world through standards setting



Emily de la Bruyère
13 July 2021

on cross-border access to information.

- Artificial intelligence governance priorities reflected in the 2023 **Biden-Harris Executive Order on Artificial Intelligence (AI)** that require reliable cross-border access to information from abroad. This topic is discussed in Section V below.

How was it that the USTR was able to take such a consequential action seemingly at odds with so many US governmental priorities?

It **appears** that there was a breakdown in USTR internal controls. Given the importance of cross-border data and trade policy to the US economy, Congress had **legislated safeguards** to avoid precisely this sort of outcome. These statutory safeguards aim to ensure that the USTR consults adequately with the public and all parts of the government before undertaking the sort of major policy shift that occurred here. USTR is obligated to consult with **the public, Congress, other Executive Branch agencies**, and the **50 US states, territories, and possessions**.

In this case, USTR did not consult the public at all. It also did not – according to both **Democratic** and **Republican** lawmakers – adequately consult with Congress. Nor did it – according to **Administration officials** – even consult with senior policymakers with shared responsibility over international data policy matters, who first learned of USTR’s action “in the press.” The swift reaction from all quarters and from across the political spectrum strongly suggests a legally and procedurally defective process.

5. What does the October 25 reversal mean for the development and regulation of artificial intelligence?

The October 25 action will have consequences for the **Biden-Harris administration Executive Order on AI** – the realization of which depends on having stable and predictable international rules on cross-border access to data from around the world. This includes health data, climate and emissions data, agricultural and meteorological data, and other data needed – in the words of US Secretaries Antony Blinken and Gina Raimondo – to address “**some of the world’s biggest**

challenges, from curing cancer to mitigating the effects of climate change to solving global food insecurity.” Cross-border access to larger data sets also aids the exchange of incident data for high-risk AI systems, improves AI functionality, and supports testing for bias, safety, and resiliency. USTR’s action vitiates a foundational premise of the Executive Order – reliable US and allied cross-border access to data to advance **innovation** and to evaluate, understand, and mitigate AI-related **risks**.

Data lies at the core of the **AI Executive Order**. Impediments to US and allied cross-border access to data would frustrate the administration’s aims to “**catalyze AI research**” in relation to agriculture, climate, health, or the economy. Such impediments will also undermine the ability to evaluate AI systems would undermine its ability ensure that AI is “**safe and secure**”. When such impediments result in AI data sets that are too small, it also impedes efforts to “**test, understand, and mitigate risks**” and to develop effective safeguards against “societal harms such as fraud, discrimination, bias, and disinformation,” as well those relating to the workplace, competition, and security.

USTR’s action puts US cross-border data access at risk. Among other things, it would countenance the imposition by foreign governments of arbitrary, discriminatory, disguised, or unnecessary barriers to that access. Such barriers jeopardize US efforts to – **in the words of Vice President Kamala Harris** – fulfill AI’s “potential to do profound good”; to “ensure that everyone is able to enjoy its benefits”; and ultimately “create a safer AI future.”

USTR’s unilateral relinquishment of the best chance in a generation to set cross-border data rules is a particularly costly consequence of the October 25 action. It is – at its core – a failure to

RELATED ARTICLE

Emergent digital fragmentation: The perils of unilateralism



Simon J. Evenett
28 June 2022

"recognize this moment we are in" and to seize it.

6. The path ahead

Cross-border access to information is critical to advancing the shared public policy goals of the United States and its allies. Their interests are harmed when discriminatory or unnecessary barriers are erected against reliable cross-border access to information. The October 25 action makes it easier for others to impose similar barriers, depriving the United States and its partners of operational predictability and legal certainty.

The costs and risks for the United States are considerable. In fact, USTR's fundamental error here offers an object lesson in the sort of wide-ranging damage that can result when organizations allow themselves to become unduly isolated from external sources of knowledge, ideas, and information. Extrapolating that object lesson to an entire economy – or a grouping of allied economies – illustrates how much is at stake here: Without rules that protect our cross-border access to information, we face real dangers from knowledge deficits that compromise our ability to make informed decisions and develop effective, evidence-based responses to urgent economic, environmental, health, safety, and security challenges.

The Biden-Harris administration should not allow USTR to repeat the negotiating errors it committed at the WTO. In the Indo-Pacific Economic Framework (IPEF), the Americas Partnership for Economic Prosperity (APEP), and trade negotiations with other economies, the United States must do everything possible to reengage with its allies so as to promote the cross-border exchange of information, protect democracy and human rights, safeguard its alliances, and address tomorrow's challenges.

