WRITTEN TESTIMONY of Nigel Cory

Director, Digital, Technology, and Trade Policy

Crowell Global Advisors

before the

U.S. House Committee on Ways and Means, Subcommittee on Trade

concerning

"Maintaining American Innovation and Technology Leadership"

January 13th, 2026

the Committee on Ways and Means Hearing Room, 1100

Longworth House Office Building in Washington, DC

Thank you to Chairman Smith, Ranking Member Sanchez, and members of the committee for this opportunity to testify on "Maintaining American Innovation and Technology Leadership."

The United States' global leadership in digital trade—the cross-border transfer of data, products, or services by electronic means—is a direct input into American innovation. When U.S. firms can scale digital exports—software, cloud-enabled services, digitally delivered professional services, and intellectual property (IP)-licensing—via foreign market access they expand the revenue base that funds private research and development (R&D), support high-wage jobs, and sustain the venture and capital markets that turn research into commercial products. Digital products and services have high fixed costs and low marginal costs, so U.S. firms rely on the ability scale across global markets via the Internet and associated digital technologies.

Conversely, when trading partners restrict cross-border data flows, discriminate against foreign digital services suppliers, or weaken IP protections, they reduce market access and scale, depress expected returns, increase uncertainty, costs, and complexity, and shrink the pool of private capital available to reinvest in next-generation innovation. Digital trade barriers essentially operate like a tax on scale and an uncertainty shock to investment. Even where the first-order effect appears as "compliance cost," the second-order effect is innovation: smaller addressable markets and higher fixed costs reduce returns to R&D, especially for data-intensive and cloud-enabled products whose economics depend on global scale. The impact of digital trade barriers compounds as U.S. firms must simultaneously comply with an ever-growing number of problematic digital regulations in key markets.

Digital trade barriers impact U.S. innovation in several other ways:

- Data as an input to innovation, especially for AI: Cross-border data flows support model training, product improvement, and resilience.[1] When governments force localization or constrain transfers, they often reduce data quality and variety and slow iteration cycles—directly degrading the pace and quality of innovation. When data must be segmented by jurisdiction, firms lose the "learning at scale" that drives quality improvements and rapid iteration. Digital trade restrictions (e.g. local processing mandates, duplicative certification, and local infrastructure requirements) raise unit costs and reduce the number of product iterations firms can afford, especially for AI and data-intensive testing.

- Data is a critical enabler of cybersecurity: Digital trade openness supports cross-border threat intelligence, fraud detection, and rapid incident response. Localization and restrictive transfer regimes can impede global security operations, increasing downtime and risk. This diverts engineering resources from innovation to compliance and remediation. Academic analysis shows that data localization negatively impacts 13 of the 14 controls of the world's leading international cybersecurity standard (ISO 27002), as well as multiple sub-controls. It also showed that localization in two or more nations clearly restricts the ability to conduct integrated cybersecurity management.[2]

- Innovation collaboration and distributed R&D: Digital trade enables globally distributed engineering, research partnerships, and "follow-the-sun" development using cloud-based tools and secure data environments. Barriers that restrict cross-border access to data and services raise collaboration costs and slow commercialization timelines.

- "Servicification" of manufacturing innovation: Modern manufacturing competitiveness increasingly depends on embedded services—software, data analytics, R&D, design, and after-sales digital services. The Organization for Economic Cooperation and Development (OECD) work shows services' pervasive role in value chains and the prevalence of services supplied together with goods (including R&D).[3] Digital trade barriers therefore hit not only "tech companies," but also the innovation capacity of U.S. manufacturers that rely on digital services to design, produce, and support advanced goods.

---

[1] OECD, Trade and Cross-Border Data Flows: Take Stock of the Potential Implications (OECD Trade Policy Papers), https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/06/trade-and-cross-border-data-flows_84946670/bcc99984-en.pdf?utm.

