2025 Trade Barriers for Digital Exports

Identifying Threats to U.S. Leadership in Global Digital Trade

Internet-enabled trade in goods and services is a driver for U.S. economic growth, but an ever-growing litany of barriers globally undermines firms' ability to access foreign markets—both through exports and in-country sales. With leading U.S. technology companies relying on foreign markets for over half of their sales, foreign market access is critical to ensuring that this engine of U.S. growth and innovation continues to deliver benefits to the U.S. economy and its workers. The U.S. should lead in setting and enforcing rules for digital trade through new and existing international partnerships. Identifying and addressing key threats and leveraging trade partners in this effort is critical to achieve this goal.[1]

What's At Stake?

A digital economy that generated[3]

$2.6T
OF VALUE ADDED IN 2022

or

10%
OF TOTAL U.S. GDP IN 2022

8.9M
JOBS IN THE U.S. IN 2022

worth

$1.3T
IN ANNUAL COMPENSATION IN 2022

U.S. generated exports abroad[2]

$730B
GLOBALLY IN DIGITALLY DELIVERED SERVICES IN 2024

generating

$282B
TRADE SURPLUS IN DIGITALLY-DELIVERABLE SERVICES IN 2024

Essential part of U.S. export strength

63%
SHARE OF ALL U.S. SERVICES EXPORTS IN 2024

or

2.5%
SHARE OF U.S. GDP IN 2024

[1] This October 2024 summary draws upon the annual submission of CCIA to the Office of the U.S. Trade Representative, as U.S. trade officials prepare the 2025 National Trade Estimate Report. https://ccianet.org/library/ccia-comments-for-the-2026-ustr-nte-report/

[2] According to U.S. Department of Commerce estimates https://apps.bea.gov/iTable/?reqid=62&step=6&isuri=1&tablelist=359&product=4.

[3] According to U.S. Department of Commerce estimates https://www.bea.gov/sites/default/files/2023-12/digital-economy-infographic-2022.pdf.

2025 Key Threats

1 Asymmetric Platform Regulation

- A growing but ill-defined push for "platform regulation," often unsupported by evidence of consumer harm, is driving ex-ante digital regulation worldwide. This untested policy trend is advancing without a proper evaluation of its intended or unintended consequences. In many cases, such regulation functions as a vehicle for industrial policy designed to advantage domestic competitors while disproportionately targeting leading U.S. platforms through carefully calibrated thresholds. These measures often constrain legitimate business models, such as app store operations and product integration, while failing to distinguish pro-competitive behavior from alleged harms. Policymakers frequently invoke competition narratives without robust market analysis to mask discriminatory intent. Far from fostering innovation, these rules risk raising prices, reducing choice, and undermining the very competitiveness they claim to promote.

2 Customs-Related Restrictions and Import Barriers for Goods

- U.S. goods exporters face a range of customs-related barriers affecting e-commerce and exports of inputs for digital infrastructure like data centers. Common obstacles include arbitrary caps and low or unpredictable de minimis thresholds, opaque import licensing and quota schemes, and preshipment inspection mandates that add costs and delays. These measures lengthen clearance times, increase working-capital requirements, heighten inventory risks, and create uncertainty that hits small exporters hardest. Functioning as non-tariff barriers, they undermine efficient trade flows and raise the cost of cross-border commerce. Many of these policies are inconsistent with best practices under the WTO Trade Facilitation Agreement. Addressing them is essential to support e-commerce growth and U.S. ICT investment abroad.

3 Barriers to the Deployment and Operation of Network Infrastructure

- The deployment and operation of global network infrastructure, ranging from subsea cables to satellite constellations, are essential to the functioning of the modern internet and the delivery of cross-border digital services, yet across many jurisdictions these networks face growing market access barriers that discourage foreign investment, slow innovation, and limit affordable connectivity. Subsea cables, which carry over 95 percent of global internet traffic and support more than US$10 trillion in annual economic activity, are increasingly constrained by designated landing sites, mandatory domestic partnerships, cabotage rules, multi-ministry approvals, and punitive customs practices like taxing repair vessels as imports, all of which drive up costs and delay maintenance. Trading partners should allow operators to freely choose suppliers and ensure transparent, objective, and non-discriminatory permitting to sustain global connectivity. Meanwhile, low Earth orbit satellite constellations, expected to generate US$40 billion annually by 2030, face inconsistent licensing regimes, heavy compliance costs, and local incorporation and data localization mandates that raise operational burdens and legal risks. Additional measures, such as denying interference protections, requiring emergency shutdown capabilities, or mandating decryption within borders, further deter deployment. Some space laws explicitly favor domestic operators while imposing disproportionate registration and compliance obligations on foreign systems, particularly those of U.S. providers. Collectively, these barriers fragment global networks, restrict competition, undermine service scalability, and weaken resilience. As demand for secure, low-latency connectivity grows, ensuring fair, transparent, and non-discriminatory conditions for the deployment and operation of digital infrastructure is essential to sustaining digital trade, competitiveness, and economic growth.