[Joseph Whitlock is the Executive Director of the [Global Data Alliance](#). The views expressed herein are those of the author and do not necessarily represent the views of the Alliance.]

EXHIBIT 20



September 25, 2023

Office of the US Trade Representative
600 17th Street, NW
Washington DC 20508
Attn: Megan Paster (InclusiveTrade@USTR.EOP.GOV)

**Re: Request for Comments on Advancing Inclusive, Worker-Centered Trade Policy
(Docket Number USTR–2023–0004)**

The Global Data Alliance (GDA)¹ appreciates the opportunity to provide views in response to the Request for Comments on Advancing Inclusive, Worker-Centered Trade Policy issued by the Office of the US Trade Representative on June 12, 2023.

The GDA respectfully submits that the United States should advance a worker-centric digital trade policy that can grow well-paid jobs at home and that fosters strategic re-engagement with key allies, including with trading partners across the Americas, APAC, and EMEA, so as to counter digital protectionism and digital authoritarianism.

The Administration can achieve these goals through a worker-centric digital trade policy that recognizes the critical role that cross-border data transfers and cross-border access to knowledge and digital tools play in protecting and promoting: (A) small businesses, (B) workers, (C) human rights, (D) economic opportunity in the developing world, and (E) digital inclusion, privacy, cybersecurity, anti-corruption, rule of law, and other policy priorities in the developing world.

We address each of these elements below.

A. Cross-Border Data Transfers & Small Business

Cross-border data transfers can help small businesses by: (1) increasing access to digital knowledge resources and overseas markets and leveling the playing field vis-à-vis larger enterprises; (2) offering a “digital dividend” that can be enjoyed by millions of small businesses globally; (3) allowing small businesses to use cross-border digital tools to seize economic opportunity with agility; and (4) reducing digital barriers that disproportionately impact small businesses.²

- **Data Transfers & Leveling the Playing Field for Small Business:** Small businesses face knowledge and access barriers that larger enterprises can more easily overcome. Data transfers and cross-border access to technology and markets help level the playing field. As the OECD has explained, “cross-border data flows are especially important for [small businesses] ... Better and faster access to critical knowledge and information also helps small businesses overcome informational disadvantages, notably with respect to larger firms, reducing barriers to engaging in

international trade and allowing them more readily to compete with larger firms.” One recent study estimates that digital tools helped small businesses reduce export costs by 82 percent and transaction times by 29 percent. Data localization and transfer restrictions make it harder to achieve these benefits, in part because they produce “a fragmented Internet [that] reduces market opportunities for domestic [small businesses] to reach worldwide markets, which may instead be confined to some local or regional markets.”

- **Data Transfers & Digital Economic Dividends for Small Business:** Small businesses are particularly well positioned to reap the economic benefits that a reliable framework for data transfers and cross-border access to markets and digital tools can provide. These benefits can also be widely disseminated and shared across populations. For example, in the United States, 32.5 million small businesses account for:
 - 99.9% of all US businesses, 48% of all US workers (61.2 million workers), and 90% of all US business openings (909,808 new openings and 9.1 million new jobs in 2019-2020);
 - 95% of all US exporting enterprises, with small business exports accounting for roughly 25% of all US exports and supporting over 6 million jobs (in 2017).
- **Data Transfers & Small Business Digital Agility:** Many small businesses demonstrate a greater degree of digital business agility than larger enterprises. Studies have found that, while 95% of small businesses were negatively impacted by the COVID-19 pandemic, the pandemic also caused 70% of small businesses to accelerate efforts to become more digitally competitive. The most digitally progressive SMEs are growing 8 times faster than the least progressive. Studies have also found that small businesses with a strong digital presence grow twice as fast, and are 50% more likely to sell outside their region, relative to those with little or no digital presence. In a recent CSIS study, 65% of small business surveyed said that they moved data across borders, with even higher percentages for those that export.
- **Data Transfers & the Disproportionate Impact of Digital Restrictions on Small Business:** Unfortunately, the number and variety of digital trade barriers affecting small businesses has increased in recent years, and today include data localization mandates; unnecessary data transfer restrictions; customs duties on electronic transmissions; or other discriminatory digital measures. These types of digital barriers fall particularly heavily on small businesses, which lack the resources that larger companies can draw upon to comply with onerous mandates. In a recent CSIS study, small businesses highlighted divergent data privacy rules (40-60% of SME survey respondents) and data localization rules (30-40% of SME respondents) as key challenges. Conversely, with greater foreign market access, small businesses estimate that they could increase sales by 15-40% and hire between 10-50 new employees each.