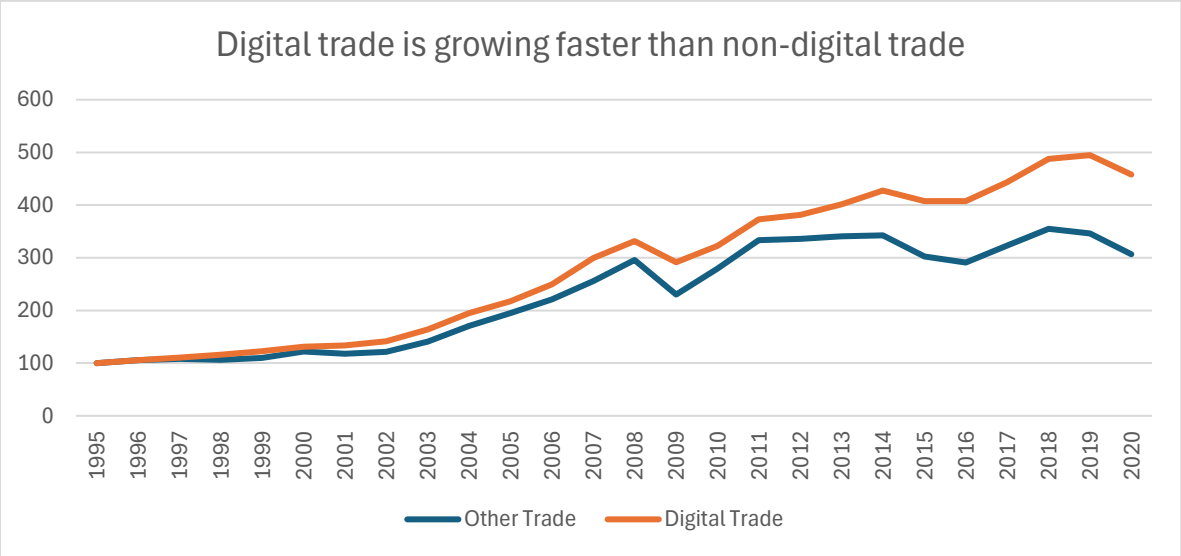
[2] Swire, P., & Kennedy-Mayo, Debrae. "The Effects of Data Localization on Cybersecurity - Organizational Effects," Georgia Tech Scheller College of Business Research Paper No. 4030905, Arizona Law Journal Emerging Technology 3 (2025). Available at SSRN: https://ssrn.com/abstract=4030905 or http://dx.doi.org/10.2139/ssrn.4030905.

[3] OECD. "Services in Global Value Chains – From Inputs to Value-Creating Activities" March 15, 207. https://www.oecd.org/en/publications/services-in-global-value-chains_465f0d8b-en.html; OECD, The Economic Implications of Data Regulation and Trade (OECD), https://cepr.org/voxeu/columns/tear-down-trade-policy-silos-or-how-servicification-manufacturing-makes-divides-trade?utm;

- SMEs and startup scaling: Digital trade lowers entry barriers for smaller firms by enabling remote delivery, platform distribution, and cloud-based operations. In contrast, localization mandates and duplicative certification regimes impose fixed costs that disproportionately shut SMEs out of export markets—reducing competitive dynamism and the pipeline of future innovators.[4]

Global trade is increasingly digital. WTO analysis shows that exports tied to digital trade have grown faster than other goods and services over the long run, highlighting digitization as a structural shift in how trade grows and where value is created (graph 1).[5] Digital trade is already a large, high-value part of the U.S. economy, and a core U.S. export strength. Out of $1.153 trillion in total U.S. services exports in 2024, $730 billion was digitally delivered. Not only does this $730 billion figure represent over half of total U.S. services exports, but also a $282 billion dollar surplus within the realm of digital trade.[6]

Graph 1: Growth of Trade: Digital trade is growing faster than non-digital trade.[7]



[4] OECD, Economic Implications of Data Regulation and Digital Trade (OECD), https://www.oecd.org/en/publications/economic-implications-of-data-regulation_aa285504-en.html.

[5] WTO. "WTO Trade Report 2024 – Trade and Inclusiveness, How to make trade work for all" 2024. https://www.wto.org/english/res_e/booksp_e/wtr24_e/wtr24_e.pdf?utm_source=chatgpt.com

[6] International Data, Table 3.1. U.S. Trade in ICT Services and Digitally Deliverable Services, by Type of Service ((A) (1999-2024)), Transactions, International Services, and International Investment Position Tables, "Table 3.1. U.S. Trade in ICT Services and Digitally Deliverable Services, by Type of Service," Lines 24 and 25, July 3, 2025, https://www.bea.gov/data/intl-trade-investment/international-services-expanded.

