National Foreign Trade Council

Input to the United States Trade Representative

2026 National Trade Estimate (NTE) Comments

Comments Regarding Significant Foreign Trade Barriers for the 2026 National Trade Estimate Report

Docket No. USTR-2025-0016

October 30, 2025

Table of Contents

Introduction

These comments are submitted by the National Foreign Trade Council (NFTC) in response to the notice entitled *Request for Comments on Significant Foreign Trade Barriers for the 2026 National Trade Estimate Report* which was published in the Federal Register on September 15, 2025. Pursuant to the Notice, The Office of the United States Trade Representative (USTR), through the Trade Policy Staff Committee (TPSC), publishes the National Trade Estimate Report on Foreign Trade Barriers (NTE Report) each year. USTR invites comments to assist it and the TPSC in identifying significant foreign barriers to, or distortions of, U.S. exports of goods and services and U.S. foreign direct investment for inclusion in the NTE Report.

NFTC is dedicated to making America more competitive in the global economy by ensuring the adoption of forward-looking tax and trade policies, by strengthening global rules and by opening foreign markets to U.S. products and services. Our strong support for these objectives, and our belief that their fulfillment is essential to our members' success in a globalized economy, have been unwavering for over a century. We, therefore, believe that it is critical to provide policymakers in the administration with our clear views about the role trade and tax policies play with respect to U.S. competitiveness in the global economy.

The National Foreign Trade Council is the premier business association advancing trade and tax policies that support access to the global marketplace. Founded in 1914, NFTC promotes an open, rules-based global economy on behalf of a diverse membership of U.S.-based businesses.

Cross-Cutting Issues

Further to the country-specific comments on trade barriers below, we want to raise two cross-cutting issues that continue to create significant challenges for U.S. technology exporters:

Customs Valuation for Intercompany Transfers: Customs valuation of intercompany transfers of technology equipment creates significant compliance burdens for U.S. companies. In particular, when goods are transferred between related parties (e.g., subsidiaries of the same ultimate corporate parent entity) without a sale, Customs authorities require complex valuation methodologies, applied inconsistently across countries (sometimes across imports to the same country) often necessitating the provision of extensive documentation to prove arm's length values (even when values are the same or similar for hardware imports between unrelated parties). This issue is particularly difficult for transfers of broken or depreciated equipment between related companies. These issues create administrative burdens, potential disputes, and unwarranted audits and investigations. The complexity of valuation requirements, onerous documentation demands, and inconsistent application of valuation requirements across countries (and across imports into a single country) act as barriers to consistent and fair treatment of U.S. imports to other countries. This issue affects trade with: Indonesia, India, Brazil, Malaysia, Thailand, and Australia.

Harmonized System Classification Challenges: Inconsistent approaches to import classifications of technology hardware under the Harmonized Tariff Schedule (HTS) creates ongoing compliance challenges for U.S. companies. Classification disputes with Customs authorities over technology hardware categories often occur, even after previous agreements are reached (e.g., when new Customs officials are appointed). Since import classifications determine duty rates and special requirements, the inconsistent application creates uncertainty, leads to supply chain disruptions, and often results in additional administrative burden and costs (e.g., when addressing unwarranted audits, investigations, and legal challenges). The complexity of classifying integrated technology systems leads to inconsistent treatment across countries and acts as a barrier to consistent and fair treatment of U.S. imports to other

countries. This issue affects U.S. trade with: Indonesia, India, Brazil, Vietnam, Malaysia, Singapore, Thailand, and Australia.

Access to AI Training Materials: Access to vast and diverse datasets, including publicly available information from the open web, is fundamental for building responsible, accurate, secure, and effective AI systems. This access is the lifeblood of AI progress. AI innovation fundamentally depends on the ability to learn from the widest possible variety of publicly available material. This allows the AI models to identify features, relationships, and patterns between and among data points. This extensive training on billions of data points helps the models learn, understand diverse perspectives, and guard against bias. To ensure AI's benefits are fully realized while addressing concerns about human creativity, establishing balanced copyright frameworks that do not restrict the fundamental learning process of AI models is crucial.

However, this essential ecosystem for AI innovation is threatened by a growing number of countries contemplating or adopting restrictive copyright policies that would serve as significant trade barriers. Nations such as Brazil are pursuing regulations that would severely limit or impose impractical licensing requirements on the use of copyrighted works for AI training. Even in the absence of formal legislative proposals, ongoing policy debates in Australia, Canada, and the UK are concerning. Within these discussions, stakeholders are challenging established copyright norms and raising fundamental questions about the use of local online content for AI training, which could have implications for AI model development, even when it occurs within the U.S. These approaches risk stifling innovation and disadvantaging developers who abide by international norms. We urge the U.S. government to protect AI innovation by ensuring restrictive copyright frameworks do not create a barrier to AI innovation or market access.

Country-by-Country Trade Barriers

Argentina

Import Policies

Benefits to Trade Facilitation: In December 2024, Argentina implemented significant changes to facilitate the clearance of informal, low-value shipments. These reforms raised the value threshold for informal shipments to US$3,000 and simplified the documentation requirements for goods falling under this category. As a result, shipments arriving via express companies now benefit from faster customs clearance and reduced administrative burdens. These changes have particularly supported the growth of e-commerce and small business imports, making it easier to bring in samples, spare parts, and consumer goods under simplified procedures.

Barriers on Electric Equipment Imports: Argentina recently established new legislation on regulatory requirements for electric equipment. The new regulation was broadly advertised as positive, since international certificates are now accepted, as long as the importer is formally authorized by the international certificate holder, dismissing the need for local certification. However, the change did not incorporate the exceptions previously extended to companies importing the equipment for internal use. Subsequently, the change imposed new barriers to these importers, as the process to obtain the international certificate, identify the certificate holder and obtain authorization is much more cumbersome than the previous possibility to present a sworn statement.

Technical Barriers to Trade

New Health Technology Assessment (HTA) Agency Potential as Market Access Barrier: In March 2025, the Argentine government announced the creation of the National Agency for the Evaluation of Health Technology Financing (ANEFiTS), which would operate under the Ministry of Health and conduct cost-effectiveness economic evaluations of all new technologies seeking registration in Argentina. The agency could determine that a product, even if approved by the FDA and marketed in the U.S. and worldwide, cannot apply for marketing authorization in Argentina because "its cost could be high for the system as a whole." This newly proposed HTA agency would establish an unprecedented non-tariff barrier to innovative medicines by allowing cost-effectiveness assessments to potentially block companies from seeking marketing authorization. **USTR should urge that the scope and operational criteria used by ANEFiTs are aligned with international technical and transparency standards.**

Government Procurement

Cloud Procurement Limitations: Argentina's public sector lacks a standardized framework for cloud service procurement, creating a significant market access barrier. The current regulations result in lengthy, inefficient procurement processes that deter cloud service adoption and create unnecessary administrative burden for providers. This limitation particularly impacts US technology companies seeking to provide cloud services to Argentine public sector entities. The proposed solution calls for establishing a comprehensive cloud procurement vehicle with flexible resource allocation and streamlined approval procedures, which would facilitate market access and promote efficient cloud service adoption in the public sector.

Services Barriers

Personal Data Transfer Restrictions: Argentina currently does not recognize the United States as an adequate jurisdiction for personal data transfers, creating a significant trade barrier for US companies. While data flows freely to EU member states, European Economic Area (EEA) countries, and nations with EU adequacy decisions, transfers to the US require additional safeguards through contractual clauses. This restriction stems from Argentina's alignment with EU data protection standards, contrasting with the US's sector-specific approach and lack of federal privacy legislation. The barrier impacts US companies through increased operational complexity, compliance costs, and service implementation delays. A resolution would require modification of Disposition E60/2016 AAIP to include the US as an adequate jurisdiction or recognition of US Data Privacy Framework (DPF) certified companies as meeting adequacy requirements.

Intellectual Property Protection

Restrictive Patentability Criteria (Pharmaceuticals): Argentina’s Patent Law through ministerial resolution applies more restrictive patentability criteria for a large portion of pharmaceutical products than most countries, resulting in innovative medicines launched in the country receiving less protection than they would in other developed markets.

Lack of Regulatory Data Protection (Pharmaceuticals): Argentina has an inadequate system for regulatory data protection, allowing local companies to use clinical data from American pharmaceutical companies to copy products and complete their own regulatory approval applications.

Australia

Technical Barriers to Trade

Market Access (Pharmaceuticals): Australia undervalues new innovative medicines by setting prices based on older inferior medicines and generics and through biased health technology assessments that rely on low and outdated monetary thresholds per year of life gained from clinically proven treatments. Moreover, the Pharmaceutical Benefit Scheme (PBS) often restricts access to a small subset of the patient population for which the product was proven safe and effective and creates access delays through unnecessary data requirements and other administrative hurdles.

Intellectual Property Protection

Inadequate patent notification arrangements: In the Australia-US Free Trade Agreement, Australia agreed to make necessary arrangements for notification to the patent owner if another party submits a medicine for marketing approval during the term of an existing patent, though action has not been taken to bring such an arrangement into existence. Instead of notifying the patent holder when a potentially infringing generic or biosimilar product commences the registration process, the patent holder only becomes aware of the potential infringement by carefully monitoring new additions to the Australian Register of Therapeutic Goods (ARTG). Immediately following the launch of the competitor product, the reimbursed price of the originator product reduces by 25%. The patent holder is left with an emergency injunction as their only recourse to prevent launch while assessing the validity of their patent and litigation is pending, which is costly for parties and time consuming for the courts. The introduction of legislative reform requiring effective notification of generic and biosimilar applications submitted to the Therapeutic Goods Administration (TGA) to originator pharmaceutical companies and an effective mechanism for the early resolution of patent disputes before an infringing product is launched in Australia.

Insufficient regulatory data protection: Australia provides a 5-year period for regulatory data protection for both small molecule and biologic products which is substantially shorter than the regulatory data protection provided in many other countries for biologic products. This creates a disincentive to registration of products in Australia as originators can't be assured that their research will be protected. This is particularly challenging for biologics where unlike traditional chemical compounds, the generic version of the biologic is not exactly the same as the originator – this means patent protection alone is insufficient. Australia should adopt a period of regulatory data protection that is in line with global best practice and provides adequate protection to products like biologics which are insufficiently protected by patents alone. Australia should also extend regulatory data protection for new indications, new formulations, new patient populations and new dosage forms would result in consistency with other markets.

Market-size damages: The Australian Government has sought "market-size" damages from patentees that have legitimately but ultimately unsuccessfully pursued patent infringement actions. These damages purportedly compensate the PBS for the effect of any delay in the PBS price reduction due to a preliminary injunction on generic launch which is ultimately lifted if the patentee is unsuccessful. These so-called "market-size damages" create significant uncertainty for pharmaceutical patent owners. It also undermines the rights of patent holders in Australia by introducing a strong disincentive to exercise their core right to enforce their IP protections and is inconsistent with Australia's international commitments under the AUSFTA and the World Trade Organization (WTO) Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS).

Services Barriers

Audiovisual Services: Australia is considering imposing screen content requirements on streaming video services as part of its National Cultural Policy. The Policy, published in January 2023, recommends that the Australian Government introduce "requirements for Australian screen content on streaming platforms to ensure continued access to local stories." The Australian Government has consulted on potential models and has publicly maintained its commitment to introducing legislation.

Ex-ante Regime for Digital Services: In December 2024, AU Treasury launched its long-anticipated consultation on a new ex-ante regime for digital services. The proposed framework adopts aspects of both the EU DMA and the UK DMCCA, which would allow the AU Government to designate digital platform services to broad obligations on matters such as self-preferencing and data use, as well as 'service-specific obligations'. The proposal would immediately trigger new compliance obligations around preventing self-preferencing, ensuring interoperability, and prohibiting manipulative design practices. The proposal identifies 'priority services' for designation as app marketplaces, ad-tech services and social media, although a wide range of digital services are flagged for future consideration, including general online marketplaces, virtual assistants and, potentially, cloud. Designation also opens the way for the ACCC to recommend service-specific (platform-specific) codes of conduct. The scheme would raise similar trade-related concerns to the DMA should only US-headquartered companies meet the criteria for designation (which is possible given the initial sectors identified). Draft legislation is expected Q1'26. The Australian government has justified its proposed intervention in terms of bolstering economy-wide efficiency. However, industry estimates suggest the regime could reduce investment in digital services by up to 17.4%, lower GDP by up to A$21.1 billion, as well as disproportionately impact international suppliers. By targeting specific firms through prescriptive obligations rather than adopting principle-based, evidence-driven enforcement, the proposal threatens to distort competition and undermine U.S. market access in Australia.

News Media-Related Digital Service Taxes: In February 2021, the Australian Government passed the News Media and Digital Platforms Mandatory Bargaining Code. The Code requires designated platforms to negotiate with Australian news publishers and pay them for online content. A Treasury report in November 2022 found that at least 30 such agreements were reached, although their contents remain confidential. Despite these agreements, in December 2024, the Albanese government announced plans to establish the News Bargaining Incentive, requiring firms that earn more than A$250m ($164m) in annual revenue to enter into commercial deals with media organizations, or risk being hit with higher taxes. The new rules target a narrow set of digital companies, predominantly US firms. While the Albanese government are calling it an "incentive" rather than a "tax," the new rules would amount to a targeted and highly discriminatory DST.

Content Regulation: Australia's 2021 Online Safety Act empowers the eSafety Commissioner to demand removal of "harmful" content, including adult cyber abuse. Under the Act, industry codes of conduct and standards for eight online sectors were developed to implement the requirements under the Act. Additionally, in November 2024, the Online Safety Amendment (Social Media Minimum Age) Bill was passed, mandating a minimum age of 16 for certain social media accounts. Industry concerns with the overall regime include: strict investment requirements for content detection and removal; the ill-defined concept of "harm" leading to censorship of lawful content; and overbroad restrictions limiting creativity, valuable online experiences for minors, and freedom of expression and information.

Local Content Quotas (Streaming Services): Australia's mooted local-content requirements for streaming services, mandating that SVOD (subscription video-on-demand) platforms invest a set percentage of their revenues into Australian-produced content, would disproportionately harm U.S. firms, and stand in conflict with the Australia-United States Free Trade Agreement (AUSFTA). In November

2024, the Australian government confirmed it is shelving those plans due to the conflict between new local content rules and AUSFTA. USTR should remain mindful of such measures being considered again given the extreme compliance burden and disincentive to investment they would place on U.S. companies.

Other Barriers

Draft Taxation Ruling on Royalties – Character of Receipts in Respect of Software: The Australian Tax Office (ATO) proposed Draft Taxation Ruling TR2024/D1 which treats certain outbound payments by in-country distributors of software as royalties subject to Australian withholding tax. This ruling is contrary to long-standing internationally accepted treaty interpretation, including paragraph 14.4 of the Commentary to Article 12 (Royalties) of the OECD Model Tax Convention. ATO's approach contemplated in the Draft Taxation Ruling was recognized in two letters from the US Treasury Department to the Australian Treasury Department, sent in August 2022 and April 2024, respectively, which highlighted that the approach violated well-settled norms, including the OECD Commentary, and threatened to "create a concerning imbalance in the benefits provided by the Australia-U.S. tax treaty." Such a withholding tax would have similar anti-competitive and discriminatory effects as a digital services tax (DST) with respect to US software companies and others that sell software products and services (including cloud services) into the Australian market. **USTR is urged to request that the Australian government withdraw the draft ruling and continue to apply its long-standing position in Taxation Ruling TR93/12.** In its evaluation, ATO should consider the holding in *PepsiCo, Inc. v Commissioner of Taxation* ([2024] FCAFC 86) ("PepsiCo"), mentioned in paragraphs 5 and 6 of the Practical Compliance Guide. The High Court found that no royalty withholding tax or diverted profits tax was applicable in the "PepsiCo" case. We strongly urge the ATO to consider this ruling as it approaches embedded royalties and the Software Directive as a whole. **If the draft ruling is finalized substantially as proposed, USTR is urged to use all of the available tools in the toolbox to resolve this issue.**

Country-by-Country Reporting: ATO's stringent public country-by-country reporting (CbCR) requires U.S. enterprises to give an annual Public CbCR to the Australian government. Public CBCR requires U.S. parents to disclose global revenues, profits and income taxes; the activities of the global group; and an entity's international related party dealings among other information. The law provides for a " blacklist" which requires that global reporting must be disaggregated for 'specified jurisdictions', which includes American Samoa and the U.S. Virgin Islands. NFTC has significant concerns regarding this in terms of its privacy and competitive implications as well as its encroachment on U.S. sovereignty. When combined with other publicly available filings, such disclosures would compromise the privacy of individual U.S. business owners, business practices, and provide a roadmap for competitors and foreign adversaries to exploit. U.S. companies will bear a disproportionate burden from the extraterritorial reach of this mandate, as their worldwide operations, including sensitive information shielded under US law, will be publicly exposed through the Public CBCR.

Azerbaijan

Services Barriers

Electronic Payment Services: The CBAR (Central Bank of Azerbaijan Republic) has been actively discussing with the financial institutions operating in Azerbaijan the plan to amend CBAR's "Regulation on maintaining payment operations and on payment instruments" to exclusively mandate financial institutions in Azerbaijan to use the local indigenously developed Instant Payment System for domestic person-to-person (P2P) transfers. The CBAR's intent to exclusively use the IPS as a single rail for

domestic P2P payments will limit the ability of U.S. payment networks to compete fairly in Azerbaijan. Such a mandate also represents a market access barrier.

Bangladesh

Import Policies

Illicit Trade: Illicit trade is becoming a more substantial challenge for U.S. companies operating in the region. One particular issue of concern is the increase in illicit trade crossing the border between India and Bangladesh. **NFTC urges USTR to encourage intensive training, strategic deployment of resources, and greater partnership between Indian and Bangladeshi authorities.** In addition, authorities should take greater action against websites selling illicit medicines and local distributors facilitating their spread.

Services Barriers

Data Localization Requirements: In October 2025, the Cabinet of the Interim Government of Bangladesh passed the Personal Data Protection Ordinance (PDPO) and the National Data Governance Ordinance (NDGO), with little industry consultation on the former and none on the latter. The PDPO contains concerning criminal liability and extraterritorial provisions, as well as data localization requirements for certain types of restricted data. Classified data (confidential and restricted) must be stored within Bangladesh's jurisdiction. Transfer of internal and confidential data abroad is allowed with consent or under specific contractual or interest-related conditions, and only to countries with suitable data protection technology and equipment. Most of the PDPO comes into effect immediately. However, Section 23 (Chief Data Officer) and Sections 31- 46 (Complaint Filing, Administrative Penalties, and Criminal Offences and Penalties) will only come into effect at a later date which is the earlier of: (1) the date specified by the Government through a gazette notification, and (2) 18 months from the date of issuance of the PDPO.

Bolivia

Services Barriers

Data Localization Requirements: Bolivia maintains restrictive data localization requirements for the public sector through its Electronic Government Plan and Open Software and Open Standards Implementation Plan (PISLEA 2025-2030). Under these regulations, public sector entities must store "non-public" government data within Bolivian territory, effectively preventing international cloud service providers from offering storage services to government institutions. While recent updates to PISLEA have provided some flexibility by allowing cloud services for "public" data and certain cloud-based operations for "non-public" data (such as processing), the regulations maintain strict data localization requirements for storage of "non-public" data. The lack of clear definitions for "public" and "non-public" data creates significant legal uncertainty for companies seeking to provide cloud services to Bolivian government entities. To address these barriers, Bolivia should consider adopting internationally recognized data protection standards while allowing cross-border data flows, and implement risk-based approaches rather than blanket localization requirements.

Financial Sector Regulations: Bolivia's Financial System Supervision Authority (ASFI) maintains burdensome regulatory requirements that create significant barriers for cloud service providers and financial institutions. Under ASFI's Information Security Management Regulations, financial institutions must obtain prior non-objection before contracting cloud services, through a process that lacks

transparency and standardized evaluation criteria. The regulations require submission of detailed implementation projects without providing clear guidelines for their assessment, leading to lengthy approval processes. Financial institutions must also maintain an on-premises data processing center and an alternate processing center, regardless of their cloud adoption plans, while ASFI requires physical auditing access to cloud providers' facilities. These requirements are more restrictive than those of neighboring countries like Argentina, Brazil, Chile, Colombia, Peru, and Paraguay, which only require notification rather than prior approval for cloud service adoption. To modernize its approach, Bolivia should consider replacing the prior approval system with a notification mechanism, streamline approval processes with clear timelines and criteria, and harmonize regulations with regional best practices.

Brazil

Import Policies

Prohibition on the Import of Refurbished Products: Brazil maintains import prohibitions on certain used ICT products. This policy is unfair, because refurbished products and components are “like new” products and should not be banned. U.S. companies are required to continue supporting customers with products that are under warranty, especially when such products have reached end-of-sale, and components are no longer available as new products.