4 Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

- Data localization mandates that require local data storage, infrastructure, and corporate presence create major barriers to cross-border digital trade. While often justified on privacy, security, or law enforcement grounds, these measures are frequently protectionist, designed to exclude foreign competitors and advance domestic tech sectors under the banner of "digital sovereignty." In reality, forced localization can undermine security by concentrating sensitive data in a single jurisdiction, making it more vulnerable to cyberattacks and foreign surveillance. It also imposes high economic costs by increasing compliance burdens, fragmenting markets, and raising prices for consumers without meaningfully boosting domestic innovation. These requirements erode U.S. advantages in cloud and data processing, undercutting a critical sector that supports global commerce and thousands of high-paying jobs. Many localization rules also fail to comply with WTO obligations, being vague, discriminatory, or unnecessary. Beyond direct mandates, governments are increasingly adopting restrictive cloud policies, such as certification schemes excluding foreign providers, domestic security requirements, and VPN or encryption access rules. These measures raise costs, limit competition, and threaten the open, cross-border flow of digital services essential to innovation and U.S. economic leadership.

5 Discriminatory Local Content Quotas and Audiovisual Service Mandates

- Some governments are pursuing regulatory frameworks that compel foreign streaming and audio-visual services to finance, distribute, or give preferential treatment to locally produced content. Such measures range from mandatory payments into local promotional funds, investment quotas tied to revenue or production budgets, "discoverability" rules that manipulate recommendation systems, to mandatory "prominence" requirements for domestic broadcasters. They often apply selectively to foreign services, excluding domestic operators or affiliated platforms from equivalent obligations. By forcing streaming services to dedicate a fixed share of revenue to narrowly defined domestic works or requiring them to reorder interfaces to highlight national content, such regimes discriminate against U.S. suppliers and U.S. content and undermine competitive neutrality. They also act as performance requirements prohibited under many trade agreements, compelling companies to structure operations and investments in ways that favor domestic industries regardless of consumer demand or commercial viability. To support sustainable cultural production without distorting digital markets, U.S. trading partners should pursue transparent, non-discriminatory policies that incentivize voluntary investment and international co-production rather than imposing mandatory, nationality-based content requirements.

2025 Key Threats

Forced Revenue Transfers for Digital News

- A growing number of governments are adopting laws that force U.S. online platforms to pay news publishers for content that publishers themselves allow or actively place on those platforms. Instead of supporting negotiated commercial agreements for full articles, these measures demand payment for snippets, headlines, or links—distorting the internet ecosystem and imposing significant costs on service providers. Some countries use "neighboring rights" or "ancillary copyrights" to compel payments in ways that conflict with trade and IP norms, while others, like Australia and Canada, bypass copyright altogether through bargaining codes and legislation clearly aimed at U.S. firms. These measures have led to canceled partnerships, reduced reach for smaller outlets, and diminished user access to information. If widely adopted, they could cost U.S. companies billions annually or drive them to exit news aggregation entirely, harming publishers and consumers alike. Past attempts in Germany, Spain, and France already resulted in traffic declines and increased media concentration. Yet similar proposals are advancing in Indonesia, New Zealand, Türkiye, and Brazil, with other governments exploring comparable approaches. These discriminatory, economically flawed policies threaten to fragment the global internet, distort media markets, and effectively subsidize foreign publishers at the expense of U.S. digital services.

Government-Imposed Restrictions on Internet Content and Related Access Barriers

- Government-imposed censorship, filtering, and shutdowns are among the most severe barriers to cross-border digital trade, with more than half of the global online population facing restrictions on platforms between June 2023 and May 2024. At least 25 countries systematically blocked messaging or social media services, often during protests, and Access Now recorded 296 shutdowns in 51 countries in 2024, causing an estimated US$8 billion in economic losses. National firewalls and state-controlled gateways further disadvantage foreign services, violating WTO obligations when applied in opaque, discriminatory, or unnecessary ways. Alongside these overt restrictions, governments are advancing content regulations that impose disproportionate compliance burdens on foreign providers. Many measures go well beyond addressing illegal content, requiring takedowns of lawful speech, generalized monitoring, algorithm disclosure, encryption-breaking mandates, or local employee liability. Some even compel the installation of state-approved apps or give domestic platforms preferential treatment, undermining competitive neutrality. These measures raise costs, create legal uncertainty, chill speech, and limit market entry, especially for smaller U.S. firms. If left unchecked, they risk fragmenting the global digital ecosystem, making clear, transparent, and proportionate content frameworks essential to safeguarding free expression and preserving cross-border digital trade.