[7] "Digital Trade" OECD. https://www.oecd.org/en/topics/policy-issues/digital-trade.html.

Digital trade has long been a critical enabler of U.S. innovation. U.S. technological leadership emerged from the open internet of the 1990s and early 2000s. That era's cutting-edge technology products—internet search, e-commerce platforms, social networks, cloud computing, and many others—were developed in the United States and sold overseas. These firms pioneered the development path of being "born global," where they capitalized on their first-mover advantage in developing and deploying leading digital goods and services globally. Today, the next generation is less a set of standalone products and more an integrated technology stack—compute, cloud, data, models, and security—where success remains dependent on the ability to deploy and improve systems continuously across borders.

The U.S. technology sector is the powerhouse of the growing private sector role in American innovation. The value of digital trade to U.S. innovation is clear. U.S. technology firms are committing a large and growing share of investments to drive innovation as U.S. government funding for R&D plays an increasingly smaller role. In 2022, the sector funded $672.9 billion, or 76 percent of total U.S. R&D, up from 69 percent in 2000 and 61 percent in 2010 (graph 1).[8] Indicative of this, Amazon, Alphabet, Meta, Apple, and Microsoft spent a combined $229 billion in R&D in the twelve months leading up to April 2024.[9]

Unfortunately, the U.S.'s comparative advantage in intangible, services- and IP-intensive activity is also one of the most at risk of trade restrictions, which I will detail in my testimony.

Digital protectionism is no longer a set of isolated, country-specific problems—it is contagious.[10] When major jurisdictions like the European Union (EU) adopts an interventionist digital regulation, others quickly copy it, often in a more restrictive form. While many of these laws and regulations frequently pursue legitimate objectives, they are also regularly used as cover for industrial policy and discriminatory market access restrictions. The result is a "copy-and-ratchet" or a "copy-morph-and-ratchet" dynamic that multiplies compliance burdens across markets, fragments global product deployment, and functions like a behind-the-border tariff on U.S. digital exports and innovation.

This contagion is most visible in the rapid spread of EU-style templates—ex ante platform and content regimes (the Digital Market Act (DMA)/Digital Service Act (DSA)), discriminatory digital services taxes (DSTs), discriminatory "sovereign cloud" and cloud cybersecurity certification schemes (including EU Cloud Cybersecurity Sovereignty Annex-style approaches), and a compliance-first, risk-based AI regulation modeled on the EU AI Act—each of which can be

[8] National Center for Science and Engineering Statistics (NCSES). "Research and Development: U.S. Trends and International Comparisons." NSF - National Science Foundation, May 21, 2024. https://ncses.nsf.gov/pubs/nsb20246/executive-summary.
[9] Ibid.
[10] Digital protectionism is the use of domestic laws, regulations, or administrative practices that restrict or discriminate against cross-border data flows and digitally delivered goods and services to advantage domestic firms or increase governmental control over digital activity. U.S. International Trade Commission, "Digital Trade in the U.S. and Global Economies*", Part 1* (USITC Pub. 4415, July 2013), ch. 5 ("Notable Barriers and Impediments to Digital Trade").

replicated abroad as a de facto market-access gate for cross-border digital services.[11] These contagions have come in waves that compound the cost and complications of prior waves. These policy waves address legitimate issues related to privacy, cloud cybersecurity, and AI, but they are also often used as cover for discriminatory digital trade barriers.

However, the EU is not the only source of inspiration for digital trade barriers. China remains the world's leading practitioner of digital protectionism, combining at-the-border restrictions (with the Great Firewall) with extensive behind-the-border rules that create a fundamentally different—and far more restricted—internet environment for Chinese users and firms.[12] Many countries, particularly authoritative ones, continue to look to China as a model. But China is creating its own waves as it's often a first mover for enacting new laws and regulations for new and emerging technologies.[13]

The U.S. technology sector's global leadership is under threat as trading partners, like China Brazil, the EU, India, Indonesia, Korea, and others, spread the contagion and enact their own novel digital trade barriers. Policymakers in many key markets want to use discriminatory and restrictive laws and regulations to reduce their dependence on American technology as they recognize the growing importance of digital technologies to the economic competitiveness. The full scope of digital trade barriers are many and varied and include forced local data storage (a concept known as data localization) or processing mandates, cross-border data transfer restrictions and approval regimes, discriminatory licensing, certification, or cybersecurity rules, forced technology transfer, source code and algorithm disclosure demands, platform restrictions, and discriminatory anti-trust and competition policies (see appendix A). Based on my review of available data at the time, the number of nations with data transfer barriers increased from 35 countries in 2017 to 62 in 2021. Together, those countries have implemented 144 data localization, up from 67 such barriers in 2017.[14] Just in the Asia-Pacific alone, the