Technical Barriers to Trade

Incorporation Delays in Public Market (Medicines): Innovative medicines face significant market access barriers in Brazil due to prolonged incorporation delays in the public market. CONITEC is the local HTA body that evaluates the incorporation of new vaccines and medicines into the public health system. This process and its associated timelines are regulated by legislation. If a medicine or vaccine is approved by CONITEC, it must be made available to patients within 180 days. However, data shows that 25% of the medications incorporated between 2019 and 2024 are still not available to the population. Out of the 143 medications approved by CONITEC, 36 are awaiting the completion of the procurement process.

Intellectual Property Protection

Misalignment with International IP Standards (Pharmaceuticals): Brazil’s intellectual property standards fall short of global best practices, posing significant challenges for U.S. companies. The absence of patent term adjustments and regulatory data protection for pharmaceutical products undermines innovation and market competitiveness. Brazilian law does not protect pharmaceutical products against unfair commercial use of undisclosed test results and other data generated to obtain marketing approval, despite providing such protection to veterinary and agricultural chemical products. These issues are further exacerbated by a substantial backlog of pending pharmaceutical applications, creating prolonged uncertainty and delays in product approvals.

Lack of regulatory data protection (RDP): Brazil does not provide RDP for biopharmaceutical products (despite applying RDP for veterinary, fertilizer, and agrochemical products).

Compulsory licensing: Members of Brazil’s National Congress continue to pursue efforts to expand inappropriately compulsory licensing provisions in Brazil’s Industrial Property Law. Recent efforts, such as PL No. 12/2021, included several unprecedented, vague, and broad provisions that go beyond what was envisioned under the World Trade Organization (WTO) Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). These efforts fundamentally undermine the predictability and certainty necessary for U.S. innovators from all sectors to successfully invest in and accelerate the launch of new products in Brazil.

Services Barriers

Data Localization Requirements: In 2018, Brazil passed a privacy law, Lei Geral de Proteção de Dados (LGPD). It came into force in August 2020 and its sanctions one year later, in August 2021. LGPD lacks a number of provisions in the GDPR designed to lessen the burden on smaller firms. Further, the LGPD does not permit cross-border data transfers based on the controller's legitimate interests, but rather lists ten instances in which cross-border data transfer under the LGPD is permitted. In addition, the national authority is tasked with determining whether a foreign government or international organization has a sufficient data protection scheme in place before any data is authorized to be transferred to the government or organization. Further, under the LGPD data privacy law and its establishment of the ANPD (Brazil's data protection authority), the ANPD is required by statute to issue a permitted country "white list" for jurisdictions that are allowed cross-border data transfers in/out of Brazil with eased restrictions. This list remains outstanding from the ANPD since the law was implemented in 2021.

AI Bill: Brazil's Bill No. 2338, introduced on May 12, 2023, aims to regulate AI technologies but presents several issues**.** The pending legislation would create substantial barriers for U.S. AI services by implementing broad regulations that fail to distinguish between high and low-risk applications. The bill's lack of clear differentiation between AI developers and deployers creates operational uncertainty for the entire AI value chain. Most significantly, it would require payment for Brazilian content used in AI model training and could effectively prevent U.S. companies from developing or deploying their generative AI features in Brazil, potentially giving an advantage to competitors from other regions. As currently written, several provisions of the bill are unreasonable and would significantly burden U.S. commerce. Specifically, the bill would introduce significant barriers for U.S. innovators attempting to export AI tools and services to Brazil. The bill would disproportionately harm U.S. technology companies that need to scale and compete globally in the race to develop and deploy AI. The bill also takes a blanket approach to AI regulation that is overly burdensome. Instead of narrowly focusing on high-risk use cases, the proposed legislation captures low-risk applications, including everyday business functions. In addition, the bill does not clearly differentiate between the developer of a high-risk AI system and the entity that deploys the system. This failure represents a burden on U.S. commerce because it significantly impedes the ability of U.S. companies to develop innovative AI applications.The Bill also designates Brazil's National Data Protection Authority (ANPD) as the primary regulator for coordinating sectoral regulators and issuing rules for "unregulated sectors", which might include social media since content recommendation systems are driven by AI. This creates uncertainty due to overlaps between Brazil's privacy law, the Lei Geral de Proteção de Dados (LGPD), and the proposed AI framework. In 2024, the ANPD launched AI-related investigations against U.S. and foreign tech firms, sometimes issuing preemptive blocking orders, reflecting a restrictive, EU-inspired approach that risks stifling innovation. Further, expansive copyright provisions under the Bill would require developers to compensate Brazilian content owners for any data used to train AI models, despite the fact that AI models extract and replicate unprotectable facts and patterns rather than protected expression, further restricting U.S. innovation and commerce by effectively imposing extraterritorial taxes on AI developers.

Ex-Ante Competition Legislation: In September 2025, the Brazilian Government sent a proposal – Bill 4675 - to Congress that would grant Brazil's competition authority (CADE) expanded powers to regulate online companies above a certain size. The bill - inspired by European frameworks including the UK's DMCC and EU's DMA - proposes creating a special division that will designate companies as "systemically relevant" as well as determine and apply special obligations to designated companies on a case-by-case basis. The bill provides CADE broad authority and open-ended criteria to designate companies, including a revenue requirement of R$50 billion globally or R$5 billion in Brazil, and key characteristics including – but not limited to - operating multi-sided platforms and access to significant amounts of personal and business user data, among others. The Finance Ministry has consistently stated that there will be no more than 5-10 designated companies but will certainly include the DMA's

"gatekeeper" companies, which are largely U.S. companies (e.g. Amazon, Apple, Booking, ByteDance (owns TikTok), Meta (owns Facebook, Instagram and WhatsApp), and Microsoft). CADE will determine and apply special obligations on a case-by-case basis following an administrative proceeding, which could include mandatory notification of all mergers, prohibiting self-preferencing, data transfers and interoperability, and ensuring users can easily switch to competing services or install third-party apps. CADE is not required to show that its obligations, including any remedies it imposes, are proportional to correcting the supposed problems identified. The bill only requires CADE to show that its remedies against a designated firm are necessary to "protect and promote competition." These objectives are so broad and undefined that they would allow CADE to argue the need for pretty much any type of intervention in any situation. The proposal abandons the fundamental principle that competition law applies equally to all economic agents across industries and should address specific harm, based on evidence, actual proof of harm, and a careful balancing of risks and consumer and economic benefits. Designation will last for 10 years and apply to the entire company, while the special obligations may be limited to specific services or products. Failure to comply with the obligations will result in the same penalties currently applicable for violations of the economic order ranging from staggering fines to company break-up.

Additional Ex Ante Competition Bills: Two other similar bills are also under consideration: Bill 2768, inspired by the European Union's Digital Markets Act (DMA), that designates the National Telecommunications Agency (ANATEL) as the primary regulator of "digital platforms" in Brazil. The bill also establishes a regulatory framework for the organization, functioning, and operation of "digital platforms" that offer services to users in Brazil. The bill uses vague terminology and does not clearly describe the specific requirements needed to comply. Instead, it grants ANATEL significant discretionary authority to define terms and create rules. While the vague language in the bill makes it hard to determine the specific obligations that would apply to U.S. companies, but, overall, the bill would at minimum increase compliance costs and may require the restructuring of business operations. Lastly, Bill 4691 would establish a general framework to protect freedom of speech online and regulate digital platforms. The bill proposes having ANATEL and CADE as co-regulators of digital platforms that have a certain number of users, and impose certain obligations to the designated digital platforms.

Network Usage Fees & Network Regulation: In 2025, Brazil continues to consider measures to apply ill-fitting or cumbersome regulations to value-added services, such as video-on-demand, streaming, or other over-the-top services (OTTs). ANATEL has expanded its authority through measures including Resolution 780/2025, which increases liability for marketplaces and digital platforms selling non-approved telecom products, extends conformity requirements to refurbished devices (see import policies above), and strengthens consumer protection enforcement. ANATEL's Resolution 780/2025 was adopted without consultation or regulatory impact assessment and imposes obligations with an unclear scope. The Supreme Court's reversal of the liability shield under Article 19 of the Internet Law has compounded uncertainty. The agency is also pursuing public consultations on OTT regulation, network usage fees, and 5G/IoT standards, signaling an intent to extend telecom-style oversight to streaming, platform, and digital service providers, raising extreme uncertainty for U.S. providers operating in Brazil.

Digital Services Tax: Despite multilateral efforts to align international taxation rules, the Brazilian Congress continues to introduce bills aimed at creating unilateral Digital Services Taxes (DSTs) that would directly affect U.S. companies operating in the country. USTR has already found that similar measures, such as France's DST, are actionable under Section 301. The implementation of these unilateral tax measures not only risks jeopardizing multilateral negotiations but also threatens U.S. businesses that fully comply with Brazil's taxes and should receive equal treatment compared to local companies. The Brazilian Congress is currently considering seven DST bills, and on July 18, President Lula publicly expressed support for such initiatives to charge taxes from U.S. digital service providers. The seven DST proposals in Brazil's Congress conflict with Brazil's existing tax system, which already taxes profit

remittances abroad, and contradict Brazil's ongoing tax reform efforts that aim to tax both digital and physical products and services equally. An additional tax exclusively targeting the revenue of multinational companies, that in practice will end up burdening mostly U.S. companies, would effectively create double taxation and unfairly disadvantage American companies competing with local providers offering identical services to Brazilian customers. The disproportionate nature of these bills is evident in data from Brazil's Federal Tax Authority from 2018 to 2022, which shows that digital services in Brazil generated average tax revenue of 16.4%, while non-digital private sector services contributed only 6.1% on average. The Brazilian government should focus its efforts and resources on achieving consensus through multilateral forums rather than implementing unilateral taxes that will discriminate against U.S. companies doing business in Brazil.

Copyright Taxes on Digital Platforms: Two significant legislative proposals in Brazil that could alter the copyright landscape for digital services and impose discriminatory taxes and obligations on U.S. technology companies:

- Bill 4968/24 (Senate, Dec 2024, Sen. Rodrigues) proposes a new remuneration right for copyright and related rights holders for content used by online platforms. A critical provision of this bill would mandate payment even in cases of unauthorized third-party uploads or where existing contractual agreements already permit the use of the work, introducing significant financial and operational risks for user-generated content platforms.
- Bill 2370/19 (Chamber of Deputies, Cong. Feghali) mirrors Bill 4968/24, aiming for broad copyright reform with uncapped liability and "must-carry" obligations for journalistic/artistic content, preventing platforms from avoiding payment by content removal.

Audiovisual Services: Brazil currently applies a Condecine tax on a per-title basis to films, pay-TV, and "other segments." This tax does not apply to video on demand (VOD) services. However, there are several bills – most notably #8889/2017 and #2331/2022 – pending in the Brazilian Congress that would introduce a new Condecine tax, set at 6% of gross revenue, to video platforms, including U.S. social media services hosting user-generated content, and assigns Brazil's film agency (ANACINE) to oversee compliance. The stated purpose of the new tax is to fund national content production through cultural promotion funds. However, access to these funds would be limited to companies directly engaged in content production, excluding most digital platforms that act primarily as intermediaries between creators and users. VOD services and the bills also impose other obligations on VOD video platforms, such as catalogue quotas, prominence for local works, prominent placement of Brazilian broadcasters on connected TV interfaces, and transparency obligations. These bills – most notably #8889/2017 and #2331/2022 – would disproportionately burden U.S. platforms, favoring domestic broadcasters with visibility and tax benefits, and act as a discriminatory digital trade barrier, impacting market access by American firms could undermine the viability of providers, chill investment, and reduce consumer choice.

Content Regulation: Brazil enacted the Digital Child and Adolescent Statute in September 2025, creating a comprehensive legal framework for minors' online safety. The law mandates robust age verification, parental controls, and strict rules for data processing and advertising targeting children. Services accessed by minors must prioritize their best interests, with privacy and safety by default. To expedite the law's enforcement, a decree was issued to accelerate the implementation timeline, reducing the compliance period from the originally planned one-year to just six months. Another presidential decree designated Brazil's National Data Protection Authority (ANPD) as the primary enforcement authority for the new law, tasked with ensuring adherence to new protective standards for minors in data processing and content moderation. Developments on this issue and guidelines/regulations issued by the

ANPD need to be closely monitored, especially considering the ANPD's broad remit over multiple regulatory subject matters relating to digital services.

Intermediary Liability: In June 2025, Brazil's Federal Supreme Court ruled Article 19 of the Marco Civil da Internet unconstitutional, removing a liability shield for internet application providers. This ruling introduced a new liability framework that holds platforms civilly liable for illicit third-party content, even without prior judicial takedown orders, creating significant legal uncertainty and disadvantaging U.S. companies. Platforms face increased, subjective liability for user-generated content, incentivizing overbroad content removal and harming freedom of expression. SMEs relying on these platforms to access Brazilian consumers may face stricter eligibility or exclusion, as platforms seek to mitigate risk from hosting their content. New compliance burdens, including due-process protocols and transparency reporting, further strain non-domestic platforms. On August 1, ANATEL expanded its telecommunications product certification framework, citing the Supreme Court's ruling. This now extends joint liability to online marketplaces and digital platforms involved in commercializing telecom products, even those only advertising or facilitating listings, without direct sales or logistics involvement. This broad interpretation forces marketplaces to ensure all telecommunications products are certified and compliant, verifying codes and preventing uncertified sales, with penalties up to BRL 50 million. U.S. marketplaces face heightened exposure for third-party non-compliance, a task outside their traditional scope and difficult to scale. This regime imposes disproportionate burdens on digital commerce platforms, creating legal uncertainty, increasing costs, and hindering foreign firms' entry into Brazil's e-commerce market. It raises concerns about proportionality, feasibility, and alignment with global digital trade principles, potentially restricting market access and deterring cross-border digital trade.

CIDE: The Contribution for Intervention in the Economic Domain (CIDE) is a 10% federal contribution on certain payments for royalties or technical services made by Brazilian entities to offshore recipients, in particular for a license or technical services that involve a transfer of technology into Brazil. *Law No. 10,332/2001* significantly expanded the scope of the tax, allowing the government to charge CIDE even when no actual transfer of technology occurs. As a result, many business operations started being taxed, increasing the cost of international transactions and directly impacting the competitiveness of U.S. companies that provide technology or expertise.

Marketplace Liability: The recent adoption of the above mentioned ANATEL Resolution No. 780/2025 also introduces a framework that disproportionately burdens online marketplaces, particularly foreign-based platforms, by extending joint liability for product certification to digital intermediaries. This includes platforms that merely advertise or facilitate product listings without participating in the sale or logistics chain. U.S.-based marketplaces operating in Brazil now face heightened legal exposure for third-party sellers' compliance failures, including the obligation to verify ANATEL certification codes and ensure product conformity—tasks traditionally outside the platform's operational scope and technically difficult to implement at scale. These new provisions create significant legal uncertainty and risk and may not only restrict market access but also deter cross-border digital trade and innovation. The resolution therefore raises serious concerns regarding proportionality, operational feasibility, and alignment with global digital trade principles.

Electronic Payment Services: In the past few years, the Brazilian Central Bank's (BCB) role as a regulator and a competitor has created a conflict of interest that affects EPS´ ability to compete effectively. The BCB's Competitiveness and Market Structure Department (Decem) oversees not only the development of policy that affects all payment schemes in the Brazilian market, but also the development and regulation of PIX, a real-time payment scheme (including its participation rules and licenses), which went live on November 16, 2020. Pix compete directly with U.S. payment firms. All Brazilian financial institutions with over 500,000 accounts were mandated to participate in the PIX scheme by November 2020. On June 15, 2020, U.S. payment networks partnered with WhatsApp and launched a new payments

solution to enable WhatsApp users in Brazil to transfer money and pay businesses. However, the BCB immediately suspended the payments program by abruptly modifying the payments regulation (through BCB Circular 4031 dated June 23, 2020), without notice or opportunity for public comment. Since then, the Central Bank's conflict of interest between a regulator and a product manager has intensified. Given the over-regulated environment of Brazil's payments industry, the Central Bank controls time to market, and can determine sector economics. Additionally, the Central Bank has been increasingly delegating supervisory functions to industry players instead of undertaking these itself.

Express Delivery Services: The 2025 NTE states that: " Brazilian Customs has established express delivery maximum per-shipment value limits of $10,000 for exports and $3,000 for imports," when in fact the maximum per-shipment limit is $1,000, placing U.S. operators in a yet more precarious position.

Data Economy: The Department of Innovation of the Ministry of Development, Industry, and Trade (MDIC) is considering policies and legislative proposals related to the "data economy" modeled after the European Union's Data Act, which impose discriminatory obligations on U.S. companies regarding the use of non-personal data. Although a formal proposal has not been released, there will likely be a public consultation on the matter by the end of the year with questions about how Brazil should implement a similar Data Act in the country. There are concerns that this proposal could unfairly target U.S. companies through specific thresholds.

Services Barriers - Telecommunications

6 GHz Spectrum Reversal and Reallocation: On December 31, 2024, Brazil's telecommunication regulator, Anatel, abruptly announced that it would reverse its 2021 decision allocating the upper 6 GHz band for unlicensed services by repurposing it for 5G, with the goal of holding a spectrum auction in October 2026. The regulator's action will disrupt millions of consumers and enterprises that invested in technology from U.S. companies utilizing the full 6 GHz band. Moreover, Anatel made the announcement without providing a formal opportunity for stakeholders to provide input. The reversal decision appears to have been motivated by efforts to promote China's spectrum priorities relating to the 6GHz band and 5G. Furthermore, Brazil's increasing technological partnership with China, as evinced in President Lula's visit to a Huawei factory in China, raises concerns about U.S. national security and economic interests.

Investment Barriers

Data Center Obligations: ANATEL's Resolution No. 780/2025 introduces stringent new requirements for data centers, including mandatory conformity assessments, enhanced operational resilience standards, and additional security and sustainability requirements. The regulation, implemented without public consultation, could particularly burden U.S. cloud providers who have already made significant investments in the country. Of special concern is the three-year transition period for existing facilities, which could require significant infrastructure modifications and investments, potentially affecting service continuity and market competitiveness.

Cambodia

Services Barriers

Content Moderation: Cambodia continues to face censorship, internet filtering, and blocking, with independent outlets often targeted during sensitive political events like the 2023 elections. A February 2021 sub-decree established the National Internet Gateway, creating a single point of entry for internet traffic. A 2024 notification requires companies to use a national domain name, raising concerns about potential abuse for content blocking and restricting foreign digital services, similar to China's "Great Firewall". Additionally, a draft Cybercrime bill from Cambodia's Interior Ministry could hold

intermediaries liable for third-party content and mandate data localization.Expected to be finalized by late 2025, the bill reportedly allows the government to control operating systems and duplicate data if companies fail to address cybersecurity threats, and includes vague prohibitions on defamation, "insulting, derogatory or rude language," and "false information" harmful to public order and “traditional culture”, with penalties including fines and imprisonment. It also permits internet traffic data collection for suspected criminals and criminalizes online content that “depicts any act or activity … intended to stimulate sexual desire”.

Data Localization Requirements: In addition to the draft Cybercrime Bill, data localization requirements are also found in the draft Cloud First Policy of Cambodia. The draft aims to accelerate digital transformation and public sector cloud adoption However, the mandates regarding data localization (specifically for Confidential data) and stringent data sovereignty requirements, while designed to protect national interests, introduce significant complexities and potential limitations that could, in practice, hinder the widespread, efficient, and cost-effective adoption of cloud computing. The policy mandates that confidential data (which includes sensitive categories like Government Classified Information, Personal Identifiable Information, and Financial Data) must be stored or processed within the in-country infrastructure of an MPTC accredited CSP or the government cloud. By limiting the storage of critical data to local infrastructure, ministries and institutions (M&Is) are prevented from accessing the massive, cost-efficient Public Clouds offered by global providers, whose infrastructure may be located anywhere.

Personal Data Requirements: Further, Cambodia released a draft Law on Personal Data Protection (LPDP) on July 23, 2025, which is inspired by the EU's GDPR. The draft law introduces rules for data processing, establishes data subject rights like access and erasure, mandates appointing a Data Protection Officer for certain organizations, and includes administrative fines for violations. It applies to both domestic and foreign entities processing personal data of individuals in Cambodia, with a proposed 2-year implementation period after it is enacted. Several provisions in the LPDP deviate from international best practices and create an unpredictable and difficult compliance environment, presenting significant barriers for U.S. service providers seeking to serve the Cambodian market. Key concerns include:

- disproportionately high administrative fines of up to 10% of annual turnover, which far exceed global standards and is not clearly tied to turnover related to the specific violation, creating immense financial risk;
- operationally challenging and rigid compliance timelines, such as requiring “immediate” action upon consent withdrawal by privacy subjects, and a 72-hour data breach notification triggered merely by “becoming aware” of an incident, which is often impractical;
- a broad “right to erasure” that lacks a balancing test to protect freedom of expression and fails to preclude a private right of action, which could lead to inconsistent enforcement and excessive litigation; and
- a high age of consent set at 16, which does not align with the widely accepted international standard of 13 and could limit teenagers' access to online services.