B. Cross-Border Data Transfers & the US Workforce

A forward-looking cross-border data policy can offer the US workforce a digital dividend of economic opportunity.³ Cross-border access to knowledge, digital training, and technology solutions can help workers upgrade their skills and the ability to support advanced manufacturing and services jobs. Workers also benefit when foreign markets offer cross-border digital access to the digitally enabled products and services that those workers produce.

In the United States, for example, jobs that depend on data transfers are growing rapidly, with:

- 67 percent of new US science, technology, engineering, and mathematics (STEM) jobs in computing and software;
- Nearly 16 million workers employed in software jobs in the United States, and more than 1 million such positions remaining open to applicants;

- 40 percent of US manufacturers urging additional upskilling for advanced manufacturing positions; and
- Numerous digital training opportunities available across all 50 US states, the private sector, community colleges, vocational schools, and apprenticeship programs.
- Dual growth in demand and available training opportunities. US advanced manufacturing jobs are growing in software engineering, computer-aided design and manufacturing (CAD/CAM), industrial machinery mechanics, and Computer Numerical Control (CNC) machinery operations.
- US workers across all export-intensive sectors earning an average 15 percent more than workers in other sectors. The highest export pay premium (19 percent) goes to workers in digitally-skilled and export-intensive manufacturing sectors.

Unfortunately, this digital dividend isn't guaranteed. For example, when other countries erect barriers to digitally enabled goods and services, they hurt the workers that design, produce, and deliver them. By some reports, digital trade barriers have [increased by more than 800 percent since the late 1990s](#). Such barriers—which may take the form of cross-border data restrictions or data localization mandates—hurt workers and impede foreign market access for US exports of aircraft, vehicles, and other connected devices, as well as US worker-delivered services that depend upon internet-, wireless-, and satellite-based communications and other IoT functionality for their sales, operations, and support.

C. Cross-Border Data Transfers & Human Rights

Promoting human rights through trade is a core aspect of an inclusive, worker-centric trade policy. This aspect of US trade policy is important at a time when a growing number of trading partners are being persuaded to deploy digital technologies in a manner that undermines privacy, civil liberties, and core human rights.⁴

One reason why authoritarian regimes have so vigorously adopted and promoted cross-border data barriers is that cross-border access to knowledge, information, and data play a critical role in challenging authoritarian disinformation and social control. This issue has been analyzed in a report by Freedom House.⁵ The report states that:

In at least 23 countries covered by Freedom the Net, laws that limit where and how personal data can flow were proposed or passed during the coverage period....The transfer of data across jurisdictions is central to the functioning of the global internet and benefits ordinary users, including by improving internet speeds, enabling companies to provide critical services worldwide, and allowing the storage of records in the most secure data centers available....[S]ome [countries] have buried problematic obligations that either mandate domestic data storage, feature blanket exceptions for national security or state actors without safeguards, or delegate increased decision-making power to politicized regulators—all of which renders users vulnerable to government abuse despite improvements pertaining to the use of personal data for commercial purposes. Such contradictory “data washing” measures ultimately fail to strengthen privacy and further fragment the internet....

Cross-border data can help promote human rights and access to content and viewpoints without undue interference or distortion from authoritarian regimes.

D. Cross-Border Data Transfers & Economic Opportunity in Developing Countries

Cross-border access to knowledge, information, and digital tools is also critical to the promotion of economic opportunity across the developing world. Those developing countries that emulate cross-border data policies promoted by authoritarian regimes will suffer harmful economic impacts multiply. USTR should not sit idly by, allowing this to happen.