---

[11] On sovereign cloud, see: Cory, Nigel. "Europe's Cloud Security Regime Should Focus on Technology, Not Nationality," The Information Technology and Innovation Foundation (ITIF), March 27, 2023, https://itif.org/publications/2023/03/27/europes-cloud-security-regime-should-focus-on-technology-not-nationality/.

[12] Cory, Nigel. "China's Digital Ambitions: A Global Strategy to Supplant the Liberal Order, Chapter: Writing the Rules: Redefining Norms of Global Digital Governance," The National Bureau of Asian Research (NBR), NBR Special Report No. 97, March 1, 2022, https://www.nbr.org/publication/writing-the-rules-redefining-norms-of-global-digital-governance/; Cory, Nigel. "Testimony Before the U.S.-China Economic and Security Review Commission Regarding China's Cloud Computing Market," ITIF, April 15, 2021, https://itif.org/publications/2021/04/15/testimony-us-china-economic-and-security-review-commission-regarding-chinas/; Cory, Nigel. "Testimony to the U.S. Senate Subcommittee on Trade Regarding Censorship as a Non-Tariff Barrier to Trade," ITIF, June 30, 2020, https://itif.org/publications/2020/06/30/testimony-us-senate-subcommittee-trade-regarding-censorship-non-tariff/; Cory, Nigel. "China and the United States: Digital Protectionism vs. Digital Free Trade," The Center for Strategic and International Studies, October 18, 2019, https://www.csis.org/analysis/perspectives-global-economic-order-2019.

[13] Luo, Yan. "China Takes the Lead on Regulating Novel Technologies: New Regulations on Algorithmic Recommendations and Deep Synthesis Technologies" Inside Privacy, February 8, 2022. https://www.insideprivacy.com/artificial-intelligence/china-takes-the-lead-on-regulating-novel-technologies-new-regulations-on-algorithmic-recommendations-and-deep-synthesis-technologies/?utm_source=chatgpt.com.

[14] Cory, Nigel and Luke Dascoli. "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them." ITIF, December 4, 2024. https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/.

Computer and Communications Industry Association (CCIA) identified 248 digital trade barriers in the APAC region, with 174 policies enacted and 74 policies in development.[15]

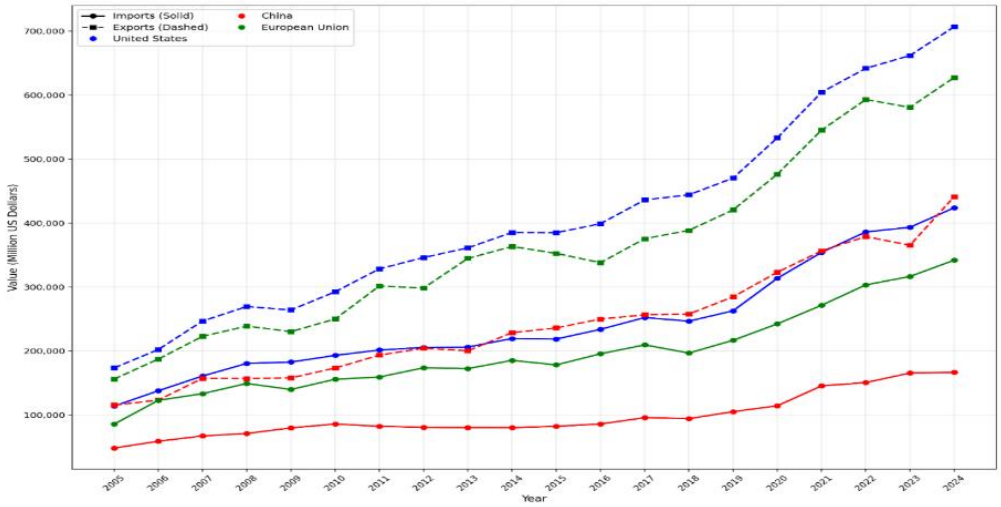
Part of the reason for the contagion and the spread of data localization and other digital trade barriers is that countries exploit an opaque, not fit-for-purpose global trading system as existing World Trade Organization (WTO) rules are largely from the pre-Internet era and have proven inadequate and ineffective in combating the rising tide of digital protectionism. This is why new enforceable digital trade rules are needed.