Services Barriers - Telecommunications

Local Testing Requirements (Telecommunications): The Telecommunications Regulator of Cambodia (“TRC”) is responsible for overseeing the “type approval” process for telecommunications equipment. Type approval is required to import telecommunications products and includes review of foreign standard test reports. The TRC imposes a variety of type approval and regulatory requirements, including enforcing country-of-origin requirements (e.g., separate certification needed for each country-of-origin for the same model of the product). In particular, the TRC requires suppliers to acquire test reports in the vendors’ name in

Cambodia for Small Form-factor Pluggable (“SFP”) modules that typically do not require certification in other countries. Reports from Original Equipment Manufacturers (“OEMs”) or Original Design

Manufacturers ("ODMs") are not accepted by the TRC. Additionally, type approval is required for line-cards (also not required in other countries). The current regulations are highly burdensome for U.S. suppliers because it is impractical to obtain certificates and type approval for line cards that cannot function independently. Lastly, the TRC also prohibits import of refurbished products.

The TRC's overly stringent enforcement of its type-approval guidelines is an unfair market access barrier that is out-of-step with practices in other countries' regulations and disrupts business operations and customer support in Cambodia. Furthermore, Cambodia made significant expansions to the scope of type approval without consultation or provision of transition periods.

Canada

Import Policies

CBSA Assessment and Revenue Management project: The Canadian Border Services Agency (CBSA) continues to pursue several concerning changes to customs procedures and practices that may conflict with Canada's customs and trade facilitation obligations in the USMCA and the World Trade Organization's Trade Facilitation Agreement. The CBSA Assessment and Revenue Management project, better known as CARM, is a multiyear initiative to change the Canadian importation process. The CARM system became the official system of record for assessing and collecting duties/taxes on imported commercial goods on October 21, 2024. Persistent issues with CARM's implementation, including system backlogs, compliance burdens, and procedural disruptions, have raised concerns among U.S. traders and logistics providers. These challenges risk undermining trade fluidity and supply chain reliability between the United States and Canada. NFTC's concerns in this section of the NTE around CARM persist. **NFTC urges USTR to emphasize that Canada should extend all transitory measures and make additional permanent changes to CARM to alleviate the backlogs and disruptions caused by the CARM program.**

Customs Act: Amendments to Canada's *Customs Act* introduced through the 2024 Budget Implementation Bill (*Bill C-19*) impose new obligations and potential liabilities on express carriers delivering goods into Canada. These provisions substantially alter the risk framework for small and medium-sized enterprises (SMEs) engaged in cross-border e-commerce. Under the revised rules, carriers continue to be held liable for additional taxes, duties, penalties, and related costs for up to four years after importation, even in cases where they act solely as intermediaries, requiring them to recover such costs from shippers after the fact. Such measures undermine trade facilitation goals under the USMCA and disproportionately affect smaller firms seeking to access the Canadian market.

C-2 – Stronger Borders Act : The Canadian government is proposing new legislation for border security. If enacted, C-2 includes new provisions related to: 1) Law enforcement and intelligence agencies will be authorized to make warrantless "information demands" compelling non-content information from service providers; 2) Productions orders for subscriber information; 3) Cross-border data sharing provisions which authorizes enforcement of foreign decisions to compel production of subscriber information or transmission data in the possession or control of a Canadian entity under the "MLAT Act"; and 4) new Authorized access to Information Act to require electronic service providers to facilitate access to and interception of information by authorized persons. Bill C-2 would give the Canadian government broader powers to access private information without a warrant and force services to install "technical capabilities" to access Canadians' encrypted communications and sensitive data. We have significant concerns that service providers will be required to enable backdoor access to, or the interception of, information processed within messaging or cloud services.

Technical Barriers to Trade

Artificial devaluation of innovative medicines through PMPRB: The Patented Medicines Prices Review Board (PMPRB) sets maximum prices for all patented medicines sold to public or private payers by referencing prices in other countries. In 2021, Canada removed the United States and Switzerland from the reference basket of countries to ensure that it referenced more countries with lower incomes and drug prices. Canada should either sunset the PMPRB or put the United States back in the reference country basket and continue to apply the PMPRB International Price Comparison Test using the Highest International Price standard.

Biased health technology assessments: Canada's Drug Agency (CDA) uses low and outdated monetary thresholds per life year gained when performing health technology assessments on clinically proven treatments. As a result, Canada's coverage recommendations for some new cancer and rare disease products are contingent on further price cuts of 70-90%. Canada should remove CDA's role in providing coverage recommendations on the cost-effectiveness of new medicines and instead ensure that recommendations focus on comparing the clinical effectiveness of treatments.

Market Access Delays (Pharmaceuticals): In Canada, it takes approximately two years following regulatory approval for a medicine to reach patients insured on public drug plans. This is due to lengthy sequential administrative processes and federal-provincial pricing negotiations through the pan-Canadian Pharmaceutical Alliance (pCPA) before individual jurisdictional funding agreements. In an ideal world, patients would not have to wait to access innovative medicines while officials and manufacturers discuss *behind-the-scenes* financial and administrative details. Canada should significantly reduce the additional bureaucratic delays following national regulatory approval to access public drug plan formularies managed by each province or territory.

Government Procurement

WTO Government Procurement Agreement Listing: Canada is a member of the WTO Government Procurement Agreement ("GPA"), which binds Members, including the United States and Canada, to reciprocal market access in government procurement. Shared Services Canada ("SSC"), a government agency that was formed in August of 2011, has not been listed in Canada's Appendix I Annexes of the WTO GPA. SCC is the Canadian government's largest procurer of information technology ("IT") products and services, as it brings together the IT resources from 42 departments.

Procurement Policies: As a result of trade tensions and sovereignty threats, the Canadian Government has introduced "Canada First" procurement policies – including digital sovereignty strategies - prioritizing local suppliers over large American hyperscalers. More recently and specifically, the Canadian government issued a Sovereign Cloud Request for Information, with the objective to discard non-domestic hyperscalers from procurement opportunities, and focus on working with local providers. This will impact foreign direct investors' ability to expand their services into procurement (particularly areas such as national security, defense, and healthcare), as well as regulated industries like financial services. U.S. companies also face discriminatory practices in the procurement of medicines and vaccines. This includes preferential treatment for locally manufactured vaccines, provincial-level preferences that are excluded from federal procurement decisions, pricing that overrides recognized product value, winner-takes-all tender structures, and a lack of transparency throughout the process.

Intellectual Property Protection

Copyright Act: Canada's Copyright Act lacks explicit provisions for AI-generated works, creating uncertainty about their copyrightability and ownership. The Copyright Act also doesn't include a specific exception for text and data mining, which are crucial for AI model training. While limited exceptions like fair dealing may apply, the absence of clear guidelines could restrict the use of copyrighted materials in AI development. As AI advances, Canada will need to update its copyright framework to address these issues and clarify AI-related activities.

Inadequate Patent Term Adjustment (PTA): The USMCA requires Canada to provide PTA for unreasonable delays during the prosecution and issuance of any patent. However, Canada has created a PTA framework which includes inequitable barriers that constructively undermine the treaty provision, and which will prevent American patent holders from obtaining compensation for unreasonable delays. The process to apply for PTA is burdensome, costly, and creates significant market uncertainty. Canadian patent holders do not face these burdens or lack of adequate adjustment in the United States. **NFTC encourages USTR to urge the Canadian government to provide up to 5 years of patent term restoration that runs consecutively with patent term adjustment instead of concurrently.**

Services Barriers

Online Streaming Act (C-11): In April 2023, the Canadian Government passed Bill C-11 Act to amend the Broadcasting Act,. The law and related rules promulgated by Canada's regulator can compel U.S. platforms to promote Canadian over U.S. content and force U.S. companies to make financial payments into funds that only Canadians can access. On June 4, 2024, the Canadian Radio-television and Telecommunications Commission (CRTC) announced that streaming services meeting certain thresholds (e.g., annual revenues of C$25 million or more in Canada) and not affiliated with a Canadian broadcaster will have to contribute 5% of their Canadian revenue starting in the 2024-25 broadcast year. In addition to the 5% levy payments which streaming services have already been required to start making, in November (absent any other developments) we expect more information on the investment obligation (IOs), which could be as high as 30% (which would be much higher than any existing IOs). CCIA recently completed an analysis estimating that Canada's new contribution regime for online streaming companies, including for music, could cost U.S. music and video services up to nearly US$7 billion by 2030. **NFTC encourages USTR to treat Canada's *Online Streaming Act* (C-11) as a deliberate and discriminatory measure against U.S. networks and streaming services.**

Québec Bill 109: On May 21, 2025, Québec's Minister of Culture et des Communications tabled Bill 109. The Bill's stated purpose is to promote discoverability of and access to original French-language cultural content in the digital environment. It will have major implications for U.S.-based streaming companies, as well as manufacturers of connected devices. It grants broad authority to the Québec Cabinet to enact regulations that will impose new registration requirements, reporting and potential French content quotas, accessibility and discoverability requirements on digital platforms and manufacturers of TVs and connected devices. It also creates a new administrative unit within the Ministère de la Culture et des Communications under the name "Bureau de la découvrabilité des contenus culturels" (the BDCC) and gives the BDCC broad powers to enforce the bill.

Data Localization: The Province of Québec adopted privacy legislation, known as Bill 64, in September 2021 that would make data transfers extremely difficult. The law only permits public and private sector entities (with limited exceptions) to transmit personal data outside of the province to jurisdictions with a level of protection equivalent to Québec's privacy law. The law will gradually come into force over the following three years. The U.S. International Trade Commission identified the law as a barrier to digital trade in its "Year in Trade 2021" report published in August 2022.

The Canadian federal government is also signaling its intention to introduce new privacy legislation in 2025, drawing heavily from the principles of the now-defunct Bill C-27, which stalled in January 2025. There are a number of concerns with this approach. First, the proposal is poised to introduce ambiguous or overly strict rules on the use of publicly available information for AI training. Furthermore, it includes renewed focus on "digital sovereignty" that may lead to new requirements for cross-border data flows and data localization. Such provisions increase compliance costs and legal uncertainty for U.S. companies, hinder the highly integrated U.S.-Canada digital market, and impede innovation in critical areas like the development of artificial intelligence. The USTR is urged to proactively engage the Canadian government to advocate for a legislative framework that is interoperable with global standards and promotes a fair and open digital marketplace.

Additionally, Shared Services Canada (SSC) issued a request for information (from August 13, 2025 through September 30, 2025) to inform the development of a sovereign procurement stream for Infrastructure-as-a-Service and Platform-as-a-Service. This framework would require all government data to be processed and stored in Canada, and providers, including parent companies, to be free from foreign laws allowing external government access. SSC cites a National Security Exception to bypass trade obligations. Canada's proposal excludes U.S. cloud providers based on ownership, not security, raising significant concerns that U.S. providers will be unfairly prejudiced in bidding for public sector contracts, making this a discriminatory trade barrier.

Digital Service Tax: Canada announced on June 29, 2025 the planned repeal of its Digital Services Tax (DST) before its first collection. The DST, adopted June 20, 2024, would have imposed a 3% tax on online services, primarily affecting U.S. firms and retroactively costing them an estimated US$3 billion in 2025. While collection is paused, reimbursements have yet to be made for payments made by industry in anticipation of the tax, and the law has yet to be formally repealed, leaving open the possibility of its revival.

News Media-Related Digital Service Taxes: Additionally, Canada's Bill C-18 (the Online News Act) enacted in June 2023, empowers the Canadian Radio-Television and Telecommunications Commission (CRTC) to mandate payments from large "digital news intermediaries" to news publishers for content reproduction. Inspired by Australia's News Media Bargaining Code law, C-18 targets specific U.S. companies (namely Meta and Google), as evidenced by Canadian lawmakers' statements in Parliament and the Parliamentary Budget Office estimates, which projected C$329.2 million annually would be paid to news publishers under the assumption that only Google and Meta would be implicated under the legislation, with 75% of that amount going to large broadcasters. Implementing regulations require platforms to pay at least 4% of their global revenue (adjusted for Canada's GDP ratio) for exemption. This has led to one of the target U.S. companies securing a five-year exemption after agreeing to an annual C$100 million payment to Canadian news organizations, while the other U.S. company ceased news linking in Canada. The law harms the user's access to the open Internet and threatens security and safety. It also conflicts with Canada's international trade obligations, including under the U.S.-Mexico-Canada Free Trade Agreement (USMCA) Articles 14.4 (Investment) and 15.3 (Cross-border Services) regarding National Treatment; USMCA Articles 14.5 (Investment) and 15.4 (Cross-border Services) regarding Most-Favored Nation Treatment; USMCA Article 14.10 regarding Performance Requirements; USMCA Article 19.4 regarding Non-Discriminatory Treatment of Digital Products and WTO intellectual property agreements. Prime Minister Mark Carney acknowledged the law's shortcomings in August 2025, suggesting that the government could seek to amend or repeal the law in view of its disruptive impact on the dissemination of news and information online.

Artificial Intelligence: In June 2022, the Government of Canada tabled the Artificial Intelligence and Data Act (AIDA) as part of Bill C-27, the Digital Charter Implementation Act, 2022. Bill C-27 has now lapsed but AI elements are expected to be re-introduced. AIDA proposed significant new powers for the

government to regulate ‘high-impact’ AI systems, but included overly broad definitions of ‘high-impact’ systems that could capture low-risk use cases. AIDA’s unclear “person responsible” definition further complicates matters, potentially requiring the revelation of proprietary information. The lack of clarity poses risks for innovators and online service providers, especially with the government's intent to reintroduce AI elements, possibly including content moderation under “high-impact”, as articulated in an October 2023 letter from then Minister of Innovation, Science and Industry, François-Philippe Champagne. The proposal also included monetary penalties of up to 3% of global revenues and introduced a first of its kind criminal enforcement provision for non-compliance. This regulatory approach poses significant risks to U.S. companies and the U.S.-led risk-based approach to AI governance and will create a massive compliance burden on leading U.S. AI researchers and developers and threaten interoperability across North America.

Separately, the Competition Bureau’s 2024 consultation on its discussion paper on AI and competition will need to be monitored. The paper is part of the Bureau’s broader inquiry on how competition is developing in AI markets, the potential for regulation to protect and promote competition in AI markets, and potential measures to address competitive harms arising from AI. Industry advises monitoring this process to ensure that any regulatory oversight on competition and AI is balanced, flexible, and nationality-neutral. The generative AI market is diverse, with no current signs of competitive harm from AI input access; and existing competition laws are sufficient to address future issues, including the potential for algorithmic collusion.

Content Moderation: In 2021, Canada proposed a framework to address harmful online content, including 24-hour takedown requirements, monitoring, filtering, and site-blocking, raising concerns about censorship and overbroad definitions. On February 26, 2025, the Online Harms Act was introduced, imposing strict obligations on social media platforms, including 24-hour removal deadlines for child exploitation and non-consensual intimate content. This bill would establish a powerful Digital Safety Commission with authority to issue codes, impose fines (up to 6% of global revenue), conduct inspections, and potentially mandate company funding, raising concerns about encryption due to possible scanning requirements. The Conservative Party also proposed an alternative bill (C-412, *Protection of Minors in the Digital Age Act*) to impose "duty of care" obligations, parental controls, private rights of action for "serious harm," and prohibit certain interface designs,[#] risking over-enforcement and frivolous lawsuits. Although these proposals expired, the Liberal government announced in June 2025 its intention to revive and expand the effort to address AI developments.

Additionally, the Office of the Privacy Commissioner of Canada (OPC) recently concluded its exploratory consultation on age assurance, which ran from June to September 2024, and is now proceeding to draft formal guidance for online service providers. While the consultation is officially complete, this process is advancing in concert with pending federal legislation, specifically Bill S-209, which seeks to mandate age verification for access to certain online content and is currently being considered in committee in the Senate. The Privacy Commissioner has endorsed this Bill, signaling a coordinated regulatory and legislative push toward mandatory, high-friction age assurance systems. For U.S. industry, this trajectory raises significant concerns that constitute a potential non-tariff barrier to trade, including: substantial operational costs and technical burdens of implementing Canada-specific systems, which disproportionately impact small and medium-sized enterprises; the creation of legal and financial liability from collecting and storing highly sensitive datasets that link verified identities to private online behavior; and regulatory uncertainty driven by a lack of clear technical standards, data protection safeguards.

Chile

Technical Barriers to Trade

Non-Harmonized Digital Rules: Chile's digital regulations serve as a significant technical barrier to trade and present challenges for foreign technology companies operating in the market. Most notably, the country requires cybersecurity incidents to be reported within 3 hours, compared to the international standard of 72 hours. This regulatory divergence functions as a non-tariff barrier, requiring foreign companies to create costly Chile-specific compliance systems. The financial impact is substantial - according to the "AI Unlocking Ambitions" study commissioned by AWS, companies must dedicate 19% of their investment capital just to meet local regulatory requirements. The situation is further complicated by Chile's fragmented institutional framework, where overlapping jurisdictions and conflicting requirements create additional barriers for international companies without local expertise. This regulatory landscape, lacking a central coordinating body, has led to inconsistent policies across agencies that could hinder the development of a coherent national digital strategy.

Express delivery shipments: Under the U.S.-Chile Free Trade Agreement (FTA), Chile committed to expedited customs procedures for express shipments and to allow a shipper "to submit a single manifest covering all goods contained in a shipment transported by the express shipment service, through, if possible, electronic means". Chile is currently implementing a low-value imported goods VAT collection mechanism. The secondary regulations create a complicated rule in the express delivery regime to separate goods below $500 from those above $500.

Services Barriers

Electronic Payment Services: U.S. Electronic Payment Service (EPS) suppliers face critical regulatory challenges in Chile due to General Instruction No. 5 ("ICG No. 5") issued by the Chilean Competition Tribunal (TDLC) and upheld by the Supreme Court. These measures impose structural limitations on U.S. EPS' ability to update their rules, standards, and scheme fees without prior agreement from licensees or approval from the National Economic Prosecutor's Office (FNE). In particular, Instruction 4.6.e mandates that any change to the payment system rules undergo a negotiation or review process that can extend for months.

This framework severely restricts operational flexibility and poses a material risk to its ability to respond in a timely manner to technological advancements, evolving regulatory requirements, and emerging security threats. The delay and uncertainty introduced by these obligations undermine the capacity to maintain a secure, competitive, and innovative payments environment.

Moreover, the requirement to provide 60 to 90 days' advance notice for adjustments to scheme fees and merchant risk categorization further impedes U.S. EPS suppliers' ability to adapt dynamically to market conditions. While intended to foster competition, these constraints create a rigid regulatory environment that threatens to slow innovation and investment in Chile's digital payments ecosystem.

Data Localization: The Chilean financial regulator (CMF) has rules related to the general IT outsourcing of services (RAN 20-7) that allow cloud adoption in country and abroad, but require financial institutions to have local data centers for contingency purposes, when processing relevant data / critical workloads abroad. The 2017 version of the regulation issued by the CMF did not allow for an exception to requirements on local infrastructure for contingency purposes. Following a public consultation process in 2019, the CMF agreed to create an exception for the aforementioned requirement, however many financial institutions in Chile cannot benefit from the exception, as they do not meet CMF's requirements

on “adequate” operational risk management. This has become a blocker for the advance of data hosting services in Chile, as it effectively funnels a broad swath of financial institutions to local infrastructure offerings. During June 2023, the CMF committed the review of RAN 20-7 as part of 2023 priorities, but has not been able to deliver.

Data Protection: Additionally, Chile approved a new Personal Data Protection Law in 2024, inspired by the EU’s General Data Protection Regulation (GDPR). The law is set to enter into force in December 2026. A significant issue is that the law’s implementation is heavily dependent on the issuance of numerous secondary regulations by a new Data Protection Agency, which will only become operational concurrently with the law itself. This creates substantial legal and operational uncertainty for U.S. companies. Critical mechanisms for enabling international data transfers—such as standard contractual clauses, binding corporate rules, and adequacy decisions—have not yet been developed. The absence of this essential regulatory framework makes it impossible for businesses to prepare for compliance, potentially disrupting transatlantic data flows that are vital for the digital economy. It is essential that Chile ensure all critical secondary regulations are finalized and published months in advance of the law's entry into force, or alternatively, that the transition period is extended to provide businesses with adequate time to adapt.

Potential Barriers in New Cybersecurity Framework Law: Chile recently approved a new Cybersecurity Framework Law (in effect as of March 1, 2025), modeled after the EU’s Networks and Information Security Directive 2 (NIS 2). While the objective of enhancing cybersecurity is laudable, its implementation could create significant trade barriers if not properly designed. It is critical that the law and its subsequent regulations, and Chile’s overall cybersecurity framework, promote regulatory interoperability with internationally recognized standards, such as the NIST Cybersecurity Framework and ISO standards. This would prevent the creation of unique, country-specific requirements that would be burdensome for U.S. firms. Furthermore, the framework must not impose bureaucratic hurdles that hinder compliance for companies without a physical or legal presence in Chile. For example, requiring a *Clave Única* (Chile's state-issued digital ID) for registration or compliance would effectively exclude foreign companies whose implementation and cybersecurity teams are located outside of Chile. The law must be implemented in a manner that recognizes the global nature of cybersecurity operations and the Digital Economy.