- **Impact on Economic Development:** The World Bank's 2020 *World Development Report* found that, "restrictions on data flows have large negative consequences on the productivity of local companies using digital technologies... Countries would gain on average about 4.5 percent in productivity if they removed their restrictive data policies, whereas the benefits of reducing data restrictions on trade in services would on average be about 5 percent."⁶ Self-isolating digital trade restrictions hinder economic development, reduce productivity, deprive local enterprises of commercial opportunities, and depress export competitiveness.⁷ Such measures are estimated to reduce GDP by up to 1.7 percent in some implementing countries.⁸
- **Impact on Developing Country Agriculture, Manufacturing, and Other Industries:** Digital trade restrictions are damaging to industries, including agriculture, which accounts for up to 25 percent of GDP and 65 percent of the lower income population in some developing countries.⁹ 75% of the value of cross-border data transfers is reported to accrue to industries including agriculture and manufacturing.¹⁰ Digital trade and cross-border access to technology and information help small-scale agricultural producers improve crop yields; mitigate crop risks (including losses from pests, disease, and weather-related events); reduce arbitrage by middlemen (up to 70 percent of smallholder production value is captured by intermediaries); and promote sustainability (agriculture accounts for 70 percent of water use, while one third of global food production is either lost or wasted).¹¹ Digital trade restrictions undermine those potential gains.
- **Impact on Developing Country Services Sectors:** The World Bank 2021 *World Development Report* has noted that measures that "restrict cross-border data flows ... [may] materially affect a country's competitive edge in the burgeoning trade of data-enabled services."¹² A 2020 World Economic Forum study found that, "approximately half of cross-border [services] trade is enabled by digital connectivity[, which] ... has allowed developing countries and micro, small and medium-sized enterprises (MSMEs) to export through greater visibility, easier market access and less costly distribution. ... Developing countries ... accounted for 29.7% of services exports in 2019."¹³
- **Impact on Developing Country Financial Inclusion:** There remain over 2.5 billion unbanked people worldwide, many living in remote locations lacking physical banking infrastructure.¹⁴ Technologies that leverage data transfers are powerful tools to increase access – particularly as 95% of the world's population is already covered by mobile broadband networks.¹⁵ USAID estimates that, by enabling digital financial services, the GDP of emerging economies could increase by more than \$3.5 trillion, or 6 percent, by 2025, and that e-commerce could increase international trade by up to \$2.1 trillion by 2030.¹⁶
- **Impact on Developing Country Global Market Access:** Digital trade and data transfers are also critical to reducing the costs of reaching markets outside of the developing world.¹⁷ One recent study estimates that digital tools helped MSMEs across Asia reduce export costs by 82% and transaction times by 29%.¹⁸ Cross-border access to e-commerce platforms, purchasers, suppliers, and other commercial partners allows local MSMEs to engage in international transactions and create jobs at home.¹⁹ Digital trade restrictions make it harder to achieve these benefits.²⁰

- **Impact on Developing Country IoT Deployment:** A 2021 GSMA study conducted in three developing regions (in South America, South-East Asia and Africa) indicates that data localization measures on Internet of Things (IoT) applications and Machine-to-Machine (M2M) data could result in:
 - Loss of 59-68% of their productivity and revenue gains;
 - Investment losses ranging from \$4-5 billion;
 - Job losses ranging from 182,000-372,000 jobs.²¹
- **Impact on Developing Country Productivity:** Local enterprises rely on digital trade and data transfers to increase productivity, drive quality, and improve output in other ways.²² To foster an environment that supports the design, production, and sale of products and services for domestic and export sales, it is important to increase the availability of IT products and services, and safeguard the ability to receive and transmit information across regional and global IT networks.
- **Impact of Internet Balkanization on Developing Countries:** Digital policies that advantage the world's largest protected market and authoritarian regime do not benefit many developing countries. Unfortunately, some developing countries have been persuaded to emulate this policy approach. In Africa and South Asia, for example, some developing countries are erecting unnecessary and costly digital trade barriers vis-à-vis one another.²³ These measures undermine the effectiveness of US development assistance and impair the ability of developing countries to realize economies of scale and specialization through larger regional markets.

E. Cross-Border Data Transfers & Cybersecurity, Privacy, Inclusiveness, Health, and Other Key Policy Objectives in Developing Countries

Digital trade restrictions undermine public policy goals relating to cybersecurity, privacy, inclusiveness, health and other policy objectives across the developing world. We address these topics below.

- **Impact on Cybersecurity in Developing Countries:** China's CSL advances the premise that that cross-border data restrictions and other forms of digital protectionism are necessary to ensure cybersecurity. However, *how* data is protected is more important to security than *where* it is stored, and transfer restrictions often result in *weaker*, not *stronger*, cybersecurity. Cross-border data transfers help improve cybersecurity because these transfers allow for cybersecurity tools to monitor traffic patterns, identify anomalies, and divert potential threats in ways that depend on global access to real-time data. Adopting rules that emulate the CSL, which mandates data localization and restricts the ability to transfer and analyze data in real-time, creates unintended vulnerabilities.²⁴
- **Impact on Privacy in Developing Countries:** China's Personal Information Protection Law (PIPL) and similar measures adopted by some developing countries advance the premise that digital protectionism is necessary to protect privacy. Yet, the PIPL and its progeny have not seemingly increased personal information protection or governmental respect for the privacy of personal communications. In fact, *how* organizations protect personal information is more important to privacy than *where* the information is stored. Organizations with operations abroad typically implement procedures to ensure that personal information is protected even when transferred outside of the country. To that end, organizations often rely on internationally recognized privacy best practices and an array of approved data transfer mechanisms.²⁵
- **Impact on Inclusiveness in Developing Countries:** Numerous organizations have underscored the importance of access to technology and digital trade, among other digital policy measures, to address inclusiveness challenges.²⁶ UN Sustainable Development Goal No. 5.b sets a goal of "enhance[ing] the use of enabling technology, in particular information and communications technology, to promote the empowerment of women." According to the World Economic Forum, "despite having less access to technology, women use digital platforms to their advantage..."