Congress and the Trump administration should do to push for new rules and to push back against this growing trend and help ensure clear, open, and fair market access for American firms in digital markets around the world. It is in the U.S.'s long-term economic and security interests that U.S. technology firms maximize sales in digital goods and services globally. Every dollar's worth of digital exports from the United States is a dollar American firms can use to reinvest in R&D and support employment domestically.

Digital trade rules have always mattered—but they are now a front-line competitiveness issue because the United States is in a fierce, fast-moving contest with China for global digital-economy market share (see graph 2). Chinese cloud and AI providers are more aggressive, more capable, and increasingly innovative, pairing rapid deployment and deep discounting (50-80 percent of U.S. providers) with state-backed financing and infrastructure buildouts that can lock countries into China-aligned stacks with high switching costs. Chinese cloud and digital infrastructure providers are competing in third-country markets with a bundled strategy: deep discounts paired with increasingly capable "good-enough" cloud and AI offerings, plus rapid infrastructure deployment and local partnerships designed to create early lock-in and dependency (including, in some markets, being first to deliver multi–availability zone footprints). At the same time, U.S. providers—despite operating some of the world's most mature privacy, security, and lawful-access compliance regimes (audits, formal law-enforcement processes, transparency reporting)—often face disproportionate regulatory and political scrutiny focused on visible U.S. legal authorities (such as the CLOUD Act), while comparatively less attention is paid to Chinese providers' legal exposure and obligations to support state security and intelligence. The result is a lopsided risk conversation in developing markets: policymakers intensively interrogate U.S. firms because their processes are transparent and contestable, while underweighting less visible governance constraints and "standards asymmetries" affecting Chinese providers—particularly where sensitive government or critical-infrastructure data is involved.

[15] "2025 Digital Trade Barriers in Asia & the Pacific," CCIA, October 30, 2025, https://ccianet.org/library/2025-digital-trade-barriers-in-asia-the-pacific/.

Graph 2: U.S., EU, and China Digitally Delivered Services: Imports vs. Exports: 2005–2024[16]



In this environment, weak digital trade disciplines translate directly into lost scale for U.S. firms. Defending open, non-discriminatory digital markets is therefore not optional—it is central to sustaining U.S. technology and AI leadership against China's accelerating push to take it. Beyond China's growing role in global markets, U.S. tech leadership also suffered in recent years due the Biden's administration unwillingness to negotiate new digital trade rules and refusal to defend U.S. firms against digital trade barriers. This sent an implicit signal that trading partners can enact restrictions that target U.S. firms without fear of reprisals.

To its credit, the Trump administration has corrected course and clearly sent the opposite signal—it recognizes the role and value of digital trade and U.S. technology leadership and aims to remove digital trade barriers in markets around the world. The Trump administration has secured major wins on digital trade, both within the context of bilateral trade talks but also via direct advocacy on problematic proposals. This includes issues in Canda (halted collection and moved to rescind its DST), France (maintains a DST, but withdrew a measure to double it), Turkey (reducing its DST), India (e.g. on a problematic competition bill (although it is trying to revive it), and removal of a DST), Indonesia (e.g. on personal data flows, removing tariff lines and import declaration requirements for intangible digital products, and supporting a permanent extension of the the moratorium on digital duties (but it is trying to backslide on these commitments), Malaysia (e.g. on a service levy on cloud service providers), New Zealand (dropped its DST bill), Pakistan (exempted U.S. firms from its DST), Thailand (on a proposed

[16] "Digitally delivered services trade dataset" The World Trade Organization, 2025. https://www.wto.org/english/res_e/statis_e/gstdh_digital_services_e.htm.

problematic platform economy law), and Vietnam (e.g. not pursuing a DST and the removal of ex ante provisions from its digital transformation law), among others, where the details depend on ongoing trade negotiations with the United States (.e.g. Korea's commitment not to introduce digital platform regulations).