Intellectual Property Protection

Patent Linkage: Despite being a clear obligation under the U.S.–Chile Free Trade Agreement, Chile has yet to implement a formal patent linkage system, leading to IP infringements on both the public and private market. These linkage issues stem from the disconnect between the authorization granted by the local medicines regulatory agency (ISP) and the patent rights granted by the National Intellectual Property Office (INAPI), where this absence of mandatory consultation allows unauthorized products to enter the private market and even the public procurement system. This gap in enforcement results in multiple costs for American pharmaceutical companies in the form of increased legal and operational costs, regulatory uncertainty, and distorted competition. Chile should implement a robust patent linkage system that includes a) legal framework mandating the ISP consult the patent registry before granting sanitary registration b) administrative interface between INAPI and ISP to flag potential conflicts and c) effective and balanced procedural rules and due process mechanisms for notification and appeals.

Inadequate regulatory data protection (RDP): Chile does not provide adequate protection for undisclosed test data, leading to possible unfair commercial use and unauthorized disclosure by third parties. This RDP system contains weaknesses ranging from inappropriate procedural barriers to seek and receive RDP to ambiguous carveouts precluding RDP for certain pharmaceutical innovations (e.g., new uses, formulations, compositions, dosage forms, etc.). Specifically, Chilean regulators inappropriately

require innovators to request RDP for specifically identified data and deny RDP in the event subsets of clinical trial data were voluntarily disclosed publicly. Chile should align its regulatory data protection standards with global norms to prevent unfair treatment of American innovation.

China

Services Barriers

Electronic Payment Services: When China joined the WTO in 2001, it committed to allowing non-Chinese EPS companies to compete and do business in its domestic market on equal terms with Chinese companies, including by processing renminbi-denominated transactions in China. While U.S. EPS suppliers have continued to process "cross-border" transactions in China for decades, which primarily involve purchases by individuals traveling to and from China as of October 2025, only two EPS suppliers have secured the license to operate in the domestic market.

Restrictions on Cloud Computing: Even though U.S. cloud service providers ("CSPs") have stimulated innovation and application of cloud services around the world, China's regulators impose market access restrictions for foreign companies, which require Value-Added Telecoms ("VAT") licenses. China has launched "pilot" programs to open its cloud market in Beijing, Shanghai, Shenzhen and Hainan "free trade zones," but CSPs still need to fulfil the previous localization requirement.

Market Access for Cloud Services: China implements a licensing system for telecommunications business operations. Only companies established in China, after obtaining a telecom business license, can engage in telecom business activities. Foreign companies' participation in the value added telecommunication (VAT) sector is highly restrictive. Based on *Telecommunications Regulations of the People's Republic of China*, *Classification Catalogue of Telecommunications Services*, and *Special Administrative Measures for Foreign Investment Access (Negative List) (2021 Version),* foreign companies are still denied access to the business sectors critical to cloud services nationwide, namely B11 Internet data center (IDC) business, and B12 content distribution network (CDN) service. Although the Ministry of Industry and Information Technology announced the expansion of the opening-up of VAT sector on a pilot basis in April 2024, the opening-up is only limited to four designated areas (Beijing, Shanghai, Shenzhen and Hainan "free trade zones"), posing commercial and technical difficulties for cloud service providers with interconnected data centers both inside and outside those areas.

In addition, China imposes sector-specific requirements for cloud services in industries such as financial services and smart vehicles, in effect prohibiting the usage of public cloud services. These unfair restrictions are exacerbated by other market access restrictions: connectivity requirements, restrictions on the ability to engage in cross-border data transfers, and requirements to localize computing infrastructure. Many international financial institutions and vehicle manufacturers are unable to use public cloud services globally for enhancing operational resilience and efficiency, and achieving consistent internal standards (e.g., risk management functions).

Critical Information Infrastructure. The CII Security Protection Regulation, effective from September 1, 2021, mandates enhanced protection of CII. This regulation promotes the procurement of "secure and trustworthy" network products and services, potentially resulting in unequal treatment between domestic and foreign companies' products. Companies identified as CII operators face additional obligations under Chinese security legislation, including mandatory certification, assessment, and cybersecurity reviews. In a similar vein, the concept of "important data" was introduced in Article 37 of the Cybersecurity Law (CSL) in 2017. In recent years, a series of guidelines have been continuously issued to guide data processors in data classification and identification of important data, imposing an increasing compliance burden on companies that own important data. Moreover, the ambiguous definitions and opaque

recognition criteria for CII and important data, coupled with the expanding application by industry regulators, have created high compliance burdens and potential entry barriers for foreign companies seeking access to certain industries or customers.

Cybersecurity Review: The *Cybersecurity Review Measures (CSRM)* were revised on January 4, 2022, making it mandatory for CII operators procuring network products and services, and online platform operators conducting data handling activities that influence or may influence national security, to proactively apply for a cybersecurity review. The review is an opaque process, presumably assessing a host of factors, including the security, openness, transparency, and diversity of sources of products and services; the reliability of supply channels, as well as the risk of supply disruptions due to political, diplomatic, and trade factors. For example, the Cyberspace Administration of China (CAC) launched and failed a cybersecurity review of Micron in early 2023, resulting in a demand for CII operators to stop purchasing its products. With vague criteria and broad scope, China's cybersecurity review regime could be abused and used to discriminate against foreign technology providers, thus creating an entry barrier for many MNCs.

Secure and Controllable ICT Policies: The Chinese government has implemented secure and controllable ICT policies through various laws and regulations, including the *Cybersecurity Review,* the *Critical Information Infrastructure Protection Measures*, and the *Cryptography Law*. These policies have been reinforced under the banner of technological self-reliance and security since the 14th *Five Year Plan* in 2021. In practice, these policies have been widely used, creating obstacles for foreign ICT products to get into sectors ranging from government, CII operators, and even State-Owned Enterprises (SOE). In past years, the concept of SOE Cloud and State Cloud in China has further exemplified the policy.

Encryption Requirements: China's 2019 Cryptography Law includes restrictive requirements for commercial encryption products that "involve national security, the national economy and public interest" which must undergo a security assessment, including critical information infrastructure. This has resulted in unnecessary restrictions on foreign ICT products and services. Recent regulations have added to concerns that China's encryption requirements are being used to discriminate against American companies. For example, China amended the Commercial Cryptography Administrative Regulations in April 2023. The amended regulations fail to support interoperable international standards and use internationally standardized encryption algorithms. Furthermore, the regulations reflect an extensive import license/export control scheme and impose requirements applicable only to CII and party and government organs to networks above Multi-Level Protection Scheme ("MLPS") level three.

Furthermore, on October 7, 2023, the State Cryptography Administration ("SCA") published the Administrative Measures for Security Assessment of Commercial Cryptography Applications (Measures), which came into effect on November 1, 2023. The measures proposed the concept of Important Network and Information Systems without providing definitions. Unless these important ambiguities are favorably resolved, these regulations will impose unfairly high compliance costs and create entry barriers for American companies that rely on internationally accepted encryption algorithms.

Digital Trade Barriers / Data Localization and Cross-border Data Flow: China imposes complex restrictions on the storage, movement, and access to data across borders, making it very difficult and costly for foreign companies to manage their global operations. In 2021, China released *Personal Information Protection Law* (PIPL) and *Data Security Law* (DSL), which, along with the CSL implemented in 2017, established an overarching regulatory framework on data. The framework sets out three pathways for the cross-border data flow, namely security assessments, protection certification and standard contracts.

On security assessment, CAC's *Measures on Data Exit Security Assessment*, effective from September 1, 2022, stipulate the requirements for cross-border transfer of important data and personal information by CII operators and other companies that reach certain thresholds of data. The Measures put forward specific requirements for data exit security assessment, stipulating that data processors shall conduct a data exit risk self-evaluation before applying for data exit security assessment. Alongside the Measures, the regulations and standards on protection certification and standard contracts of personal data cross-border flow were also promulgated, forming a cross-border personal data flow management mechanism.

Noting that the existing data transfer framework is impeding economic growth and impractical for domestic and foreign businesses operating in the global economy, on March 22, 2024, CAC promulgated new provisions on promoting and regulating and cross-border data flows, which would limit instances in which the aforementioned cross-border personal data flow mechanism would apply or a data exit security assessment would be necessary. In particular, the new provisions allow that personal data transfers due to human resource management and contractual transactions, such as cross-border e-commerce, cross-border payments, plane ticket purchases and hotel bookings, and visa applications be exempted under the cross-border personal data flow management mechanism. While the new provisions do not further elaborate on the scope of "important data", they stipulate that data processors are not required to apply for a data exit security assessment if they have not been notified by the relevant authorities, or if the data has not been publicly declared as important data. Pilot Free Trade Zones within Beijing, Tianjin, Shanghai and Hainan may also develop their own negative list of data for which the cross-border personal data flow mechanism would not apply. Beijing, Tianjin and Shanghai authorities have started to publish such negative lists.

While the People's Bank of China, the National Financial Regulatory Administration, the China Securities Regulatory Commission, the State Administration of Foreign Exchange, CAC, and the National Data Administration jointly issued the *Compliance Guidelines on Promoting and Regulating Cross-border Data Flow in the Financial Sector* in April 2025, the guidelines were only shared with selected financial institutions, making it difficult for the industry and other related stakeholders such as technology services provider to work out viable compliance measures with the regulators.

Intellectual Property Protection

Data Requirements for NMPA Clinical Trial Applications: NMPA has in recent years required an unusually detailed review of manufacturing and control process for biologic CTA filing at the Center for Drug Evaluation (CDE) and sample testing requirements of vaccine material at NIFDC at the CTA stage, which requires biopharmaceutical companies to reveal proprietary information about manufacturing steps and test methods and additional data beyond what is required on the face of the CTA application materials. This is not consistent with international practice and is particularly concerning for innovative biologic and vaccine products. The additional information and testing requirements delay the clinical trials and raise concerns about potential disclosure of confidential information (including manufacturing and commercial information) at early clinical phase.

Patent Term Extension Conditions (Pharmaceuticals): China introduced the PTE to the revised Patent Law in 2021, and the detailed guidelines took effect on January 20, 2024. The new Implementation Rules establish specific basic conditions for PTE eligibility, which weaken the value of PTE and its ability to encourage innovative medicines to enter China and benefit the Chinese patients. For example, PTE is restricted to "innovative drugs" and certain "improved new drugs". According to the definition in Registration Classification of Drugs, this refers to drugs that have not been approved in other countries before submitting applications in China, following the 'new-to-the-world' standard. Also, the protection scope during the extended patent term is confined to the approved new drug, specifically limited to the

relevant technical solution for the approved indication. Finally, the narrow scope of PTE protection may have unintended consequences, which may potentially impact the scope of protection of innovative products.

Patent Linkage (Pharmaceuticals): In 2021, the new law and various measures were released to implement the patent linkage system in China. While aspects of an effective early dispute resolution system are reflected in these measures, the system still has deficiencies. For example, there is no procedure that provides for patent certification modification or opposition. Moreover, ANDA filers can circumvent patents that are listed on the PL platform by using a different dosage form. This patent linkage system must be improved in a manner that advances innovation: 1) ANDA filers should make certifications with respect to relevant patents they know or should have known listed in the PL system even if these patents are technically listed for a different product having the same API (e.g., a product with different dosage form). 2) ANDA filers should be afforded an opportunity to amend/correct their statements.

Delayed Review of Patent Applications (Pharmaceuticals): An unreasonable delay at the patent office (CNIPA) has resulted in China's National Medical Products Administration (NMPA) approval of generic versions of products that have a patent pending.

Anticompetitive Practices

Domestic Substitution: In recent years, China has enacted a range of industrial policies aimed at promoting its own technological self-sufficiency to reduce the dependence on American technology. In particular, China's "secure and controllable" measures put American companies at a severe disadvantage against Chinese firms. For over ten years, China has required its public sector and state-owned enterprises to purchase so-called "secure and controllable" Chinese products; it has also imposed domestic research and development ("R&D") requirements and considers the location in which R&D was conducted as a cybersecurity risk factor. These "secure and controllable" standards are not transparent, and are not accessible to American companies.

Colombia

Import Policies

Invoicing: Colombia allows traders to submit electronic copies of invoices; however, a physical copy must still be attached to the shipment. While the Colombian Government has reported ongoing efforts to upgrade its customs digital systems, progress has been limited, and no definitive timeline has been confirmed.

Customs: Colombia is introducing an advanced customs declaration requirement for all formal shipments, excluding express shipments. Importers will be required to file declarations 48 hours before goods arrive, and failure to submit a final import declaration within two days (air) or five days (sea) may result in goods being deemed abandoned. These strict timelines and penalties could significantly disrupt U.S. exports, particularly for small and medium-sized enterprises (SMEs) unfamiliar with the new procedures.

Penalties: Colombia's proposed new customs penalties regime expands DIAN's authority to demand data from all actors in the supply chain, including carriers and couriers. It introduces fines based on shipment value for documentation errors—often disproportionate to the actual harm caused—and allows for immobilization of goods, shifting liability to intermediaries.

Technical Barriers to Trade

The National Food and Drug Surveillance Institute (INVIMA) delays: In recent years, the pharmaceutical industry has experienced worsening delays in regulatory approval times, resulting in significant market access barriers. In November 2023, the Administrative Court of Cundinamarca issued an emergency measure in response to the growing shortage of drugs in Colombia due to the delays in regulatory approvals. The Court mandated a contingency plan, developed jointly by INVIMA and the Ministry of Health, detailing necessary actions to reduce the shortage of drugs in Colombia, including accelerating regulatory approvals. This order was revoked by the Consejo de Estado, eliminating the obligation for INVIMA and the Ministry to proceed with these plans. In December 2024, the Administrative Court of Cundinamarca again mandated the continuation of an urgent response plan to address ongoing medicine and supply shortages.

Substandard biologics regulation: On September 18, 2014, Colombia issued Decree 1782, which establishes marketing approval evaluation requirements for all biologic medicines. As part of the Decree, Colombia created an unprecedented "abbreviated" pathway for the registration of non-comparable products, which is inconsistent with WHO guidelines and accepted standards in the United States and other countries, and which could result in the approval of medicines that are not safe and/or effective. Industry urged the Colombian Government to remove this third pathway from the Decree but was unsuccessful.

Services Barriers

Digital Services Tax: Colombia's implementation and proposed expansion of its digital services tax (DST) represent a significant trade barrier that disproportionately affects U.S. companies. The provision regulates Significant Economic Presence (SEP) and was initially established at a 3% rate in January 2024. The Colombian government now seeks to increase this to 5% through a September 2025 tax reform bill. This measure directly violates the United States-Colombia Trade Promotion Agreement (USCTPA) through discriminatory treatment of U.S. providers and contradicts international tax norms. The tax structure effectively functions as a de facto tariff by increasing costs for imported digital services while favoring domestic providers. Most concerning is the reduced rate offered to companies establishing local presence, violating USCTPA Article 11.5's prohibition on local presence requirements. The proposed 5% rate would position Colombia's DST among the highest globally, creating substantial market access barriers and potentially violating multiple USCTPA provisions, including restrictions on digital products and services under Articles 2.3, 2.8, and 15.3.

Restrictive Network Usage and Digital Service Regulations: Colombia's proposed "Internet Solidarity" bill, introduced in August 2025, creates a new trade barrier through excessive regulation of digital services, despite the Communications Regulatory Commission's (CRC) earlier finding against implementing "Fair Share" contributions. The legislation establishes a new "Digital Intermediary Service Providers" category that subjects U.S. cloud providers to burdensome registration requirements, mandatory authority cooperation, and content moderation obligations. The bill's broad scope and six-month implementation timeline for regulations create significant operational uncertainty for U.S. technology companies. Of particular concern is the combination of expanded CRC authority to demand provider information while establishing internet access as a fundamental right, potentially enabling future implementation of network fees or similar financial obligations that could disadvantage U.S. providers in the Colombian market.

Electronic Payment Services (Tax):The tax regulation establishes income, VAT and other municipal withholding taxes applicable to credential payments. However, this regulation has not evolved with the financial industry and has not been applied to identical payments made by newer payments systems such

as digital wallets, QR code payments, e-commerce payment buttons, the public real-time payment system (Bre-B), which is now operating, and other payment methods such as cash. This discourages the adoption of card acceptance among merchants. Withholdings sum up to ~5% of transaction amount: Income: 1.5%, VAT: 2.85%, Municipal Tax: ~0.4%. The reduction in cash flow for merchants derived from accepting credential payments constitutes a significant barrier to the general adoption of credential payments acceptance. These tax asymmetries create unjustified advantages for companies participating with other payment methods (cash, QR, transfers) and prevent the fully successful deployment of US credential companies in the country's payment ecosystem.

Intermediary Liability: Colombia has not met its 2006 U.S.-Colombia Free Trade Agreement (FTA) obligations regarding Internet service provider protections. A 2018 revision to its copyright law omitted online intermediary protections, leaving intermediaries that export services to Colombia vulnerable to civil liability. The law also lacks standard exceptions like text and data mining. A new AI bill (Bill 043/2025) further compounds concerns, imposing a "permission-first" regime requiring express consent from rights holders for AI training. This approach would create insurmountable barriers to AI development and deployment, increasing legal uncertainty for online services in Colombia.

Government Procurement

Restrictive Cloud Services Procurement: Colombia has established a significant trade barrier in its $218 million public sector cloud services market through the deliberate expiration of its Cloud Computing Framework Agreement (CCFA) and subsequent preferential treatment of state-owned enterprises. The government's failure to formalize the CCFA extension beyond August 31, 2025, coupled with Presidential Directive 06, which promotes Internexa (a state-owned enterprise) as the primary technology procurement vehicle, creates direct discrimination against U.S. cloud providers including AWS, Microsoft, Google, and Oracle. This action threatens existing government systems operated by U.S. providers and likely violates multiple USCTPA provisions regarding non-discriminatory treatment and transparent procurement procedures. The barrier not only jeopardizes commercial interests but also raises concerns about bilateral security cooperation and the protection of sensitive government data through increased reliance on non-U.S. technology providers.

Intellectual Property Protection

Compulsory licensing (Pharmaceuticals): The threat of unmitigated compulsory licensing in Colombia is a continued risk for the innovative biopharmaceutical industry. In April 2024, the Colombian Government issued a compulsory license (CL) on an antiretroviral medicine on vague and ambiguous grounds. Since that action, the Ministry of Health (MoH) has publicly signaled its desire to use the threat of CLs as a price "negotiation" tool despite other and more effective options that would not compromise incentives for innovation.

Regulatory data protection (RDP) failures: Colombia fails to respect existing legislation that would otherwise provide RDP upon approval of novel pharmaceutical products.

Restrictive patentability criteria: Contrary to its obligations under the World Trade Organization (WTO) Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), Colombia does not grant patents for second uses.

Effective patent enforcement: Despite having a specialized court under the auspices of the Superintendence of Industry and Commerce (SIC) designed to address IP infringement matters, Colombia needs to implement effective early resolution mechanisms that provide for the timely resolution of patent disputes before marketing approval is granted to infringing follow-on products during the patent term through increased collaboration between INVIMA and SIC.

Investment Barriers

Cost containment measures focused solely on the biopharmaceutical industry: Government measures to improve the sustainability of the Colombian health system have focused solely on the biopharmaceutical industry and have not addressed broader issues within the pharmaceutical supply chain or other health care sectors. For example, in 2020, the Colombian Government issued regulations to limit expenditures on medicines not included in the publicly funded Health Benefit Plan (HBP) based on historical levels that would effectively restrict new innovative medicines from entering the country. These measures have been criticized for their technical shortcomings by virtually all sectors of the health system and academia.

New drug price regulation methodology: A draft circular was published by MOH in September 2023, outlining a new method for pricing new medicines. In addition to international reference pricing (IRP), it established a value-based pricing model based on clinical value assessments undertaken by the *Instituto de Evaluación Tecnológica en Salud* (IETS). In March 2024, the National Drug Pricing Commission (NDPC) issued Circular 18 of 2024 adjusting the methodology for regulations in place since 2013. This Circular allows for more restrictive IRP by expanding the number of reference countries from 17 to 19 and cherry-picking countries to include those that are less supportive of innovation. In addition, if a drug is declared by the government to be of public interest, then the price will be set to the lowest price in the reference basket of countries.

The Superintendency of Commerce issued Resolution 35379: This resolution authorized the intervened HMOs to jointly coordinate purchasing processes for high-cost medications (invoking an exception to competition regulations) with the goal of leveraging collective bargaining power to secure price reductions and curb escalating pharmaceutical expenditures. However, the implementation of these measures has triggered significant legal and regulatory uncertainty. The resolution compels companies to sell directly to HMOs—entities whose financial standing remains precarious—while obliging the industry to absorb the costs of dispensing and delivering medications, all under a regime of prices significantly below established regulatory thresholds.

Costa Rica

Technical Barriers to Trade

Market Access Delays (Pharmaceuticals): It can take up to 18 months for pharmaceutical products to progress from approval to registration due to human resource issues. While mechanisms exist to expedite the review of high-standard medicines, they lack the efficiency to manage the volume of requests and reduce response times—resulting in significant delays. To address inefficiencies in current regulatory mechanisms, it is crucial to establish systems that prioritize medicines targeting unmet medical needs and those already authorized by high-standard regulatory agencies.