[F]our out of five small businesses engaged in cross-border e-commerce are women-owned, while just one in five firms engaged in offline trade is headed by women.”²⁷ Digital trade restrictions promoted undermine these economic opportunities. As noted in congressional reports, similar restrictions have been misused to target racial, ethnic, religious, and other communities in some countries.²⁸

- **Impact on Healthcare in Developing Countries:** Digital trade and data transfers also aid in the delivery of remote health services for medically underserved populations and the search for medical treatments. Cross-border access to data and cloud-enabled technologies enable online healthcare education efforts and cross-border humanitarian assistance;²⁹ cross-border access to clinical testing to address not only globally prevalent, but also rare and neglected diseases; and consultations between remote providers in one country with specialists located at research facilities abroad. Cross-border consolidation of anonymized data sets from around the world also allows for real-time statistical tracking, analytics, and monitoring of aggregated anonymized data—resulting in a better grasp and more rapid response to emerging epidemics or localized disease outbreaks.³⁰
- **Impact on Regulatory Compliance in Developing Countries:** Data transfers are critical to support various regulatory compliance functions. As US financial regulators have noted “data localization requirements can increase ... operational risks, hinder risk management and compliance, and inhibit financial regulatory and supervisory access to information.”³¹ Likewise, data transfers are critical to other public policy priorities, including financial fraud monitoring and prevention; anti-money laundering; anti-corruption; and other legal compliance objectives.
- **Impact on Innovation in Developing Countries:** Some claim that digital trade barriers and data transfer restrictions promote innovation. On the contrary, innovation in developing countries benefits from an increase – not a decrease – in cross-border access to technology, ICT connectivity, and digital trade. The UN Sustainable Development Goals 9.b and 9.c stress support for “domestic technology development, research and innovation in developing countries, including by ensuring a conducive policy environment for, inter alia, industrial diversification and value addition to commodities,” as well as “increasing access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries.” Digital trade barriers undermine innovation—from accessing global scientific and technical research databases, to engaging in cross-border research and development (R&D), to securing regulatory product approvals for new products and services.³²

Conclusion

We welcome the opportunity to provide these comments. Please let us know if you have any questions or comments.

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/downloads/aboutgda.pdf>

² Relevant references include the following: AlphaBeta, *MicroRevolution: The New Stakeholders of Trade in APAC* (2019), <https://alphabeta.com/our-research/micro-revolution-the-new-stakeholders-of-trade-in-apac/>; Asia-Pacific Economic Cooperation, *Small and Medium Enterprises* (2022), <https://www.apec.org/groups/som-steering-committee->

[on-economic-and-technical-cooperation/working-groups/small-and-medium-enterprises](#); eBay, *United States Small Online Business Report: eBay Boosts Small Business Resiliency During the Pandemic* (May 2021), <https://www.ebaymainstreet.com/sites/default/files/policy-papers/2021%20Small%20Online%20Business%20Report.pdf>. (A 2019 survey of US-based SMEs shows that 96 percent of eBay-enabled SMEs exported to an average of 16 different markets, whereas 0.9 percent (less than 1 percent) of other businesses exported to an average of four markets. Furthermore, eBay-enabled SMEs across the United States averaged 16 different export markets.); Federal Reserve Banks, *Small Business Credit Survey: 2021 Report on Employer Firms* (2021), <https://www.fedsmallbusiness.org/medialibrary/FedSmallBusiness/files/2021/2021-sbcs-employer-firms-report>; Goodman, Matthew P. and William Reinsch, *Filling in the Indo-Pacific Economic Framework*, Center for Strategic and International Studies (2022), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220126_Goodman_Indo_Pacific_Framework.pdf?eeGvHW0ue_Kn118U5mhopSjLs7DfJMaN; IDC, *2020 Small Business Digital Transformation: A Snapshot of Eight of the World's Leading Markets* (2020), https://www.cisco.com/c/dam/en_us/solutions/small-business/resource-center/small-business-digital-transformation.pdf; Organisation for Economic Co-operation and Development, *Mapping Approaches to Data and Data Flows* (2020), <http://www.oecd.org/trade/documents/mapping-approaches-to-data-and-data-flows.pdf>; Organisation for Economic Co-operation and Development, *Enhancing SMEs' Resilience through Digitalisation: The Case of Korea* (2021), https://www.oecd-ilibrary.org/economics/enhancing-smes-resilience-through-digitalisation_23bd7a26-en; Organisation for Economic Co-operation and Development, *SME Digitalisation to Build Back Better*, Digital for SMEs (D4SME) Policy Paper (2021), https://www.oecd-ilibrary.org/economics/sme-digitalisation-to-build-back-better_50193089-en; Suominen, Kati, *What Do CPTPP Member Country Businesses Think about the CPTPP*, Center for Strategic and International Studies (2021), <https://www.csis.org/analysis/what-do-cptpp-member-country-businesses-think-about-cptpp>. (For SMEs engaged in online sales, the most important digital economy provisions were those that (1) ensured that companies can move customer data across borders; (2) permitted companies to choose where to store their data; (3) prohibited digital customs duties; and (4) protected consumers from harmful practices, such as spam.); Urata, Shujiro, *How Can Asia Reignite Its SME Growth Engine through Trade?* (2021), <https://development.asia/explainer/how-can-asia-reignite-its-sme-growth-engine-through-trade>; US Census Bureau, *Preliminary Profile of US Exporting Companies, 2022* (November 4, 2021), <https://www.census.gov/foreign-trade/Press-Release/edb/2019/2019prelimprofile.pdf>; US Chamber of Commerce, *Growing Small Business Exports: How Technology Strengthens American Trade* (2021), https://www.uschamber.com/assets/archived/images/ctec_googlereport_v7-digital-opt.pdf; US International Trade Commission, *Digital Trade in the US and Global Economies (Part 2)* (2014), <https://www.usitc.gov/publications/332/pub4485.pdf>.