Securing commitments to withdraw, remove, or reform problematic digital trade barriers is just the first step. Congress and the Trump administration need to keep applying clear, consistent pressure on trading partners as digital market access can quickly regress when trading partners think they can get away with it. For example, while U.S. advocacy played a role in ensuring data localization didn't feature in India and Indonesia's new data laws, localization remains a part of the debate over implementation so could well reappear if policymakers in these countries think that they can get away with it and not face scrutiny and repercussions from the United States.[17] There's already been anecdotal reporting that Indonesia, India, Korea, Thailand, and others are considering how to renege on their commitments to the Trump administration and reintroduce problematic digital trade barriers.

The EU highlights the need for constant vigilance and pressure to address ever evolving digital trade barriers. Since the August 2025 U.S.-EU joint statement on reciprocal, fair, and balanced trade, the EU has taken several steps that violate its commitment to address digital trade barriers.[18] Among others, these include steps taken to expand the DMA to cloud service providers.[19] The European Commission (EC) also recently announced investigations targeting Amazon and Microsoft's cloud businesses, as well as issuing a multibillion-Euro fine on Google.[20] The EC has also breached its commitment to the United States not to impose network usage fees by proposing a backdoor way to impose such a fee through the Digital Networks Act (DNA).[21] The EC advanced its Cloud Sovereignty Framework, which expressly restricts market access for U.S. cloud providers while simultaneously advancing the EU Space Act, which similarly discriminates against American space firms.[22]

---

[17] Roy, Raktima & Zanfir-Fortuna, Gabriela. "The Digital Personal Data Protection Act of India, Explained - Future of Privacy Forum," Future of Privacy Forum, August 2023. https://fpf.org/blog/the-digital-personal-data-protection-act-of-india-explained/; Dorwart, Hunter & Demetzou, Katerina. "Indonesia's Personal Data Protection Bill: Overview, Key Takeaways, and Context" Future of Privacy Forum, October 19, 2022. https://fpf.org/blog/indonesias-personal-data-protection-bill-overview-key-takeaways-and-context/.

[18] Trade and Economic Security. "Joint Statement on a United States-European Union Framework on an Agreement on Reciprocal, Fair and Balanced Trade," August 21, 2025. https://policy.trade.ec.europa.eu/news/joint-statement-united-states-european-union-framework-agreement-reciprocal-fair-and-balanced-trade-2025-08-21_en.

[19] "European Commission Extends the Digital Markets Act Into Cloud: Investigations Into Amazon, Microsoft Reveal." *Chamber of Progress*, January 5, 2026. https://progresschamber.org/news/european-commission-extends-the-digital-markets-act-into-cloud/.

[20] "Commission fines Google €2.95 billion over abusive practices in online advertising technology" European Commission, September 05, 2026. https://ec.europa.eu/commission/presscorner/detail/da/ip_25_1992

[21] Markeviciute, Egle. "Digital Networks Act: New Pushback From 6 EU Member States." EU Tech Loop, November 28, 2025. https://eutechloop.com/digital-networks-act-new-pushback-from-6-eu-member-states/#:~:text=Consumers%20are%20against%20network%20fees,therefore%20should%20not%20be%20reopened.

[22] European Commission. "Cloud Sovereignty Framework | European Commission," October 20, 2025, https://commission.europa.eu/document/09579818-64a6-4dd5-9577-446ab6219113_en.; Hitchens, Theresa. "US Slams 'Discriminatory' Draft EU Space Law as Imperiling NATO Cooperation." Breaking Defense, November 5, 2025. https://breakingdefense.com/2025/11/us-slams-discriminatory-draft-eu-space-law-as-imperiling-nato-cooperation/.;

In terms of recommendations, the policy implication of this testimony is straightforward: if the United States wants to lead in the next generation of innovation—AI, cloud-enabled services, and other IP-intensive technologies—it must treat foreign digital market access as a first-order input into the U.S. innovation base, not a niche trade issue. The recommendations therefore focus on an action-oriented agenda for Congress and the Administration to expand market access for U.S. digital exports, build durable rules of the road, and deter discriminatory measures before they harden.