Services Barriers

Extraterritorial application of local regulation (EPS): Costa Rica is exerting extraterritorial authority over U.S. Electronic Payment Services providers (EPS) and U.S. banks through a Central Bank of Costa Rica's (BCCR) regulation of inbound cross-border payments. In March 2020, the Congress of Costa Rica enacted Law 9831 granting the Central Bank of Costa Rica (BCCR) authority to set price control measures to the card payments system, including a wide range of electronic service providers with operations in Costa Rica. In November 2022, the BCCR updated its regulation and capped among others, the international Interchange Reimbursement Fee (XB IRF), and the international Merchant Discount Rate (XB MDR). This measure restricts U.S. commerce of digital services by setting a cap on the fees that

U.S. banks can charge for transactions conducted in Costa Rica using debit or credit credentials issued in the U.S. As a result, this regulation affects commercial agreements between U.S. EPSs and U.S. banks, even though these agreements are governed by U.S. law.

The BCCR's regulation of inbound cross-border payments favors Costa Rican entities to the detriment of U.S. banks and EPS suppliers. The regulation disproportionately affects U.S. banks as the 60% of inbound cross-border transactions in Costa Rica are with payment credentials issued by U.S. banks.

NFTC recommends that USTR urge Costa Rica to withdraw the extraterritorial provisions established by the BCCR that affect the business operations of U.S. financial institutions regarding cross-border card payment transactions. Specifically, we recommend the removal of Article 44 and any references to cross-border transactions since they fall under the jurisdiction of countries other than Costa Rica.

Tax Asymmetry: While tax withholdings on card payments continue to create an uneven playing field for U.S. EPS, a proposal from the Costa Rican Ministry of Finance to address this issue has stalled. The plan, which would extend tax withholdings to include the Central Bank's mobile payments platform, Sinpe Móvil, has faced strong opposition from the Central Bank, political actors, and the general public, reducing its viability.

We urge USTR to emphasize to Costa Rica the critical need for an equitable payments ecosystem, highlighting the direct negative impact of the current fiscal asymmetry on U.S. EPS and proposing a definitive solution: either impose the withholding tax across all payment methods or eliminate it entirely.

Ecuador

Import Policies

Reweighing Procedures: Ecuador's reweighing (*repesaje*) procedures are a major non-tariff barrier in the import process, causing delays, added costs, and uncertainty. All shipments are weighed multiple times—despite advance data being provided—under inconsistent and discretionary processes that vary by port and operator. These delays, compounded by lengthy inspections and lack of time limits, significantly increase import costs and extend clearance times by several days, directly impacting U.S. exporters' ability to deliver goods efficiently and competitively.

Courier Regime: Additionally, Ecuador's Category B courier regime imposes several non-tariff barriers that hinder U.S. exports. The mandatory $20 fee per shipment has raised costs for U.S. exporters and discouraged small-scale trade. Eliminating or reducing this fee would help restore competitiveness. Furthermore, the current weight and shipment frequency limits under Category B are restrictive, especially given the fee and VAT already applied.

Services Barriers

Restrictive Artificial Intelligence Regulations: Ecuador's proposed artificial intelligence regulations, introduced by the Data Protection Authority (SPDP), represent a significant trade barrier that threatens U.S. companies' market access and operational capabilities. The "Regulation for the Guarantee of Personal Data Protection Rights in the Use of Artificial Intelligence" creates multiple compliance challenges through jurisdictional overreach, as it conflicts with Ecuador's Digital Transformation Law (LOTDA) which designates MINTEL as the AI governance authority. The regulation imposes discriminatory operational burdens on foreign technology providers through mandatory human supervision requirements, complex traceability standards, and expansive audit rights. Of particular concern are the blanket prohibitions on crucial AI applications, including real-time biometric

identification systems and synthetic content generation, which effectively bar U.S. companies from deploying innovative technologies in the Ecuadorian market. These restrictions, coupled with excessive compliance costs, create disproportionate barriers for U.S. businesses, especially affecting technology startups and SMEs. The proposed framework contradicts Ecuador's international commitments to facilitate digital trade and promote technological innovation, while establishing unnecessary obstacles that particularly impact U.S. companies' ability to compete effectively in Ecuador's digital economy.

Electronic Payment Services: Current tax regulation establishes income and VAT withholdings applicable to credential payments which discourage the adoption of card acceptance among merchants. Simplified tax regimen “RIMPE” establishes an exemption from these withholdings only for taxpayers (individuals and legal persons) with an annual income ranging from USD 1 to USD 20.000, but any other taxpayer is subject to withholdings up to ~13% of transaction amount. The reduction in cash flow for merchants derived from accepting credential payments constitutes a significant barrier to the general adoption of credential payments acceptance and prevents the fully successful deployment of US credential companies in the country´s payment ecosystem.

Egypt

Services Barriers

Electronic Payment Services: Central Bank of Egypt (CBE) ambitions to promote domestic payment infrastructure (scheme) and push for co-badge with international payment networks is forcing such networks to adjust their business models in accordance with the government's political ambitions to enhance domestic payment infrastructure rather than independent / market-led commercial ambitions..

Data Localization Requirements: The Personal Data Protection Law, which aims to regulate data collection, processing, and storage, is awaiting the release of its Executive Regulations (ERs). These ERs, initially anticipated in early 2025, will provide businesses with specific compliance guidelines and introduce a one-year transition period after issuance. The delay in their release, reportedly due to recent political and crisis management priorities, has left businesses in a state of uncertainty.

Content Regulation: In 2018, Egypt enacted a law requiring all social media users with more than 5,000 followers to obtain a license from the Supreme Council for Media Regulation (SCMR). Additionally, in May 2020, Decree No. 26 of 2020 established a detailed licensing regime for media and press outlets, including online platforms. This regulation requires platforms to remove harmful content within 24 hours and obligates international companies to establish a local representative office to provide legal liability and act as a point of contact for content-related matters. Licensing fees for international platforms are set at EGP 3,000,000, and there are no explicit safe harbor protections for foreign companies, which may increase compliance complexity.

In June 2024, the SCMR reiterated its licensing requirements, issuing notifications to all digital and satellite platforms operating in Egypt to comply with relevant regulations under Law No. 180 of 2018, Prime Ministerial Decree No. 418 of 2020, and SCMR Decision No. 29 of 2020. Platforms were given a 90-day grace period to regularize their status, with potential consequences for non-compliance, including financial penalties, service blocking, or license revocation. The enforcement of these requirements is supported by the National Telecommunications Regulatory Authority (NTRA) and the Central Bank of Egypt (CBE), which can restrict payments and access to non-compliant platforms.

While the SCMR has primarily focused on over-the-top (OTT) platforms such as regional streaming services, international platforms face additional requirements to meet compliance standards. Social media

platforms, although not the current primary focus, also fall under the same regulations. While Decree No. 92 of 2020 introduced an accreditation model for social media platforms, offering a less demanding alternative to licensing, the accreditation model is not widely emphasized by the SCMR, and platforms are often guided toward pursuing full licensing. This can introduce additional operational and financial requirements, particularly for international entities navigating Egypt's regulatory environment.

El Salvador

Government Procurement

Lack of regulatory framework for MEAs: A significant barrier to accessing innovative medicines is the absence of regulatory frameworks that facilitate negotiations through managed entry agreements (MEAs) within public procurement systems. Without a structured framework for managed entry agreements, healthcare systems face challenges in incorporating innovative treatments into their formularies—ultimately limiting patient access to cutting-edge therapies. Implementing clear and structured regulatory frameworks that facilitate managed entry agreements can enable effective negotiation of prices and terms for innovative medicines. Additionally, adopting value-based pricing models helps ensure that the cost of innovative medicines reflects their clinical benefits, while making them more accessible to patients.

Intellectual Property Protection

Inadequate regulatory data protection (Pharmaceuticals): El Salvador does not provide adequate protection for undisclosed test data or other data generated to obtain marketing approval for pharmaceutical products, leading to possible unfair commercial use and unauthorized disclosure by third parties. El Salvador should align its regulatory data protection standards with global norms to prevent unfair treatment of American innovation and meet its IP obligations under CAFTA–DR.

Ethiopia

Services Barriers

Electronic Payment Services: In 2023 the National Bank of Ethiopia opened up the digital payment market to issue payment instruments and operate payment systems licenses to foreign operators. Kenya-based Safaricom has obtained a license to issue payment instruments with a reportedly high investment protection fee (USD 150M). A high investment protection fee to allow international payment networks to obtain a license to operate payment systems may be a barrier to allowing more international companies the opportunity to operate in the market and generate economic growth.

The European Union

Import Policies

Carbon Border Adjustment Mechanism (CBAM): The Carbon Border Adjustment Mechanism ("CBAM") imposes a requirement on businesses to report on embedded emissions of imports. In January 2026, CBAM will also add a carbon price on imports in emission-intensive sectors (cement, iron, steel, aluminum, fertilizers and electricity) whose production/related emissions have not been taxed (or not at the same level as the EU) in the producer's country. This is important to ICT companies – because these companies use some of these components in our products. Additionally, businesses will have to purchase and surrender "CBAM Certificates."

Even for small imports, CBAM imposes a significant compliance burden. The first year of reporting created uncertainty as U.S. suppliers were forced to grapple with a lack of clear guidance, available tools, and time and resources invested in compliance. The next steps of the CBAM implementation will further raise costs for importers in Europe since free Emissions Trading Scheme (ETS) allowances will be gradually phased out.

CBAM discriminates against products from countries like the United States that do not have equivalent carbon emissions taxation schemes in place.

Technical Barriers to Trade

EU Corporate Sustainability Due Diligence Directive and Sustainability Omnibus Package: The EU's 2023 Corporate Sustainability Due Diligence Directive (CS3D) threatens to impose substantial and disproportionate compliance costs on U.S. businesses, particularly due to its extraterritorial scope. For most U.S. companies operating in the EU, the CS3D will impose sustainability-related due diligence requirements on their U.S. parent companies and any of their subsidiaries, impacting relations with suppliers anywhere in the world, regardless of the existence of a relevant EU nexus. The EU institutions are currently revising the CS3D as part of the EU's 'Omnibus I Package', which proposes amendments to certain aspects of the law's due diligence obligations, penalties and civil liability. A final agreement is expected in late 2025.

The 'Omnibus I Package' could address key issues faced by U.S. businesses in relation to the CS3D, including: (1) the law's unprecedented extraterritorial reach, which impacts supplier relationships across all subsidiaries, regardless of location and EU nexus; (2) requirements to adopt prescriptive due diligence systems across global operations, which will lead to costly and time-consuming risk management exercises; (3) burdensome supply chain obligations, which are extended indefinitely and make it impossible for companies to know when they have done enough to mitigate sustainability risks; (4) significant (potentially uncapped) and unpredictable financial penalties; and (5) fragmented litigation risks (even if mandatory EU-wide civil liability is removed from the CS3D, fragmented national civil liability systems create significant legal exposure for U.S. businesses across 27 EU Member States).

EU Deforestation Regulation: The EU's Regulation on deforestation-free products ("EUDR") creates a due diligence process for companies regarding the import of deforestation-risk products such as palm oil, timber, cocoa, coffee, leather, wood, pulp and furniture, among others. U.S. companies market collaboration suites that include wood furniture and other pulp/wood fiber products.

Pursuant to the EUDR, businesses must provide a statement demonstrating compliance with all relevant local laws in each exporting country along with full traceability of the goods throughout their supply chains. The regulation also provides for periodic reviews that would expand the regulation's scope to cover new products and ecosystems. Information requirements include geolocation data to the exact plot of land where the covered material was produced and documentation demonstrating that there has been no deforestation or degradation of forest in the relevant area since December 2020.

EUDR is unfair because it imposes significant compliance costs and creates conflicting legal requirements due to its extraterritorial application (*i.e.*, imposing compliance obligations on suppliers in third countries). The EUDR also makes sourcing raw material more challenging due to current and potential third country suppliers' inability and lack of capacity to comply with the regulation. While the EU keeps postponing the entry into force of the EUDR, a substantial review of the rules or the removal of the law as such is critical.

Pharmaceutical Market Access Barriers:

- **France**: France combines price cuts, rebates, revenue clawbacks and pharmaceutical-specific taxes to drive net prices on innovative medicines to be among the lowest in Europe. When setting prices, France asserts that 60% of new innovative medicines provide no added benefit over current treatments. Older inferior medicines and generics are often used as price benchmarks, and increasingly excessive rebates are required by the statutory health insurance system. New innovative medicines supposedly awarded "price stability" are still subject to excessive rebates that can push net prices far below the agreed-to price floors. Revenue clawbacks and pharmaceutical-specific taxes further reduce spending on already devalued medicines with calls for additional reductions.
- **Germany**: Germany rejects clinical trial evidence to assert, when setting prices, that 55% of new innovative medicines provide no added benefit over current treatments. The Federal Joint Committee (G-BA) selects comparators for these required benefit assessments, often using older inferior medicines and generics as price benchmarks (in 74% of assessments). New innovative medicines are often priced 10% lower than older patent protected medicines deemed to offer the same benefit and new medicines deemed to offer a minor added benefit are often not priced higher than older medicines offering less benefit. An additional 20% rebate is imposed on all patent-protected medicines used in combination therapies. Germany has also maintained a price freeze for all medicines reimbursed by statutory health insurance since 2010.
- **Italy**: Italy imposes revenue clawbacks, driven by underfunded hospital budgets, that have rapidly become unsustainable for biopharmaceutical manufacturers. In 2024, manufacturers were required to pay back approximately €2B of €17B in hospital medicine revenues (AIFA). The Italian Medicines Agency (AIFA) deems only a third of new innovative medicines as "fully innovative," which means many new medicines are not exempted from revenue clawbacks nor placed immediately on regional formularies. Pricing and reimbursement processes at the national level already delay patient access to new medicines, which is exacerbated by further unnecessary delays and uncertainty in listing products on regional formularies.
- **Spain**: Spain sets prices of new innovative medicines by using older inferior medicines and generics in Spain and other countries as price benchmarks. The Spanish government selects the comparators from a broad group of treatments and then chooses from the drugs with the lowest prices as the comparator. When recommending coverage of new medicines, the Inter-Ministerial Commission on Medicine Prices (CIPM) examines a broad group of existing treatments and then selects the medicine with the lowest price as the comparator. Regional authorities often require additional assessments, rebates and price cuts that further undervalue new innovative medicines and further restrict and delay patient access. In addition, Spain requires mandatory discounts of 7.5% for all innovative medicines and a revenue clawback of 2% on all retail pharmacy sales to further reduce spending on already devalued medicines.

Government Procurement

Plans for European Preference in EU Public Procurement and Funding Instruments: Since taking office in December 2024, the new European Commission has repeatedly supported the introduction of European preference criteria in EU public procurement and funding procedures. The reform proposals are due to be published in 2026 and raise concerns amongst U.S. businesses with operations in Europe. The European Commission plans to launch a comprehensive public procurement reform in 2026. As part of the reform, the Commission plans to propose European preference criteria for strategic sectors. Similarly, the recent Defence EDIP/SAFE proposals and the Clean Industrial Deal reference EU content requirements as one of the criteria and a mandate for funding. We expect the upcoming Industrial Decarbonisation Act (IDA) and Cloud and AI Development Act (CAIDA) to include similar requirements. The strategic sectors under scope are yet to be defined but could include clean energy

technologies, along with critical technologies that are deemed important for Europe's industrial and economic security, such as AI, quantum, and advanced semiconductors.

The EU's proposed European preference is discriminatory and contrary to the EU's international trade obligations, which incorporates a principle of non-discrimination and requires that treatment accorded to the goods and services of other GPA Parties shall be no less favorable than the treatment accorded to domestic goods and services. European preference criteria and EU content requirements will limit U.S. businesses' ability to access parts of the EU government procurement market, impacting a wide range of industrial sectors including defense, clean tech and critical digital technologies. In addition, the EU is also progressively adding localization requirements in new Research and Innovation projects (eg, under Horizon 2020), notably those related to 6G and secure connectivity projects, excluding U.S. companies from the initiatives.

Croatia - Public Procurement Barriers: Croatia's Public Procurement Act requires all tender documents to be submitted in Croatian, creating exclusionary procedural hurdles for foreign bidders. In parallel, government ICT projects are shaped by APIS IT, the state-owned agency that operates the Government Cloud and manages roughly 90% of critical public sector systems. This centralization embeds a de facto preference for state-run infrastructure, limiting opportunities for U.S. cloud providers to compete on equal terms. These practices restrict cross-border participation and investment.

Greece - Energy Efficiency Requirements in Procurement: Under Greece's Recovery and Resilience Facility (RRF), the Ministry of Finance requires that all data centers used in funded digital projects be listed as participants in the European Code of Conduct on Data Centre Energy Efficiency (EU CoC). While the EU CoC is a voluntary initiative, Greece has made it a mandatory eligibility condition for RRF projects. Because U.S. CSPs' data centers are not on this registry, they are automatically disqualified from RRF-related tenders, despite meeting equivalent or higher international standards (EN 50600, ISO). This exclusionary procurement practice restricts U.S. participation in Greece's largest EU-funded digital modernization projects.

Ireland - Public Procurement Barriers: Despite Ireland being home to extensive U.S. cloud infrastructure, its public sector remains a laggard when it comes to cloud adoption. A principal reason for this is the refusal of its authorities to establish a cloud procurement framework that would facilitate the purchase of services from U.S. CSPs. Under intense pressure from industry, the Irish procurement authority sought to establish such a framework in 2024. That process, however, ended in failure, with the procurement authority insisting on unworkable terms and conditions that no U.S. CSP could meet. A leaked internal Government briefing note cited the extraterritorial application of the U.S. CLOUD Act – which it likened to the Chinese Cybersecurity Law – as a red-line issue. It also suggested that "U.S. political turmoil" gave rise to excessive risk, thereby precluding the use of U.S. cloud services by the Irish public sector.

Intellectual Property Protection

Injunctions for SEPs Licensed on FRAND terms: European courts routinely issue injunctions against U.S. companies for alleged infringement of standard essential patents ("SEPs") without adequately considering patent owners' commitments to license these SEPs on fair, reasonable, and non-discriminatory ("FRAND") terms. To be able to continue to export to Europe, the U.S. companies are often forced to take excessively costly licenses for not only the allegedly infringed European patents but also related patents around the world, including U.S. patents. Put differently, bad actors circumvent the American judicial process to unfairly target U.S. companies. In fact, companies from foreign adversary countries are successfully using this tactic to create trade barriers in Europe, thereby maximizing the patent royalties that it collects from U.S. companies.

Companies that contribute their technology to industry standards, such as Wi-Fi or 5G, set by Standards Setting Organizations ("SSOs") are contractually obligated to license their SEPs on FRAND terms. But if the owner of a SEP is able to obtain an injunction against an accused infringer who is implementing the standard, the implementer is faced with a choice between paying potentially excessive royalties or losing market access, even when they are willing to license on FRAND terms. This is increasingly the situation in Europe today because of the practices of German courts and, more recently, the Unified Patent Court, which is empowered to issue injunctions in multiple European jurisdictions simultaneously. In theory, European competition law should constrain courts from awarding injunctions to SEP owners who charge excessive royalties. In practice, however, the German courts and the Unified Patent Court are quick and frequent in labeling the accused infringers as "unwilling licensees," subjecting them to injunctions.

By contrast, the U.S. courts follow the Supreme Court's 2006 decision in *eBay v. MercExchange* and do not award injunctions in SEP disputes given that money damages, more specifically damages based on FRAND terms, are adequate remedies. The EU Court's pattern of issuing injunctions on U.S. companies for alleged infringement of SEPs unfairly restricts market access and imposes significant costs on U.S. businesses.

The EU Commission proposed a regulation in April 2023 to standardize Standard Essential Patent (SEP) licensing, creating a SEP registry and essentially checks administered by the European Union Intellectual Property Office (EUIPO) to promote transparency and Fair, Reasonable, and Non-Discriminatory (FRAND) license terms – the regulation is unfortunately on hold at this stage.

Services Barriers

Digital Markets Act (DMA) Implementation: The Digital Markets Act (DMA), adopted in 2022, is an ex ante competition regulation that designated six U.S. companies and one Chinese firm as 'Gatekeepers'. 'Gatekeepers' are subject to strict restrictions on the use of data, obligations on data portability and access, and requirements on interoperability. 'Gatekeepers' are also prohibited from engaging in a range of business practices often considered pro-competitive, forcing them to de-integrate offerings from different areas of their portfolio that were previously organized into a single, easy-to-use product. As a result, U.S. companies have had to redirect substantial internal resources away from product development and innovation to instead focus on regulatory compliance. Some of these product changes have significantly degraded the quality of services and generated complaints from European consumers. Compliance costs for each of the five U.S. "gatekeepers" are estimated to average around $200 million annually, totaling up to $1 billion annually, and require extensive engineering hours, vastly exceeding the EU's initial per-gatekeeper cost of EUR 1.4 million ($1.64 million). Now, the European Commission is subjecting U.S. 'Gatekeepers' to large fines and significant business model changes. A mandatory review of the DMA by May 2026 could expand its scope to include new services (e.g., GenAI, cloud). Some policymakers and competition authorities are already suggesting such an expansion. In addition, we see ongoing politicized use of the 'Gatekeeper' designation in unrelated legislation as a further way to target the designated companies. No European companies have been designated as 'Gatekeepers'.