³ Relevant references include the following: BSA | The Software Alliance, *Advancing a Jobs-Centric Digital Trade Policy* (2021), <https://www.bsa.org/files/policy-filings/11132021jobscentricdigitrade.pdf>; BSA | The Software Alliance, *BSA Workforce Agenda* (2019), <https://www.bsa.org/policy-filings/innovation-competitiveness-opportunity-a-policy-agenda-to-build-tomorrows-workforce>; Congressional Research Service, *Digital Trade and US Trade Policy* (2021), <https://sgp.fas.org/crs/misc/R44565.pdf>; International Trade Administration, *COVID-19 Economic Recovery: An Important Moment Arrives for U.S. Exporters* (May 2021), <https://blog.trade.gov/2021/05/19/covid-19-economic-recovery-an-important-moment-arrives-for-u-s-exporters/#:~:text=Additionally%2C%20export-intensive%20industries%20pay%20more%2C%20on%20average%2C%20than.who%20work%20in%20manufacturing%20industries%20that%20don%E2%80%99t%20export>; Software.org, *Every Sector Is a Software Sector—Manufacturing* (2019), https://software.org/wp-content/uploads/Every_Sector_Software_Manufacturing.pdf; Software.org, *Supporting US Through COVID* (2021), <https://software.org/wp-content/uploads/2021SoftwareJobs.pdf>; Transform Your Trade website (2022), <https://transformyourtrade.org>.

⁴ Senate Foreign Relations Committee – Minority Staff Report, *The New Big Brother – China and Digital Authoritarianism*, pp. 6, (July 21, 2020) (hereinafter “Democratic Staff SFR Report”), at: <https://www.foreign.senate.gov/imo/media/doc/2020%20SFR%20Minority%20Staff%20Report%20-%20The%20New%20Big%20Brother%20-%20China%20and%20Digital%20Authoritarianism.pdf>; House Ways & Means Committee – Minority Staff Report, *China Task Force Report*, p. 4 (Sept. 2020) (hereinafter “Republican Staff HWM Report”), at https://republicans-waysandmeansforms.house.gov/uploadedfiles/china_task_force_report.pdf; US-China Economic and Security Review Commission, *2020 Report to Congress*, pp. 88, 96, 100, 110-111, (Dec. 2020) (hereinafter “USCC 2020 Report to Congress”), at: https://www.uscc.gov/sites/default/files/2020-12/2020_Annual_Report_to_Congress.pdf As USAID has stated, “[m]any governments choose to adopt protectionist digital trade policies (e.g., data-localization, forced transfer of technology, the use of standards that favor domestic

industry...). These policies, when combined with inefficient cross-border trade processes ..., impair trade that contributes to economic growth." See USAID Digital Strategy, at p. 19.