Imposing Legacy Telecommunications Rules on Internet-Enabled Services

- Applying outdated telecommunications-era rules to modern internet services creates major barriers for U.S. digital exports. A prominent example is "sender-pays" or "network usage fee" proposals, which force content and application providers to pay ISPs for traffic that users themselves request. Despite claims that such fees offset network costs, they ignore economic realities and the internet's user-pays model. South Korea's long-standing regime has led to higher latency, poorer performance, and reduced investment as providers relocate services abroad. Similar proposals in the EU, Australia, Brazil, and the Caribbean would effectively tax U.S. digital exports, distort competition, and raise costs for consumers. In parallel, governments are imposing legacy telecom-style rules on OTT and cloud services, treating them like network operators despite operating at the application layer. This includes licensing requirements and compliance obligations designed for monopolistic, infrastructure-based industries. By blurring the line between networks and services, these outdated frameworks threaten innovation, fragment markets, and undermine the open architecture that made the internet globally competitive.

Potential Challenges to the Development of AI

- AI is poised to transform global trade by lowering costs, boosting productivity, and significantly expanding U.S. digital services exports, with the WTO estimating it could expand trade by up to 37 percent and global GDP by 13 percent by 2040. Access to vast and diverse datasets, including publicly available online content, is central to developing accurate, secure, and effective AI systems, but this foundation is increasingly threatened by restrictive measures. Countries such as Brazil are considering impractical licensing rules for AI training, while debates in Australia, Canada, Korea, and the United Kingdom signal similar risks, potentially creating trade barriers and stifling innovation. Unlike the United States, where fair use enables responsible AI training, many countries lack equivalent safe harbors, which underscores the need for the United States to promote fair use internationally. At the same time, governments are advancing regulations that, while often framed as safety measures, risk targeting U.S. firms through discriminatory or protectionist approaches. These include data localization, cross-border data restrictions, onerous transparency rules, and forced disclosure of source code, algorithms, model weights, or training data. Additional risks stem from vague or inaccurate risk classifications, obligations that conflate developers and deployers, and labeling requirements that are misaligned with best practices. To protect U.S. AI competitiveness and ensure fair market access, the United States should lead in shaping global AI governance that safeguards innovation, trade, and open data flows.

Restrictions on Cross-Border Data Flows

- The free flow of data across borders is a cornerstone of the global digital economy and essential to growth, innovation, and trade across all sectors. In 2023, digitally deliverable services dependent on cross-border data transfers generated nearly $4.25 trillion worldwide, enabling businesses of all sizes to operate seamlessly across markets. Despite this, many governments continue to impose unclear privacy regimes, onerous transfer conditions, and restrictive export requirements that drive up costs, reduce efficiency, and undermine competitiveness for industries reliant on data flows. The absence of clear and interoperable mechanisms for data transfer, particularly in restrictive data governance regimes, further disadvantages the ability of foreign digital firms to operate effectively in these markets. Such rules not only distort competition but can also lower GDP, deter foreign investment, disrupt supply chains, and significantly reduce productivity and export potential, effects that are particularly damaging for local firms dependent on digital tools and services.

2025 Key Threats

Taxation of Digital Products and Services

- A growing number of jurisdictions are advancing unilateral digital services taxes (DSTs) that overwhelmingly target U.S. companies and distort global trade. While some governments, such as Canada, India, Pakistan, and New Zealand, have withdrawn or paused DSTs, others continue to collect or propose them. In the United Kingdom, France, Spain, and Italy alone, DSTs extracted more than $9 billion between 2020 and 2024, with most of the burden falling on U.S. firms. These measures rest on the false premise that U.S. companies do not pay sufficient tax, ignoring that they are already taxed in the United States on global revenues and risk creating double taxation in the absence of a multilateral agreement. Many DSTs are discriminatory by design and may conflict with tax treaties and trade agreements, prompting bipartisan U.S. opposition and calls for a strong trade response. A parallel risk comes from efforts to impose customs duties on electronic transmissions, which would reverse more than two decades of WTO-backed liberalization. Such tariffs would create significant compliance burdens, especially for SMEs, because origin, value, and destination data are often unknowable for cloud-based services. With the WTO moratorium set to expire in March 2026, the United States should push for a permanent extension and resist attempts to incorporate electronic transmissions into tariff schedules.

Threats to the Security of Devices and Services

- Providers of digital devices and services have long relied on strong encryption to protect communications and transactions, securing sensitive personal and financial data from malicious actors. However, many governments, often citing national security or law enforcement, are pursuing or enacting laws that undermine end-to-end encryption. The UK's 2023 Online Safety Act, for example, allows the government to compel digital firms to scan for illegal content, effectively weakening encryption, while amendments to the Investigatory Powers Act could delay security updates and hinder innovation. Similar "exceptional access" regimes are emerging elsewhere, often requiring technical assistance or compliance with infeasible judicial orders. These mandates create legal and technical uncertainty, forcing companies to modify global platforms, build region-specific products, or face severe penalties. Secrecy provisions prevent firms from disclosing government demands, compounding compliance risks and deterring market entry. Because technology is deployed globally, mandated vulnerabilities threaten the security and privacy of users worldwide. In parallel, some governments are mandating app store configurations or interoperability rules that weaken device security and expose users to greater privacy risks.