Data Act / Data Governance Act: The Data Act regulates access to and transfer of data generated by connected products and related services in the EU. The regulation entered into force in January 2024, and its main provisions started to apply in September 2025. The regulation mandates sharing of commercial data and the transfer of trade secrets under certain conditions. It also creates new discriminatory barriers that limit data sharing with companies designated as 'Gatekeepers' under the DMA resulting in primarily U.S. companies being at a distinct disadvantage compared to European and other non-U.S. entities in a constantly innovating and growing digital market.

For cloud providers, the Data Act imposes price caps for multi-cloud use, whereby the exchange of data

between different providers may only be charged at cost. Data transfers when a customer switches to an alternative cloud providers must be free of charge. While cloud providers may recoup data transfer costs that are directly linked with such transfers (incremental costs), the Data Act disregards that the costs incurred by each provider for the fixed assets related to data transfers and interconnection vary significantly. Some U.S. providers invest heavily in developing custom networking hardware and software, scaling out their fiber network globally, and interconnecting in many locations with many providers. Such a strategy requires years of sustained, high-cost investment, whereas other strategies that rely on using intermediary third-party networks for interconnection might involve minimal investment. In sum, the Data Act risks penalizing those who have made significant long-term investments in advanced network infrastructure, with U.S. cloud providers being the most harmed.

Additionally, EU's Data Governance Act, enforceable since September 24, 2023, implements restrictions on the transfer of certain non-personal data held by public intermediaries to third-party countries, where the data is protected by EU trade secrets or intellectual property laws. These restrictions are similar to the General Data Protection Regulation (GDPR) ranging from "adequacy decisions", consent, and standard contractual clauses, as well as an outright ban for sensitive non-personal data. While the GDPR governs restrictions for personal data, the DGA extends these obligations to non-personal data.

The restrictive data measures under the Data Act and the Data Governance Act risks penalizing those companies that have made significant long-term investments in advanced network infrastructure, with U.S. cloud providers being the most harmed.

Content Moderation / Digital Services Act: The Digital Services Act (DSA) creates new rules alongside existing safe harbors for the handling of illegal third-party content on hosting and intermediary services in the EU, such as video-sharing services, social networks, and online marketplaces. In addition, the DSA creates a new classification of companies called Very Large Online Platforms (VLOPs) - a grouping that disproportionately targets U.S. companies, based on a presumption that services with more than 45 million active users present "systemic risk", irrespective of any specific risk assessment. The DSA imposes obligations such as: notice & takedown systems for hosting services; 'know your business customer'; strict transparency and reporting obligations; risk assessments, yearly audits; obligations to disclose the main parameters used in their recommendation systems; data access; and requirements to appoint a compliance officer. Fines can reach up to 6% of annual turnover.

On April 24, 2023, the European Commission designated the first very large online platforms and search engines. Indeed, out of the 20 services designated, the majority ended up being U.S. firms. The DSA was weaponized to incorporate regulations on a variety of other topics not initially germane to the stated goal of online safety. For example, the inclusion of restrictions on personalized targeted advertising undermines the horizontal normative purpose of the DSA proposal and harms European companies along with U.S. firms. Throughout implementation, the European Commission continues to use the DSA to further regulate online services beyond the scope of the legislation. We see ongoing politicized use of the VLOP designation in unrelated legislation as a further way to target the designated companies.

Electronic Payment Services: The European Commission and the European Central Bank are continuing to drive a European payment sovereignty agenda that is geared at making instant payments the "new normal", reducing reliance on International Card Schemes, and Europeanizing the payment value chain in Europe. Responding to geopolitical volatility is increasing central bank and regulator influence over market participants, and towards those objectives. This remains evident in the political support for the European Payment Initiative, which notably excludes non-European players from participating. The finalization of the negotiations on the instant payments regulation in 2024 has also been a step forward, with some of its measures to apply over 2026. Discussions continue on the European Commission proposals to review the Payment Services Directive (PSD3/R), and a proposal for Financial Data Access

(FIDA) framework, with the aim to improve consumer protection and competition in electronic payments as well as to develop fairer access and use of data in the EU Digital Single Market. Separately, both the Council of the EU and the European Parliament continue discussing the regulation on a retail Digital Euro, with political skepticism over the project still present. As currently envisaged, it gives extensive power to the ECB as both the issuer of the Digital Euro and the scheme manager while also overseeing most of the competitors to the future digital currency. Despite little progress on the legislative side in Brussels, the European Central Bank has vowed to keep advancing across several key elements of the digital euro project. In fact, as of October 2025, it is in the "preparation phase," focusing on finalizing the scheme rule book and selecting providers for developing parts of the needed infrastructure.

EU Cybersecurity Certification Scheme for Cloud Services (EUCS): The European Commission has developed several policies seeking to restrict market access for U.S. cloud service providers (CSPs), particularly through the use of 'sovereignty requirements' (i.e., restrictions on foreign-owned and/or foreign-headquartered companies). The EU Cybersecurity Certification Scheme for Cloud Services (EUCS) was proposed in 2020 to harmonize the cybersecurity certification process for cloud services in the EU, but became contentious due to the introduction of sovereignty requirements, which would have prevented U.S. CSPs from serving customers in the public sector and certain regulated industries. These requirements were removed from the draft in March 2024, but adoption was suspended because of continued disagreement between EU countries. The Commission is now focused on the upcoming revision of the EU Cybersecurity Act (CSA) – the underlying legal basis for EUCS and other certification schemes – which is planned for Q4 2025. The public consultation on the CSA revision indicated that the Commission may use this opportunity to include sovereignty requirements across all future certification schemes, in addition to EUCS.

Network and Information Security 2 (NIS2) Directive Transposition/Implementation: While the NIS2 Directive aims to create a harmonized cybersecurity framework across the EU, the transposition process grants Member States significant leeway in interpreting and implementing its provisions.

This flexibility has led to a fragmented landscape of national requirements, as highlighted by the early transposition efforts of Croatia, Hungary, and Belgium, and the various draft proposals. Areas exhibiting variations in national interpretations include, among other things, scope, reporting, audits and certifications. The Hungarian transposition, for instance, adds some (sub)sectors to the original NIS2 sectors while the draft Czech Republic transposition demonstrates divergence in its definition of "important" and "essential" entities, potentially leading to discrepancies in which organizations fall under the scope of the regulation. Diverging reporting obligations can be seen in the Croatian draft transposition and the audit and certification requirements vary across the countries having already transposed NIS2.

These discrepancies pose significant challenges for organizations operating across multiple EU Member States. They face navigating a complex web of diverging requirements, potentially increasing compliance costs and creating an uneven cybersecurity landscape within the EU. Such divergence creates significant hurdles for pan-European providers, who now face:

- Disproportionate Burden: Navigating a complex web of national requirements strains resources and stifles innovation. The need to comply with multiple, potentially overlapping, regulations diverts time and resources away from core business operations and cybersecurity enhancements.
- Reduced Competitiveness: Increased compliance costs and complexity, without a corresponding improvement in security decision-making, put pan-European providers at a competitive disadvantage compared to entities operating solely within less regulated Member States.
- Barrier to the Single Market: Divergent requirements create unnecessary obstacles for companies operating across borders, hindering the free flow of services and potentially fragmenting the Digital Single Market. This runs counter to the principles of a unified digital space within the EU.

- Reduced Effectiveness of NIS2: The administrative burden associated with compliance can overshadow the directive's core objective which is enhancing cybersecurity. Instead of focusing on proactive measures and long-term strategies to counter emerging threats, organizations become bogged down in navigating and adhering to a complex regulatory maze.

To fully realize the potential of NIS2 and achieve a truly robust cybersecurity landscape within the EU, addressing this fragmentation is crucial. Member States must strive for greater harmonization of national requirements, ensuring consistency and interoperability across borders and encouraging the adoption of existing, widely recognized, international standards in order to streamline compliance and reduce unnecessary duplication of efforts. The European Union Agency for Cybersecurity (ENISA) has already highlighted the benefits of such an approach in its guidance on the European Electronic Communications Code (EECC), advocating for the use of established international standards to reduce compliance burdens on providers operating across multiple EU countries.

Cloud and AI Development Act (CAIDA): In the EU AI Continent Action Plan, published in April, the Commission announced plans for a new Cloud and AI Development Act (CAIDA). The proposal is expected in Q1 2026, and will be accompanied by EU-wide guidelines for public sector cloud procurement. Through CAIDA, the Commission aims to boost EU 'technological sovereignty' by promoting investment in 'homegrown' cloud infrastructure and increasing domestic compute capacity for AI. While the proposal is still pending, the Commission has already announced its intention to include measures to ensure the availability of 'highly secure EU-based cloud services' for 'critical use cases'. In meetings with industry, the Commission has confirmed that it plans to include sovereignty requirements in CAIDA to reserve a part of the public sector market (and potentially other strategic sectors) for EU CSPs. Together with EUCS, these initiatives aim to deny U.S. CSPs access to a substantial share of the EU market. Such risks have already manifested in individual tenders, which have explicitly excluded U.S. CSPs from participation. One way this risk could materialize more systematically is through a legal definition or set of criteria for 'sovereign cloud' in CAIDA. This definition could emphasize European ownership and headquarter location, or legal guarantees requiring exclusive EU jurisdiction and operational control. The definition could then be used in supply chain risk management requirements for 'critical sectors', or in the upcoming guidelines on public sector cloud procurement. These could work in combination with sovereignty requirements in the revised CSA – and subsequently EUCS – to exclude U.S. CSPs from large segments of the EU market.

Digital Networks Act: Since 2022, the European Commission has sought to introduce network usage fees (network fees), which would require large digital service providers – primarily U.S. technology and content providers – to subsidize the infrastructure of European telecommunications network operators (telcos). Despite the EU's commitment in the EU-U.S. Joint Statement that it will not adopt or maintain network fees, the Commission is now considering backdoor measures – particularly in the upcoming Digital Networks Act, expected in December 2025 – that would effectively function as network fees, resulting in additional compulsory payments from U.S. technology and content providers to European telcos.

Specifically, due to continued lobbying from European telcos, and despite broad opposition from industry, consumer associations, civil society organizations and telecoms regulators, the Commission is considering using the Digital Networks Act to extend the European Electronic Communications Code (EECC) to Internet Protocol (IP) interconnection. This would make internet-enabled Content & Application Providers (CAPs) and Content Delivery Networks (CDNs) subject to out-of-court dispute resolution mechanisms in commercial disputes with telcos. The introduction of these dispute resolution mechanisms would allow European telcos, who control access to internet users as 'termination monopolies', to launch interconnection disputes against CAPs and CDN providers, and extract additional payments for the delivery of internet traffic to users. This would result in a proliferation of disputes against CAPs and CDN

providers that deliver the majority of internet content, with U.S. providers being the primary targets. By multiplying disputes against U.S. CAPs and CDN providers, and building on the precedent set by these disputes, European telcos will be able to establish *de facto* network fees.

In addition to considering the introduction of backdoor network fees, the Commission is also evaluating an extension of the EECC to 'private networks' operated by large technology and content providers. This approach would result in an asymmetric regulatory intervention, mainly impacting U.S cloud services and infrastructure (including submarine cables), and satisfying ambitions from European telcos to become alternatives to U.S. cloud through regulatory intervention rather than market competition. Relatedly, in **Italy**, AGCOM's recent efforts to require CAPs to be subject to telecoms regulations and thus be subject to dispute regulation mechanisms provides similar cause for concern.

EU AI Act: The EU AI Act establishes a horizontal risk-based framework to regulate AI systems in the EU. The regulation entered into force in August 2024, triggering the gradual phase-in of its provisions over a 36-month period. It is now being supplemented with implementing rules and standards to operationalize its requirements for general-purpose AI, low-risk AI and high-risk AI. Despite some alignment with OECD work, the lack of clarity in key definitions in the AI Act undermines the effectiveness of this law and could hinder AI adoption in Europe by both EU and U.S. companies. Problematic definitions include AI systems, general-purpose AI models, and the classification of high-risk and prohibited AI. The broad definition of "high-risk" applications, along with burdensome compliance requirements and steep fines, imposes new compliance burdens on U.S. companies operating in the EU, and could dampen innovations and create legal uncertainty and new obstacles for products and services that are already subject to a multitude of regulatory mandates. Compliance requirements for "high risk AI" are administratively cumbersome and may not be technically possible for firms to adhere to with certainty, given obligations such as requiring human oversight. The problem is compounded by the ambiguous allocation of responsibilities within the AI value chain. Furthermore, the vague wording of certain prohibited systems creates legal uncertainty and risks banning low-risk applications.

CEN and CENELEC, the European standardization bodies, have launched a dedicated technical committee (JTC 21) to develop harmonized standards that will support the implementation of the AI Act, including a framework for AI trustworthiness and standards for AI risk management and quality assurance. However, current estimates indicate harmonized standards will not be ready until mid-2026, which creates timing challenges given the regulatory requirements for high-risk AI will begin applying in August 2026. Industry is therefore requesting a delay in the application of these requirements, which the European Commission seems open to including in targeted legislative amendments, expected in the upcoming Digital Omnibus. It remains unclear whether the standards developed in JTC 21 will be fully consistent with existing ISO standards (e.g., ISO 42001). Divergent standards would require businesses to adapt, at least in parts, to EU-specific requirements.

In addition, the AI Act also requires providers of general-purpose AI models to disclose a "sufficiently detailed" summary of their model training data. The Commission has developed a template for these disclosures, which was finalized in July 2025. Industry stakeholders have raised concerns about the technical feasibility and commercial sensitivity of granular training data disclosure requirements, particularly regarding the protection of trade secrets. It remains to be seen whether the Commission will allow companies not to disclose trade secrets in the template. It also remains unclear whether the Commission will enforce the AI Act's suggestion of applying EU copyright law to any general purpose AI model, regardless of where its training was conducted. This would contravene copyright territoriality principles.

EU Data Act Article 32 on International Governmental Access and Transfer: The EU Data Act establishes rules and "safeguards" for foreign governmental bodies' access requests to non-personal data

stored in the EU. Specifically, Article 32 of the EU Data Act (2023/2854) provides that data processing services "shall take all adequate technical, organizational and legal measures, including contracts, in order to prevent international and third-country governmental access and transfer of non-personal data held in the Union where such transfer or access would create a conflict with Union law or with the national law of the relevant Member State".

Article 32 of the Data Act makes U.S. companies responsible for potential conflicts in law relating to governmental access to data. At a minimum, this de facto item requires companies to conduct and publish evaluations of U.S. and other non-EU laws equivalent to the Transfer Impact Assessments (TIA) under the General Data Protection Regulation (GDPR) for non-personal data, which is disproportionate to the risk presented. GDPR TIAs are already very complex for U.S. companies providing data processing services for *personal* data. In a maximalist scenario, it could force U.S. companies to localize non personal data infrastructure and operations to provide the requisite guarantees. This measure is specifically targeted at and discriminates against U.S. companies due to EU concerns around U.S. governmental authorities' requests for information.

Digital Fairness Act: The European Commission is assessing whether there are gaps in the EU's consumer regulations, and evaluating possible regulatory solutions, as part of its Impact Assessment for a future Digital Fairness Act (DFA). The breadth of the range of topics they are examining presents a risk for business disruption, including for U.S. businesses, and uncertainty in the broader digital economy. An outcome that introduces intrusive rules around business models and service design could have specific negative consequences on audiovisual services.

AVMS-D: The EU's Audiovisual Media Services Directive (AVMSD), last refined in 2018, sets rules for content quotas, advertising, and the promotion of European works on both traditional broadcasters and digital platforms. In May 2025, the EU Council signaled a revision to adapt the directive to video-sharing platforms and social media, with emphasis on content prominence, protection of minors, and European content visibility. For U.S. businesses, the AVMSD creates operational and compliance burdens, restricts flexibility in content offerings, and may limit market access for streaming and digital media services. As of 2024, **Germany** has implemented investment obligations for foreign video-on-demand (VOD) providers under the Audiovisual Media Services Directive (AVMSD) (see 'Germany' section below).

Financial Information for Data Access Regulation: The European Parliament and the Council of the EU are seeking to exclude companies designated as 'Gatekeepers' under the DMA from the draft FIDA Regulation, making them ineligible for the financial data sharing scheme. The policy options prominent in the FIDA discussions are: (1) full exclusion (based on Germany's non-paper), where the definition of 'data user' would be modified to explicitly exclude 'Gatekeepers' from the full regime; and (2) partial exclusion (based on the Commission's non-paper), preventing 'Gatekeepers' from processing, combining and cross-using customer data under FIDA, and requiring 'Gatekeepers' to obtain authorization to operate as a FISP (Financial Information Service Provider).

EU Digital Simplification Omnibus: The European Commission is expected to publish a Digital Simplification Omnibus in Q4 2025. The Omnibus will likely propose several targeted amendments to simplify current EU digital regulations. While this is a welcome opportunity to address existing digital trade barriers and burdensome compliance costs for U.S. providers, the Commission has suggested that many of the simplification measures will not apply equally to all companies, and that larger companies – primarily U.S. companies – will continue facing significant regulatory burdens. For example, the Commission has indicated that it may introduce targeted exemptions to the AI Act for smaller-sized companies, and that planned revisions of the GDPR/ePrivacy Regulations could create a two-tier system with stricter rules for larger companies. This tiered approach to simplification would create an asymmetric regulatory system and structurally disadvantage larger U.S. providers.

EU Space Law: The EU Space Act (EUSA) proposal would introduce stringent requirements for satellite constellations, in some cases discriminating against non-EU operators. Critical provisions include:

1. Constellation size classification: The EUSA establishes three categories of operators, which are subject to different requirements. The category subject to stricter requirements, 'giga-constellations' (≥1000 satellites), targets two U.S. constellations.
2. Technical requirements: The proposal creates uncertainty by deferring crucial technical specifications to future Implementing Acts (IAs). However, the draft already shows that the Commission is intending to introduce novel standards lacking scientific basis and deviating from international norms, including on orbital congestion, orbit selection and intra-constellation risk.
3. Collision avoidance services: EU operators must use EU Space Surveillance and Tracking (EU SST), while non-EU operators are excluded and must rely on alternative services that meet certain requirements. Several of those requirements are not met by the U.S. Space-Track system and are not aligned with best practices, creating operational challenges for non-EU operators.
4. Registration process discrimination: Non-EU operators face undefined registration timelines, while EU operators benefit from a 12-month process. The governance framework, involving a Compliance Board at the EU Agency for the Space Program (made up of delegates from Member States), raises concerns about potential delays and conflicts of interest (e.g., the French Government has recently invested €1bn+ in Eutelsat OneWeb, a competitor to U.S. constellations).
5. Implementation timeline: The EUSA will apply to spacecraft launched after January 2030, with a 2-year exemption for satellites completing critical design review in the prior year. With final adoption of the full legislative package expected in 2028/2029, this creates tight compliance windows for next-generation constellations.

Inspection rights: The European Commission seeks authority to inspect non-EU facilities, raising concerns about business secret disclosure and potential conflicts with U.S. regulations, particularly ITAR requirements.

News Media-Related Digital Service Taxes: The European Media Freedom Act (EMFA) was enacted on April 17, 2024, with a dual goal of supporting media freedom and diversity and protecting journalists. In particular, the EMFA introduces a special treatment of media content on very large online platforms. While the adopted text claims that this special treatment would not contradict the horizontal rules established in the Digital Services Act, the implementation will be challenging as the EMFA create additional complexity in interaction with other digital regulations.

More concerningly, the creation of a press publishers' right under Article 15 of the Copyright Directive creates problems with respect to online services providers needing to pay news organizations for hosting news content, including links. In contrast to U.S. law and current commercial practices, Article 15 may effectively require search engines, news aggregators, applications, and platforms to enter into commercial licenses before including snippets of content in search results, news listings, and other formats. As EU states continue to implement the rules in the Copyright Directive into their national laws, some governments are re-interpreting key provisions to the detriment of users, publishers and platforms alike, and creating new barriers and challenges for U.S. companies when complying with national rules:

- One example of this trend can be found in Croatia. While the European Commission, and former Commissioner Breton specified that "*Member States are not allowed to implement Article 15 . . . through a mechanism of mandatory collective management*", the Croatian draft law includes a provision which would make it mandatory for all publishers to license these rights collectively..

- In 2019, while in the process of implementing Article 15, France created an analogous right for press publishers. News publishers can now request money from platforms when platforms display their content online. In response, Google changed the way news articles appeared in search results, but this did not prevent the French competition authority from ordering Google in April 2020 to pay French publishers based on the new law; and while, in October 2020, Google and the "Alliance de la Presse d'Information Générale" (representing newspapers such as Le Monde) announced that future licensing agreements would be based on criteria such as the publisher's audience, non-discrimination and the publisher's contribution to political and general information, the French competition authority imposed a €500 million fine on Google in July 2021 as it considered that the company did not negotiate "in good faith" with the press industry over licensing fees.