⁵ Freedom House, *Countering an Authoritarian Overhaul of the Internet* (2022),

<https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet>

⁶ World Bank, *World Development Report* (2020), at: <https://www.worldbank.org/en/publication/wdr2020>

⁷ See e.g., Ferracane et al., *The Costs of Data Protectionism*, VOX (2018); Ferracane et al., *Do Data Policy Restrictions Impact the Productivity Performance of Firms and Industries?* ECIPE Digital Trade Estimates Working Paper No. 1 (2019); Lund et al., *Defending Digital Globalization*, McKinsey Global Institute (2017). Access to foreign markets, innovation, education, and economic growth are all jeopardized by governmental measures that: (1) block cross-border access to information; (2) interfere with the circulation of technology, knowledge, and commercial data; (3) restrict connectivity to the Internet; (4) deny MSMEs and other local enterprises or citizens opportunities to engage with the technologies they need to engage with the economy. See <https://hbr.org/2017/07/60-countries-digital-competitiveness-indexed>

⁸ See Lee-Makiyama et al., *The Costs of Data Localization*, ECIPE Occasional Paper (2014), at: https://ecipe.org/wp-content/uploads/2014/12/OCC32014_1.pdf

⁹ World Bank, *Agriculture and Food* (2020), <https://www.worldbank.org/en/topic/agriculture/overview>

¹⁰ See Global Data Alliance, *The Cross-Border Movement of Data: Creating Jobs and Trust Across Borders in Every Sector* (2020), at [https://www.globaldataalliance.org/downloads/\[\]everysector.pdf](https://www.globaldataalliance.org/downloads/[]everysector.pdf) ; See Global Data Alliance, *Jobs in All Sectors Depend Upon Data Flows* (2020), at [https://www.globaldataalliance.org/downloads/infographic\[\].pdf](https://www.globaldataalliance.org/downloads/infographic[].pdf); Global Data Alliance, *Cross-Border Data Transfers Facts and Figures* (2020), at [https://www.globaldataalliance.org/downloads/\[\]factsandfigures.pdf](https://www.globaldataalliance.org/downloads/[]factsandfigures.pdf)

¹¹ See e.g., Global Data Alliance, *Access to Global Markets, Innovation, Finance, Food, and Healthcare* (2021); Every Sector Is a Software Sector: Agriculture, https://software.org/wp-content/uploads/Every_Sector_Software_Agriculture.pdf; World Bank, *Agriculture and Food* (2020), <https://www.worldbank.org/en/topic/agriculture/overview>; IDB Climate Smart Agriculture, *Thematic Paper: Climate-Smart Agriculture* (Revised Version), p. 5, <http://www.iadb.org/document.cfm?id=EZSHARE-1914875107-52>. The IDB explains the underlying challenge that cross-border access to technologies and export markets can help ameliorate: "Smallholders typically capture a low share of the final value of its products and encounter non-transparent commercialization markets and difficulties in buying inputs and selling their products at fair prices. On top of that, small farm holders typically face limited access to export to new markets and unfavorable prices in international trade, and they are particularly vulnerable to volatility in commodity prices."

¹² World Bank, *World Development Report – Data For Better Lives* (2021), at: <https://openknowledge.worldbank.org/bitstream/handle/10986/35218/9781464816000.pdf>

¹³ World Economic Forum, *Paths Towards Free and Trusted Data Flows* (2020).

¹⁴ USAID, US Global Development Lab website, available at: <https://www.usaid.gov/digital-development/digital-finance>

¹⁵ Ericsson. 2019. "Ericsson Mobility Report November 2019."

<https://www.ericsson.com/en/mobility-report/reports/november-2019>

¹⁶ USAID Digital Strategy, p. 9; see also See Global Data Alliance, *Access to Global Markets, Innovation, Finance, Food, and Healthcare* (2021).

¹⁷ Global Data Alliance, *Cross-Border Data Transfers and Supply Chain Management* (2021), at [https://globaldataalliance.org/downloads/03182021\[\]primersupplychain.pdf](https://globaldataalliance.org/downloads/03182021[]primersupplychain.pdf)

¹⁸ Micro-Revolution: The New Stakeholders of Trade in APAC, Alphabet, 2019. Likewise, the Asia Development Bank Institute estimates that electronic commerce platforms, which operate on the basis of cross-border data transfers, have helped some local firms reduce the cost of distance in trade by 60%. Asia Development Bank Institute, *The Development Dimension of E-Commerce in Asia: Opportunities and Challenges* (2016), at: <https://www.adb.org/sites/default/files/publication/185050/adb-pb2016-2.pdf>

¹⁹ USAID Digital Strategy, p. 37. As USAID has explained, "[d]igital ecosystems have the potential to equip informal merchants, women entrepreneurs, smallholder farmers, and MSMEs engaged in cross-border trade with access to markets, information, and finance. These diverse users require trustworthy services that reflect their needs. ... [D]igital trade that spans borders depends on free data flows, digitized customs, and innovations in trade finance made possible by new approaches to lending."