First, Congress and the Administration should explicitly treat digital market access as an innovation policy imperative by directing USTR and relevant agencies to elevate digital barriers alongside traditional tariff and goods issues in the National Trade Estimate and in bilateral negotiating agendas. This should be paired with a standing "digital barriers" scoreboard—tracking economy-by-economy restrictions on cross-border data transfers, cloud certification and licensing schemes, and discriminatory digital taxation—and a clear interagency objective to expand market access for U.S. cloud, digital services, and AI-enabled exports as part of broader economic security and innovation strategies.

Second, the United States should keep pushing for strong, enforceable digital trade rules—and pair them with a broader "stick-and-carrot" strategy that both disciplines discriminatory barriers and builds alignment around a U.S.-led digital economy and AI ecosystem. On the "carrot" side, the United States should offer targeted technical cooperation on trusted cloud, cybersecurity, digital identity, and AI governance, and mobilize tools such as EXIM and the U.S. International Development Finance Corporation to prioritize digital technologies in key emerging markets where U.S. firms face aggressive competition from Chinese providers. On the "stick" side, the Administration should make clear that rules targeting U.S. firms or imposing non-neutral market-entry gates will trigger escalating trade responses and, where necessary, enforcement—while continuing to pursue modern digital disciplines through trade agreements.

Third, the United States should lead with a pragmatic trusted data agenda that enables cross-border data flows with strong safeguards while preserving legitimate public safety and national security objectives. That agenda should make cooperation on lawful government access a core pillar—grounded in rule-of-law safeguards, transparency, and redress—and treat trust architecture as a competitive asset that differentiates U.S. providers from opaque, state-directed access models. Concretely, this means deepening interoperable privacy and security frameworks with allies and building coalitions through vehicles such as the Global Cross-Border Privacy Rules Forum and the OECD Data Free Flow with Trust initiative.

Fourth, the United States should adopt a more systematic deterrence posture against digital trade barriers—especially measures restricting data flows, conditioning cloud market access, or

---

Information Technology and Innovation Foundation. "The EU's Space Act." ITIF, December 8, 2025. https://itif.org/publications/2025/08/26/the-eu-space-act/.

imposing AI deployment requirements that function as disguised industrial policy. This requires earlier identification of problematic proposals (before rules harden), clearer bilateral escalation pathways, and consistent use of available tools—from consultations and trade agreement committees to enforcement mechanisms—when partners cross the line from legitimate regulation into discrimination. Congress can reinforce this by requiring regular reporting on priority digital barriers and by treating recurring "country-specific compliance gates" (localization, unique certifications, forced disclosure, local content or investment mandates) as presumptively trade-restrictive unless clearly necessary and proportionate.

Fifth, the United States should lead a durable extension—ideally permanent—of the WTO moratorium on customs duties on electronic transmissions. This is an immediate priority because it preserves predictability for digitally deliverable trade and prevents the creation of a new tariff layer on software, data, and digital services. The action agenda should be to rally a coalition of like-minded economies, make the economic case that digital duties are administratively complex and distortionary, and emphasize the disproportionate burden such duties would impose on SMEs and cloud-based services.

Finally, the United States should treat restrictive "AI sovereignty" as the next iteration of digital protectionism—implemented through data, cloud, and AI governance rules—and respond accordingly. An AI-driven trade agenda requires protecting cross-border data flows; preserving non-discriminatory market access for cloud and AI services; resisting forced disclosure and de facto performance requirements; and promoting workable, innovation-supporting approaches to AI training data and IP that avoid turning AI development into a jurisdiction-by-jurisdiction licensing and localization exercise.

The extended written testimony covers all these issues in more detail. First, it expands on why digital trade is a core driver of U.S. innovation and R&D scale—and how behind-the-border digital barriers directly erode market access, revenues, and reinvestment in innovation. Second, it shows how rapidly global trade is digitizing and why digital rules now shape competitiveness and services exports. Third, it assesses the U.S.–China contest for third-country digital market share and how this competition, and related regulatory choices, can lock countries into lower-trust and -quality technology ecosystems. Fourth, it catalogs major digital trade barriers and cases (e.g. data localization; discriminatory licensing, standards, and platform rules; digital taxes; and related measures). Fifth, it addresses the emergence of restrictive "AI sovereignty" as the next wave of digital protectionism. Sixth, it highlights two WTO priorities—the e-commerce moratorium and the Joint Statement Initiative (JSI) on e-commerce as a useful baseline—before concluding with concrete recommendations for Congress and the Administration. Finally, appendix A details major digital trade barriers in the Asia Pacific.