Austria - Digital Services Tax: Austria imposes a 5% DST on revenue from online advertising. The threshold is for companies with worldwide revenue of €750 million and local revenue of €25 million. On February 15, 2024, the U.S. Treasury announced the extension of the agreement between the United States and Austria, allowing DST liability accrued by U.S. companies through June 30, 2024 to be creditable against future income taxes accrued under the OECD's Pillar 1. The transitional credit arrangements remain under negotiation, leaving continued uncertainty for U.S. firms exposed to DSTs in this market.

Belgium - Digital Services Tax: In 2025, the new ruling government of Belgium put forward a plan to implement a 3% "digitax" by 2027 at the latest, pending further European and global discussions. If it follows Belgium's 2019 proposal, it would apply to companies with worldwide revenue of €750 million and local revenue of €5 million and would have the same scope as the European Commission's DST proposal, which would allow the revenue streams of advertising services, intermediation and marketplace services, and data transmission to be taxable.

Croatia - Digital Services Tax: The government of Croatia has announced plans to adopt a digital services tax, potentially modeled after the DST in Austria. CSI urges USTR to encourage Croatia to refrain from enacting a DST and instead re-commit to the multilateral project through the OECD/G20 Inclusive Framework to address tax challenges of the digitalizing global economy.

Czechia - Digital Services Tax: In 2019, the Czech government proposed a 7% DST on revenue generated by (a) supplying targeted advertising on a digital interface to Czech users; (b) making available to Czech users a multisided digital interface that facilitates the provision of goods and services among users; and (c) transmitting data about Czech users derived from their activities on digital interfaces. In-scope companies would have global revenue exceeding EUR 750 million, revenue from supplying covered services in Czechia exceeding CZK 100 million, and revenue from supplying covered services in the EU amounting to at least 10% of total revenue in the EU. The DST has not been adopted to date.

Cyprus - Data Sovereignty Barriers: Cyprus does not impose explicit data localization rules, and global cloud providers can compete for public tenders if registered in the EU. However, procurement specifications increasingly reference "European management" of data centers. While not binding, when applied in tender scoring, this reference creates a structural preference for EU-managed infrastructure, disadvantaging U.S. providers with non-EU management structures. The result is a discriminatory procurement practice that narrows customer choice and discourages cross-border sourcing.

France - SecNumCloud Certification Requirement: SecNumCloud is a national cybersecurity certification scheme for cloud service offerings that handle sensitive data, primarily in the French public sector. France's SecNumCloud is an unfair trade practice and barrier to market access, because it requires cloud providers to store data, and conduct primary operation and supervision, in the EU and guarantee

protection against extra-European legislation, such as the U.S. Cloud Act. In addition, certified cloud providers must be headquartered in the EU, and their ownership must be under European control to be eligible to supply covered cloud services. As a result, U.S. companies do not qualify to supply cloud services to specific French government procurements for sensitive data, including in the healthcare and defense sectors. France is expected to extend the SecNumCloud certification requirement to “Operators of Vital Importance” (OVI), such as banks, energy, and telecommunications providers, a move that would further limit market access for U.S. cloud service providers.

France - Digital Services Tax: A 5% DST on revenue from services connecting users through a digital platform and the sale of advertising space and digital data. The threshold is for companies with worldwide revenue of €750 million and local revenue of €25 million. On February 15, 2024, U.S. Treasury announced the extension of the agreement between the United States and France allowing DST liability accrued by U.S. companies through June 30, 2024 to be creditable against future income taxes accrued under the OECD's Pillar 1. As of October 2020, the National Assembly’s Finance Committee has been reviewing proposals to raise the DST. If any of these amendments are adopted, the committee will submit them for debate in the National Assembly, scheduled between Oct 24 and Nov 3 — a phase that may lead to additional amendments. The text will then move to the Senate for examination between Nov 24 and Dec 10. The entire parliamentary process must be completed by December 31.

Germany - Competition / Ex Ante Rules: The German competition authority (FCO) has specific oversight powers under Article 19a of the Act Against Restraints of Competition (ARC). Five U.S. tech companies have been designated as companies with "*paramount significance for competition across markets*" (UPSCAM), on which the FCO can impose specific obligations. In 2025, the assessment of the UPSCAM provisions and a revision of ARC are due, and there is a risk of further restrictions on U.S. tech companies to address AI concerns.

Germany - Digital Levy Proposal: German Cultural Minister Wolfram Weimer (independent, CDU/CSU appointee) proposes a 10% ‘platform/digital levy’ on large digital platforms that use media or cultural content. While no official draft legislation exists yet, Weimer recently indicated publication of a non-binding position paper in fall 2025. At the moment little detail about potential design is known. However, in the past Weimer referenced the Austrian Digital Service Tax, implemented in 2020, as a potential blueprint for this proposal.

Germany - Streaming Investment Obligation Proposal: The German Minister of Culture, with pressure from the Ministry of Finance, is preparing to introduce legislation targeting U.S. streaming service providers that would force them to invest 10% of their local revenue in German productions. An investment obligation was included in the governing coalition's plans in spring of 2025. It is not yet confirmed. There are ongoing industry discussions with the German government to encourage 'voluntary' investments and render the IO unnecessary, but there remains a risk of legislation.

Hungary - Data Localization: In Hungary, data management rules for state and local government bodies providing essential services are governed by Act No. 50 of 2013 on the Electronic Information Security of State and Local Government Bodies (Act). The data managed by state and local government bodies under this Act may only be processed and stored on Hungarian territory, except where the supervisory authority authorizes the processing on the territory of another EEA country. Any entity not registered in Hungary handling data covered by the Act must appoint a representative in Hungary.

Italy - Digital Services Tax: Italy maintains a 3% DST on revenue from advertising services, intermediation and marketplace services, and data transmission (i.e. the transfer of data collected from users and generated through the use of digital interfaces). The tax applies to companies with worldwide revenue of €750 million.

Italy - Network Fees: Despite the EU's commitment in the EU-U.S. Joint Statement, the Italian telecom regulator (AGCOM) is currently setting a precedent for the introduction of backdoor network usage fees. On August 5, AGCOM ruled that CDNs fall within the scope of the European Electronic Communications Code (EECC), and are therefore subject to dispute resolution mechanisms. This will allow Italian telecom operators to initiate disputes with U.S. tech companies as a means of extracting payments for the delivery of traffic requested by users. By multiplying disputes, and building on the precedent set by these disputes, Italian telecom operators intend to establish *de facto* network usage fees. If left unchallenged, this could create a precedent for other countries and the European Commission to follow.

Italy - Data Localization in Education: The Ministry of Culture's current interpretation of the Italian Cultural Heritage Code (D.Lgs. 42/2004) creates barriers to the provision of cloud services to educational institutions. Specifically, the broad classification of public archives (including school records and educational documentation) as "cultural heritage" under Italian law effectively restricts the storage and transfer of digitalized public documents outside Italian territory. The lack of clear harmonization between cultural heritage protection requirements and modern cloud computing needs creates an obstacle to digital trade, particularly impacting non-EU cloud providers seeking to serve Italian schools and educational institutions.

Malta - Data Mirroring and Hosting Requirements: The Malta Gaming Authority (MGA) requires licensed operators to maintain a live mirror server physically located in Malta, containing "essential regulatory data" (e.g., player identity, transactions, revenues), even when core systems are hosted in other EU or international jurisdictions. This data localization mandate forces costly duplication of infrastructure, creates latency, and offers little incremental regulatory assurance. It is discriminatory because it excludes efficient cross-border hosting models and raises operational barriers for U.S. providers.

Poland - Digital Services Tax: On August 13, 2025, Poland's Ministry of Digital Affairs released two potential options for DSTs, modeled after existing DSTs in the U.K. and France. The first potential DST would implement a tax rate of 3%, 4.5%, or 6% on e-commerce, search engine marketing, display advertising, and other sectors. The second option would implement a tax rate of 5%, 6%, or 7.5% on search engine marketing and display advertising. A draft bill is expected before the end of 2025. Depending on the variant chosen, this DST has the potential to cost U.S. firms well over USD $100 million in the first year of implementation.

Spain - Digital Services Tax: Since 2021, there has been a tax on certain digital services. It is an indirect 3% tax on revenue from (a) supplying targeted advertising on a digital interface to Spanish users; (b) making available to Spanish users a multisided digital interface that facilitates the provision of goods and services among users; and (c) transmitting data about Spanish users derived from their activities on digital interfaces. The threshold is for companies with worldwide revenue of €750 million and local revenue of €3 million.

Services Barriers - Telecommunications

Upper 6 GHz Spectrum Allocation: More than five years after the US first made the full 6 GHz band available for unlicensed operations, Europe continues to debate the issue. On the 12th of November, the Radio Spectrum Policy Group (RSPG), a group of EU regulators, is expected to present its final recommendation on the long-term allocation of the upper 6 GHz band. That recommendation will guide a final decision of the European Commission by late 2026/early 2027.

While a hybrid sharing scenario between 5G/6G and unlicensed technologies like Wi-Fi is the most likely recommendation, we expect the RSPG to recommend only a small portion of the band to be allocated to unlicensed technologies, with the rest allocated for 5G/6G. This is mainly due to several factors: 1/Tech sovereignty: Wi-Fi being perceived as a US technology; 2/Preference for EU champions: several Member States such as France, Finland and Slovenia strongly advocating for 5G/6G; 3/Misinterpretation of the recent One Big Beautiful Bill by EU stakeholders, who assumed the US reversed its position on the upper 6Ghz band.

This outcome will not only hurt US technology companies that manufacture Wi-Fi products, but also European consumers and enterprises that rely on Wi-Fi for their connectivity needs. By limiting Wi-Fi's capabilities, Europe will force consumers and enterprises to use 5G/6G connectivity, which costs more than Wi-Fi and has significant limitations for indoor connectivity. In addition, Chinese companies dominate 5G/6G technology and will likely benefit greatly from this outcome in terms of product sales and licensing revenue.

Investment Barriers

Proposal for a Foreign Investment Screening Regulation: In January 2024, the European Commission published a proposal for a new foreign investment screening Regulation. The Regulation would require EU Member States to impose an *ex ante* authorization requirement on all foreign investments involving companies that (i) are active in one of 42 listed "critical technology areas" (e.g., AI, cloud), (ii) are subject to dual-use or military export controls, (iii) provide critical financial or healthcare services, or (iv) participate in a listed EU funding program. This includes investments that do not currently qualify for antitrust review, such as minority investments and greenfield investments. Initial engagement with EU policymakers on this regulation suggests that it is likely to have a significant impact on U.S. investors, subjecting them to extensive review processes.

Ireland - New Grid Connections: While U.S. data center operators have invested heavily in Ireland over the last decade, it is now virtually impossible to obtain grid connections to allow more data centers to be built. A de facto moratorium was imposed on data center growth by the grid operator in 2022, partly to mitigate the country's security of electricity crisis (data centers were widely scapegoated for electricity shortages, with much less attention paid to the failure by the authorities to invest in new grid infrastructure and generation). The energy regulator has also been seemingly unable to complete a protracted process to adopt a new grid connection policy, having been working on the document for nearly three years. This regulatory paralysis has had a significant negative impact on U.S. data center operators' investment strategy for Ireland, with businesses unable to proceed with long-planned projects.

Subsidies

EU Foreign Subsidies Regulation (FSR) implementation: In July 2023, the EU's FSR entered into force, giving the EC new powers to target economic distortions in the EU market caused by foreign subsidies. Under the FSR, the Commission has broad powers to request sensitive business information regarding companies' interactions with non-EU governments, including confidential contracts. The Commission also has broad discretion to decide whether a non-EU subsidy distorts the EU single market and to impose strict sanctions. While the EC claims that the FSR targets subsidies from non-market economies, the FSR in fact subjects U.S. businesses to the same procedures as companies from non-market economies that unfairly compete in the EU market. From October 2023, for example, any company operating in the EU market will be required to disclose "financial contributions" from non-EU governments (e.g., subsidies, certain fiscal incentives, capital injections) granted up to three years prior to their participation in the following activities: (i) public procurement procedures where the tender exceeds €250M and (ii) mergers and acquisitions in which parties' aggregate EU revenues exceed €500M. In

addition, the FSR also provides the EC with an *ex officio* tool to investigate financial contributions on an ad hoc basis from July 2023. If the EC finds businesses to have benefitted from "distortive" subsidies, it could: (i) disqualify them from public tenders and M&As in the EU; and (ii) apply regressive measures such as subsidy repayments. Failure to disclose financial contributions or to comply with regressive measures may result in fines up to 10% of companies' global revenue.

Complying with the FSR's intensive reporting requirements has proven to be exceptionally burdensome, demanding significant human and technical resources across global teams. FSR filings are often the most resource-intensive filings for any global transaction. This is in stark contrast to the Commission's initial prediction that the regulation would create a "limited administrative burden". The regulation also disadvantages non-EU businesses by imposing significantly higher compliance costs on them, as they must track non-EU incentive schemes that are not required to be tracked in the EU.

U.S. businesses are also facing excessive information requests under the FSR. The Commission regularly asks for information far beyond what appears necessary for its assessments, including: data on "financial contributions" granted after a notification, often with unrealistic deadlines; and significant information regarding U.S. federal, state and local incentive schemes that are not limited to specific companies or sectors and therefore do not fall under the FSR's own definition of a subsidy. Further, for public procurement procedures, U.S. businesses have been asked to submit multiple FSR filings and repeatedly update their "financial contributions" for periods exceeding three years.

In March 2025, the Commission issued draft guidelines seeking to provide clarity on several important aspects of the FSR.Unfortunately, rather than clarifying the application of the FSR, the draft guidelines seek to expand its scope and would create a more uncertain legal environment for U.S. businesses:

- First, the draft deviates from the FSR's original goal by extending its scope to include subsidies without a clear EU connection, introducing a new cross-subsidization theory that any subsidy can "free up" resources for EU activities, regardless of intent or use. This effectively reverses the burden of proof, requiring companies to disprove cross-subsidization.
- Second, the draft weakens the FSR's distortion test. It proposes a low legal standard, where a "reasonable link" or even a minor contributory relationship between a foreign subsidy and a negative impact on EU competition is sufficient for a finding of distortion.
- Finally, the draft expands the FSR's public procurement scope. Beyond current notification obligations, it adds compliance burdens by allowing examination of any "financial contributions" from any corporate group entity under vague "specific circumstances." This undermines legal certainty and proportionality, potentially hindering businesses from participating in tenders due to demands for extensive information during short deadlines.

Overall, the FSR has created significant legal uncertainty and disproportionate compliance burdens and costs for U.S. businesses and investments in the EU.

Other Barriers

EU Defense Funding: The EU is implementing significant defense funding and investment initiatives that are reshaping market access requirements across the sector. The Security Action for Europe (SAFE) framework, approved in May 2025, establishes a €150 billion loan instrument for defense procurement with strict European preference provisions that create tiered requirements for providers. For contracts exceeding 35% of the total value of SAFE loans, providers must be EU/EEA/EFTA/Ukraine-based with local executive management, and demonstrate freedom from third-country control, undergo FDI screening, or provide security guarantees. Contracts representing 15-35% of value require providers to be established with executive management in eligible regions or have existing contractor relationships, while maintaining the same control and screening requirements. Only contracts under 15% of total value are

exempt from specific eligibility requirements.

The European Defense Industrial Programme (EDIP), a €1.5 billion funding instrument, is currently in negotiations after stalling in late 2024. Following SAFE's approval, EDIP discussions have resumed with similar European preference requirements. The U.S. tech industry has proposed several technology-specific exemptions, including allowing technology services to qualify if (i) delivered from EU/EEA territory, (ii) certified for classified information processing, and (iii) free from foreign military export controls. They also suggest focusing on operational sovereignty rather than ownership, and clarifying requirements for software where foreign entities hold IP but European operators maintain control. Looking ahead, the 2028-2034 Multiannual Financial Framework allocates €131 billion to defense and space - five times more than the previous MFF. This funding is expected to incorporate similar European preference requirements as SAFE and EDIP.

Italy - Tax Issues: Many US multinationals continue to experience issues interacting with Italy's tax authority and court system. Examples include:

- Tax authority not entering in good faith negotiations concerning common tax issues, such as transfer pricing or withholding tax issues, and instead applying a heavy-handed approach including criminal penalties.
- Italian Competent Authority denying access to or refusing to participate in mutual agreement procedures (MAP) under applicable income tax treaties.
- Tax authority taking technical positions that are contrary to their own tax laws or long-established international tax principles, as embodied in OECD tax treaty commentary (e.g., *Principio di Diritto No. 5* of February 20, 2023, which imposes royalty withholding taxes on mere distribution of software in contravention of OECD Commentary).

In the context of the ongoing trade negotiations with the EU, USTR is encouraged to request its counterparts to remove this barrier to trade by requiring the Italian government to reform its tax administrative practices and tax policies to be consistent with internationally-accepted norms. Similarly, reform of the tax court system is necessary to ensure that courts respect international law obligations of Italy and deliver a level of adjudication that is appropriate for high-stake controversies resulting from exaggerated assessments imposed by the Italian tax authority. An additional step would be if USTR (in coordination with US Treasury) could convince Italy to accept binding arbitration in its tax treaty with the US, which arbitration could be initiated at the request of the taxpayer in the event that MAP does not lead to an agreed resolution.

India

Import Policies

Unfair Import Tariffs: Since 2014, India has imposed a 20% tariff on imported switches and other products that fall under HS 85.17 and should be tariff-free because its bound rate for this tariff code is zero. This is unfair because the United States accords duty-free treatment of such products when they are imported from India. In its recent Union Budget, the Indian government harmonized the differential duty rate between carrier grade and enterprise grade switches to a uniform rate of 10%. Earlier, carrier grade switches had a 20% customs duty. While a step in the right direction, the lower duty rate is still not zero.

Import Authorization for Ultra-small Form Factor Computers and Servers and Information and Communication Technology (ICT) Equipment: In August 2023, the Indian government announced that beginning November 1, 2023, import authorizations are needed to import laptops, tablets, all-in-one personal computers, and ultra-small form factor computers and servers. India has implemented an import monitoring system ("IMS") to monitor the import of ICT products. The Ministry of Electronics and IT

deliberates on the applications before the Directorate General of Foreign Trade (DGFT) can grant the authorizations. This import authorization requirement delays and disrupts imports of in-scope information and communication technology (ICT) equipment into India. U.S. companies have applied for import licenses for servers. However, India only granted licenses for approximately 25-35% of the value of imports requested. India's action is an unfair restriction on market access that negatively impacts the ability of U.S. companies to compete in the Indian market. India's import authorization requirements for laptops, tablets, computers, and servers, originally set to expire on December 31, 2024, have been extended into 2025. Implementation has, however, become increasingly problematic due to conflicting interpretations among Indian government agencies (MEITY, DGFT, and India Customs). This has resulted in significant delays in ICT equipment deliveries, with companies experiencing 7-10 day delays. Further, the receipt of contradictory guidance from different agencies has resulted in Customs investigations. The inconsistent application of these requirements creates substantial uncertainty for U.S. companies and effectively functions as a non-tariff barrier to trade, violating India's WTO obligations regarding transparency and predictability in trade measures.

Additionally, India has implemented an import monitoring system (IMS) to monitor the import of ICT products such as laptops, tablets, PCs, and servers. This is intended to discourage imports and force local manufacturing. U.S. companies have applied for import licenses for servers. However, India only granted licenses for approximately 25-35% of the value of imports requested. India's action is an unfair restriction on market access that negatively impacts the ability of U.S. companies to compete in the Indian market. Additionally, there are concerns of the IMS evolving into a quota system which would cause supply chain disruptions or include requirements for local sourcing/manufacturing before import licenses are granted. Introducing such a quota would also be a violation of India's WTO obligations.

Equalization Levy: In March 2020, India adopted an additional two percent equalization levy, expanding on an earlier equalization levy that targeted digital advertising revenue earned by non-resident providers. The tax applies only to non-resident companies and covers online sales of goods and services to, or aimed at, persons in India. The tax applies only to companies with annual revenues in excess of approximately Rs. 20 million (approximately U.S. $267,000). India's Lower House of Parliament voted to withdraw its 6% Equalisation Levy from 1 April 2025, which was contained within amendments proposed in August 2025 Finance Bill. NFTC appreciates USTR's work to remove this barrier but encourages USTR to continue to monitor the implementation of the removal of India's levy and the transitional approach agreed to by India.

Export Controls: In an effort to diversify supply chains away from China but continue to have a regional fulfillment model, U.S. companies have recently invested in India manufacturing capabilities. The Indian government has stringent export control rules for dual-use items, called Special Chemical, Organisms, Materials, Equipment & Technology ("SCOMET") Rules. India considers specific telecom products to be dual-use, and therefore, to export from India, U.S. companies are mandated to obtain an export license.