²⁰ See Global Data Alliance, *Access to Global Markets, Innovation, Finance, Food, and Healthcare* (2021).

²¹ GSMA, [Cross-border Data Flows – The Impact of Localization on IOT](#) (2021).

²² Data localization mandates and unnecessary data transfer restrictions hurt local innovation because a country that limits cross-border data transfers limits its own industries' access to technologies and data sources that are critical to growth and innovation, business operations, and the transfer of technology. These include: (a) productivity-enhancing software solutions; (b) scientific, research, and other publications; and (c) manufacturing data, blueprints, and other operational information. Faced with higher software costs and an unpredictable environment for R&D investments, local industries face challenges keeping technological pace with foreign competitors — threatening both domestic and export market sales. Furthermore, as data restrictions place an undue burden on industries operating in countries imposing them, they also undermine those countries' attractiveness as a destination for investment and R&D.

²³ See e.g., USTR, *2021 National Trade Estimate Report on Foreign Trade Barriers* (March 2021), at:

<https://ustr.gov/sites/default/files/files/reports/2021/2021NTE.pdf>

²⁴ Global Data Alliance, *Cross-Border Data Transfers and Data Localization* (2020), at

<https://www.globaldataalliance.org/downloads/02112020GDACrossborderdata.pdf>

²⁵ These data transfer mechanisms may include adequacy decisions, certifications, codes of conduct, Binding Corporate Rules (BCRs), and Standard Contractual Clauses (SCCs) that contain built-in data protection safeguards.

²⁶ UNCTAD, *Digital trade facilitation for women cross-border traders* (2020), at: <https://unctad.org/news/digital-trade-facilitation-women-cross-border-traders>;

E-Trade for Women Website (2019), at: <https://etradeforall.org/et4women/>;

United Nations Rwanda, *Closing the Gender Digital Divide - Boosting Africa's Economy* (2019), at

<https://rwanda.un.org/index.php/en/7153-closing-gender-digital-divide-boosting-africas-digital-economy> ("According to

the World Bank, a 10% increase in digital penetration could result in over 1% increase in GDP, while closing the gender digital divide could add up to 140 million USD per year to the mobile industry for the next 5 years.");

UNESCO, *Overcoming the Digital Divide - Understanding ICTs and Their Potential for the Empowerment of Women*

(2003), at: <http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/SHS/pdf/Overcoming-Gender-Digital-Divide.pdf>;

OECD, *Bridging the Digital Gender Divide* (2018), at: <https://www.oecd.org/digital/bridging-the-digital-gender-divide.pdf>;

See also, Global Innovation Forum, *How women are leveraging digitally-enabled networks and how governments can help through COVID-19* (2020), at: <https://globalinnovationforum.com/wp-content/uploads/2020/06/2020-06-19-Power-of-a-Global-Network-Final-reduced-size-for-web.pdf>

²⁷ See World Economic Forum, *E-commerce is Globalization's Shot at Equality* (2021), at:

<https://www.weforum.org/agenda/2020/01/e-commerce-sme-globalization-equality-women/> (citing statistics showing that, in Indonesia, women involved in online commerce generate more revenue than that contributed by those in traditional commerce, and that one in three Middle East start-ups is female-founded.)

²⁸ See *supra*, Democratic SFR Staff Report; Republican HWM Staff Report; USAID Digital Strategy; USCC 2020 Report to Congress.

²⁹ World Health Organization, *Long-Running Telemedicine Networks Delivering Humanitarian Services*, Bulletin of the World Health Organization (2012), <https://www.who.int/bulletin/volumes/90/5/11-099143.pdf>

³⁰ See Global Data Alliance, *Access to Global Markets, Innovation, Finance, Food, and Healthcare* (2021);

Global Data Alliance, *Cross-Border Data Transfers and Innovation* (2021), at

<https://globaldataalliance.org/downloads/04012021cbdtinnovation.pdf>;

Global Data Alliance, *Cross-Border Data Transfers and Remote Health Services* (2020), at

<https://globaldataalliance.org/downloads/09152020cbdtremotehealth.pdf>

³¹ See e.g., United States-Singapore Joint Statement on Financial Services Data Connectivity, at:

<https://www.mas.gov.sg/news/media-releases/2020/united-states-singapore-joint-statement-on-financial-services-data-connectivity>;

³² See Global Data Alliance, *Cross-Border Data Transfers and Innovation* (2021), at

<https://globaldataalliance.org/downloads/04012021cbdtinnovation.pdf>