Under the SCOMET rules, the OEM must submit End-User Certificates (EUC) from all end users. This is a challenge, as the exports are likely to be re-transferred multiple times within the supply chain before they reach the end user. Further, there is also a requirement for post-reporting of exports made from India to the stockiest, transfers made by the stockiest to the final end-users and inventory with the stockiest as on December 31 of each calendar year, by January 31 of the following year. A failure to do so may entail penalty and/or cancellation of authorization. Meeting this requirement even on a post shipment basis would be impossible. Most importantly, there is no global precedence of such documentation for export licenses.

U.S. companies have provided an end user certificate on behalf of customers and have also agreed to facilitate Post shipment verification of the items at end users' site if required by the Government of India, after prior/suitable notification. Some companies obtained licenses for a period of two years based on exemptions, especially from the EUC from customers. This is unfair, because the U.S. government provides bulk export licenses without such onerous requirements to exporting companies for dual-use items. A failure to obtain export licenses other than on an exemption basis hurts U.S. company's ability to scale manufacturing for additional products.

Illicit Trade: Illicit trade is becoming a more substantial challenge for U.S. companies operating in the region, raising health and safety concerns for patients. One particular issue of concern is the increase in illicit trade crossing the border between India and Bangladesh. **NFTC urges USTR to encourage intensive training, strategic deployment of resources, and greater partnership between Indian and Bangladeshi authorities – which should include a cross departmental task force with MoH, DoP, and Ministry of Home and Customs**. In addition, authorities should take greater action against websites selling illicit medicines and local distributors facilitating their spread.

Technical Barriers to Trade

Mandatory telecom certification framework: Indian Telecom licensees are required to connect their networks only with telecom equipment that has been tested and certified under the Mandatory Testing and Certification Framework (MTCTE). The mandatory testing and certification scheme is operational for certain IT and telecom products on parameters of safety, functionality and potentially security as well. The scope of this requirement was recently increased to include cloud software (Hypervisors), which goes beyond telecom products. This marks a significant policy shift, extending regulatory oversight from physical network equipment to virtualised and software-defined network elements, thereby broadening the ambit of compliance obligations for cloud service providers and telecom operators alike. This expansion introduces onerous localisation and testing requirements for software that is not manufactured or deployed solely in India. Hypervisors and other virtualisation software are typically developed, tested, and maintained globally, often as part of multi-tenant, cloud-native architectures. Requiring such software to undergo local testing – and potentially disclose proprietary source code or security configurations — can expose intellectual property, conflict with global security standards, and delay product deployment cycles. Moreover, since MTCTE is applied only to equipment and software used by Indian telecom licensees, it disproportionately affects foreign suppliers who serve the Indian market, while domestic software or cloud providers may face fewer compliance hurdles if their infrastructure is already localised. In practice, this creates a de facto barrier to market access, inconsistent with India's commitments under the WTO's Agreement on Technical Barriers to Trade (TBT), which discourages discriminatory treatment and mandates that conformity assessments not be more trade-restrictive than necessary. The inclusion of cloud-based software like hypervisors under MTCTE represents an undue regulatory burden — one that duplicates existing international certifications and cybersecurity frameworks (such as ISO/IEC 27001, SOC 2, or FedRAMP) already adhered to by global providers. Instead of enhancing national security, it risks fragmenting global cloud operations, increasing compliance costs, and reducing the competitiveness of international firms in India's rapidly growing digital infrastructure market.

Restrictions on Multi Brand Retail: India has restricted American e-commerce providers from operating in the market on a level playing field as domestic companies, including through limitations on foreign companies operating in "multi-brand retail trading (MBRT)." This means that any company with foreign investment, including American e-commerce companies, cannot sell its own inventory directly to customers, requiring significant changes to their business models. These rules, which began in 2012 but were expanded in 2016 and 2018, establish several obstacles to American companies operating in India. American companies cannot invest more than 51% in a firm operating in India, with a minimum investment requirement of $100 million that carries obligations micromanaging companies' business

decisions. For example, at least 50% of this initial FDI must fund backend infrastructure such as processing, storage, distribution, and logistics, and at least 30% procurement of manufactured or processed products must be from Indian micro, small, and medium industries. American companies are prohibited from selling their own inventory directly to consumers and are only permitted to operate a marketplace business model. They also face severe restrictions for marketplace e-commerce operations, including being unable to set prices, facing limitations on inventory management, and being prohibited from entering seller exclusivity arrangements. Specifically, American marketplaces and their group entities cannot provide more than 25% of the inventory for any of the vendors using their service. The regulation undermines American companies' ability to efficiently reach Indian consumers and optimize their supply chains.. None of the above restrictions apply to domestic, non–FDI-funded entities. Domestic companies are permitted to operate inventory-based models without any additional conditions and have complete flexibility in pricing, inventory management, and seller exclusivity agreements for their e-commerce operations. These restrictions prevent leading U.S. e-commerce companies from accessing the rapidly growing Indian market, undermine current and potential investments in the U.S., and diminish U.S. technology leadership.

Market Access Challenges (Pharmaceuticals): The Indian government's largest public health program, Ayushman Bharat Pradhan Mantri Jan Arogya Yojana (AB-PMJAY), which provides health coverage to over 700 million Indian citizens, does not reimburse any patented medicines. Instead, it only covers locally produced generic drugs, creating a significant barrier to market access for innovative U.S. pharmaceutical products. The Indian government uses a different pricing mechanism for patented drugs that requires them to meet unreasonable prices resulting from a cost effectiveness analysis that is not suited to India's socio-economic parameters. By design, this framework excludes all innovative medicines by deeming them 'not cost effective'. This is in contrast to the approach followed for locally produced generics for incorporation into the AB program, thereby creating a de facto ban on innovative medicines. While generic drugs are priced based on existing government-negotiated rates for programs such as CGHS and ESIC, patented medicines are subject to a health technology assessment (HTA) analysis that typically demands up to an 80% lower price, effectively pricing out U.S. innovators. These barriers stand in stark contrast to the substantial access Indian companies have to the U.S. pharmaceutical market contributing to the trade imbalance. Increasing U.S. companies' share of the AB program will increase exports and jobs in the United States, while also creating tremendous revenue potential.

- **Regulatory Uncertainty & Delays**: At present, Indian authorities require significant additional local data and studies to approve new therapies and clinical trials for the market that are already approved worldwide. In 2024, India issued guidance to implement Rule 101 that allows drugs approved by U.S. FDA (and others) to be approved in India without requirement of local trials, if companies undertake to conduct post launch trials in the country. However, this process (Rule 101) is not being used as expected in practice. The lack of operationalization of this rule amounts to a technical barrier to trade in our view and unfair treatment of U.S. companies, as Indian companies are not required by the FDA to submit local data.
- **Price Controls on Innovative Medicines:** India imposes price controls on drugs that are supplied not only to the government but also in the private non-reimbursed market. Several provisions of this pricing policy place unreasonable commercial restrictions on medicines, including patented/innovative medicines developed by innovative bio-pharmaceutical companies. A rational and predictable pricing policy will go a long way in enhancing confidence, allowing for longer-term market entry planning, and creating reasonable expectations in the marketplace.

Government Procurement

Discriminatory Government Procurement Policies: India's public procurement policy has evolved over the years and required stricter implementation, especially for the telecom sector. Various regulations, such as the General Financial Rules ("GFR") 2017, the Public Procurement (Preference to Make in India)

("PPP-MII") Order, 2017, and sector-specific regulations, establish procurement guidelines for central ministries, departments, and public sector enterprises. The PPP-MII Order was updated in 2020 to create specific classes of local suppliers with varying levels of value addition. This is further customized by each Department for each notified product. The Department of Telecom's PPP-MII policy mandates extremely high value addition thresholds for telecom products and requires 100% component localization and a high percentage of value attributable to an Indian intellectual property (i.e. a design patent residing in India).

Such government procurement policies are unfair, because they favor domestic suppliers and discriminate against U.S. companies that seek to compete fairly in India's government procurement market.

Local Content Requirement: Aligned with the Government of India's continued rhetoric on self-reliance, the Public Procurement (Preference to Make in India), Order 2017 and subsequent revisions mandates that only Class-I suppliers (with local value addition >50%) and Class-II suppliers (local value addition – 20% to 50%) are eligible to bid for government procurement. This is applicable to both products and services. This order poses a significant compliance challenge in particular to foreign software and cloud service providers (CSPs) to demonstrate local value add. This model does not consider the investments and other contributions made by foreign CSPs that enable the Indian Tech ecosystem and their global competitiveness, such as skilling initiatives, cloud innovation centers, quantum computing lab etc. Even if CSPs don't directly bid for government contracts, partners need to certify their percentage of local content, for which they rely on their vendors' local value addition as well. For example, where cloud services are a substantial cost element in a public procurement bid, percentage of local value add from a CSP becomes important. Moreover, the Indian government is considering revisions to the order and increasing the minimum local content requirement for Class-I suppliers to 60% and Class-II suppliers to 30%.

Intellectual Property Protection

- **IP Challenges**: American companies face continued IP violations in India including lack of regulatory data protection, patent linkage, and patent term restoration. Substantial reform is needed in the IP policy frameworks to meet trade obligations and ensure American IP is treated the same as Indian IP in the United States. We were encouraged by a recent amendment to patent rules addressing concerns around pre-grant opposition delays. However, there are larger issues at hand that must be addressed to prevent patent infringements in India. Such infringements are enabled by a gap between federal patent grants and state drug approvals. India should amend the IP and regulatory laws to make it necessary for drug approval authorities to verify absence of existing patents prior to granted approvals for generics. Additionally, it should institute a system where all applications for drug approvals are put up on a public platform so that patent holders can take preemptive legal action where it is merited.

Services Barriers

Requirement to Report Importation of "Non-physical Imports": Indian banks have a requirement to advise Indian Customs of the importation of "non-physical imports" when related to Direct Import Remittances. This requirement appears to originate from a 2010 Circular "Master Circular on Import of Goods and Services" of the Reserve Bank of India. Specifically, the requirement is: "Payment for software download If the import payment is towards design and drawing, advance payment for Software import, a Declaration from the importer is required confirming that they will inform customs of such import." Therefore, a U.S.-origin sale to an Indian buyer of downloaded software would be considered a

capital good under Indian regulations. Thus, the payment is leaving India to the U.S, and the requirement forces the importer to obtain specific certifications in order to release funds from the bank.

Financial Services: The United States has continued to raise concerns relating to informal and formal policies with respect to electronic payments services that appear to favor Indian domestic suppliers over foreign suppliers. The National Payment Council of India (NPCI) is a quasi-government agency that operates the largest domestic payment system in the country, including Unified Payments Interface (UPI) and RuPay (debit and credit) cards. In the past several years, the Government of India has taken many direct and indirect actions that give preferential treatment to NPCI, creating a non-level playing field for international EPS providers, including:

- Rupay and NPCI are the de facto solutions for any Government disbursement programs, known collectively as Direct Benefit Transfers (DBT), and are now being pushed in government-driven credit and commercial transactions, keeping U.S. international networks out of consideration.
- Storage of cards on file and tokenization are globally recognized to offer faster, more secure, and seamless customer experiences where B2C or Account to Account transactions are concerned. In September 2020, the RBI issued guidelines disallowing storage of cards on file by merchants and payment aggregators. Given that this ban did not extend to the UPI network it provides NPCI with an unfair advantage.
- In November 2020, the state-owned National Payments Corporation of India (NPCI) announced a market share limitation of 30 percent (measured by transactions) for foreign electronic payment service suppliers processing online payments made through India's Unified Payment Interface, which is owned and operated by NPCI.

The United States also has expressed concern over plans to expand the adoption of a National Common Mobility Card (NCMC) that only uses a domestic proprietary standard, which disadvantages foreign suppliers. India has not yet shared the domestic qSPARC standard, effectively prohibiting U.S. firms from participating in the roll-out of the NCMC. The Finance Ministry's Department of Financial Services (DFS) requires any re-carding or issuance of new cards by banks to be compliant with the standards defined for the National Common Mobility Card (NCMC). Subsequently the Ministry of Housing and Urban Affairs (MoHUA) mandated that the NPCI qSPARC standards would be the NCMC standards. U.S. networks have been blocked from accessing the qSparc specification. In July 2023, the DFS issued another circular instructing all banks to issue only NCMC compliant contactless cards. The banks view the circular as a mandate which directly impacts their ability to issue contactless cards from international card networks, hence creating an unlevel playing field.

Interoperable payment options across multiple transport modes simplify commuters' experience with public transit and encourage public transit use. Given that a large base of Indian customers already has cards that allow contactless payments (using open loop EMV standards), enabling existing cards on transit ecosystem would be both economically viable (given the costs associated with issuing separate, specific NCMC compliant cards) and boost uptake and use of transit systems to benefit Indian citizens at large.

Digital Commerce/Digital Trade Barriers: In 2018, the Reserve Bank of India (RBI) implemented a requirement that all payment service suppliers store all information related to electronic payments by Indian citizens on servers located in India. RBI announced this rule without advance notice or input from stakeholders. In 2019, RBI stated the requirement to store payments data locally also applied to banks operating in India. Foreign firms assert that the data storage requirement hampers the ability of service suppliers to detect fraud and ensure the security of their global networks.

Potential data localization under Data Protection Rules: The Digital Personal Data Protection Act (DPDP Act) entered into law on August 11, 2023, instituting a requirement for affirmative consent for all

data processing and narrowly defining legitimate processing bases. It also permits the government to restrict data export to certain countries without clear criteria or recourse, causing uncertainty for industry regarding data protection and cross-border data flows. The Draft Digital Personal Data Protection Rules (DPDP Rules), published in 2025, have further heightened industry concerns by imposing expansive obligations on "significant data fiduciaries" and empowering the government to impose data localization mandates for certain categories of personal data (currently undefined). The draft DPDP Rules risk creating significant compliance burdens by targeting specific companies rather than specific types of data, while leaving businesses uncertain whether they will be subject to future localization requirements. At the same time, proposed restrictions on cross-border transfers would allow personal data to be moved abroad only on terms set by the government, without clear criteria or mechanisms, such as standard contractual clauses, that would enable companies to ensure compliance, resulting in an overall lack of uncertainty on the GOI's stance on data localization. While India explores a digital sovereignty policy, this could be one mechanism to ensure data residency and control. The DPDP Act and Rules empower the GOI with broad powers to categorize certain types of data for localization, for significant data fiduciaries (SDF). There is no process or clarity on who would be designated as a SDF. This would introduce uncertainty for digital transfers and businesses, along with increasing cost to operate.

Direct Tax Permanent Establishment Issue for Cloud Service Providers (CSPs): India's income tax laws are ambiguous on whether the provision of data center services by an Indian entity to a foreign entity establishes a taxable presence, such as a permanent establishment (PE) or business connection, for that foreign entity. This risks overly broad tax liability for cloud service providers (CSPs) on their tax liability in India. CSPs typically have arrangements with the data hosting service providers (which may be a group affiliate of the CSPs) owning and operating the data centers across the globe including India. The data centers can serve the customers of any region and are not limited to the local country customers. CSPs operating in India are facing tax uncertainty, as in their recent tax audits/ assessments the tax authorities are claiming that CSPs constitute Permanent Establishment ("PE") in India. Tax authorities are claiming that the CSPs have control over data centers through the technology/ software that gets deployed on the data center and cloud services are provided by CSPs through clusters of servers in the data centers in India. This creates a net new, large direct tax impact on American CSPs who are investing billions of dollars in the country and need business and taxation certainty to operate. In July 2025, the case of *Hyatt International* raised further questions over taxation certainty when India's Supreme Court ruled that continuous and substantive control over operations of Indian entities established fixed place PE.

Content Moderation: India's digital economy presents significant opportunities for U.S. digital service exporters, yet increased government control over online speech poses a growing concern. Indian policymakers have rapidly escalated censorship practices and restrictions on companies that fail to remove content deemed "objectionable", leading to novel and aggressive enforcement actions against U.S. firms. Direct censorship measures like internet shutdowns have resulted in substantial human rights impacts and economic losses, with U.S. social media companies like Facebook, Instagram, YouTube, and Twitter incurring an estimated $549.4 million in losses between 2019 and 2021 alone.

Legislative changes in 2023, particularly the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (amended in 2023), further challenge U.S. exporters by imposing onerous obligations on intermediaries. These rules require online platforms to prevent the display and sharing of an extremely broad range of information, including content deemed obscene, harmful to children, or that "threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign States, or public order, or causes incitement to the commission of any cognisable offence, or prevents investigation of any offence, or is insulting other nation". The rules also impose strict content takedown timelines, onerous due diligence requirements, and localization and traceability mandates that could compromise security encryption, leading to privacy and security risks, a chilling effect on human rights, and potential over-removal of legitimate content. Additionally, the IT Rules provide expansive government oversight

and regulatory control over Internet content through Grievance Appellate Committees and fact-checking bodies, blurring the lines between self-regulation and state control. The Sahyog portal, launched in October 2024, expanded government powers to issue takedown and blocking notices, a move recently upheld by the Karnataka High Court, raising concerns about the fundamental rights of foreign companies.

Further, efforts by the Telecom Regulatory Authority of India (TRAI) and the Ministry of Information and Broadcasting to expand the regulation on online service providers raise concerns of regulatory overreach and duplication, and censorship:

- In July 2023, TRAI proposed to bring OTT providers into the same licensing and registration framework as telecommunications operators, and "selective banning" of certain OTT services. TRAI has, however, yet to issue final binding rules for licensing or selective banning of OTT providers.
- The Ministry of Information and Broadcasting proposed a draft Broadcasting Services (Regulation) Bill in 2023, expanding the scope of broadcasting regulation from traditional broadcasters and platforms with online curated content to also include social media platforms and independent content/video creators, potentially subjecting them to broadcast-style oversight, including content evaluation committees and registration requirements. While the Bill was ultimately withdrawn in 2024, the government's intent to extend broadcasting-style regulation to online services raises alarms both for the internet ecosystem and the ability for online services providers to operate in India with regulatory certainty while also raising grave freedom of expression concerns.

India's escalating censorship, internet shutdowns, and stringent IT Rules, including localization and traceability mandates, impact digital service providers that are disproportionately American by increasing compliance burdens, compromising security and privacy, and creating a chilling effect on human rights and future investment. Additionally, the expanded government oversight and potential for selective banning and regulation of OTT and other online content services and producers further threaten the operational freedom and market access for these entities.

Delays in Bureau of Indian Standards Certificate: Entities (factories) looking to export certain ICT equipment (including server-racks) into India have to apply for a BIS certificate. Applications from factories based in South-East Asian countries require a No-Objection Certificate (NOC) from Ministry of Electronics and IT (MeitY). The requirement for the NOC substantially delays the release of the certificate for factories delivering Highly-Specialised Equipment (HSE) into India adversely impacting the supply chain of critical equipment into India. Global AI development cycles are rapidly accelerating with evolving customer demands where they need landed data center capacity (infrastructure and racks) immediately on a very short notice (in weeks). Delays and long lead times often render equipment obsolete by the time it is certified/ready to land in country. To import the AI/ML server racks (containing servers), the current process of dual licensing system, involving both BIS certification and DGFT import authorization, requires ~6-8 months, which risks delaying the deployment of the latest technology. This delay affects the speed with which customers are able to access the cloud services. The BIS should be removed for equipment that is for self-use if CSPs are complying with the international regulatory safety standards in accordance with IEC and local safety laws. Removing the 100-unit HSE cap would allow for rapid deployment of the latest AI/ML technologies in India, securing India's place as an industry hub. Streamlining the certification process and removal of the MeitY NOC restriction based on manufacturer location will also address concerns on ability to scale and meet our demands in India.

Ex ante digital competition proposals: The Digital Competition Bill proposal was withdrawn by the Government of India in August 2025, marking a notable victory for the U.S. government and industry operating in the country. This bill, which drew heavily from the EU's Digital Markets Act, would have resulted in burdensome rules for U.S. companies that would not have been applied to their foreign

competitors. If implemented, this would have reduced the competitiveness of U.S. companies in India and diverted U.S. companies' investments toward compliance and away from U.S. research and development, infrastructure, and innovation. Despite its withdrawal, the threat of similar future regulatory frameworks remains. Both the Ministry of Corporate Affairs and the Competition Commission of India continue to express strong support for ex-ante regulation. Relatedly, the Competition Commission of India has filed numerous cases against US companies, and will initiate new investigations into how US companies are launching AI tools. These developments risk delaying AI product launches in India and creating non-tariff barriers for American companies.

Data localization and data flows: In October 2018, the Reserve Bank of India (RBI) implemented a requirement for all foreign payment system providers to ensure that data related to electronic payments by Indian citizens are stored on servers located in India. The requirement for local storage of all payment information is explicitly discriminatory as it raises costs for payment service suppliers and disadvantages foreign firms, which are more likely to be dependent on globally distributed data storage and information security systems. Government data on the cloud is also localized in India and the upcoming privacy bill might impose further data localization requirements for all companies, including US CSPs.

The now-withdrawn Personal Data Protection Bill, 2019 (PDP Bill) proposed a data localization mandate requiring businesses to ensure the storage of certain categories of personal data in India. Under this now-withdrawn bill, cross-border transfers of sensitive personal data would only be allowed on limited legal bases, such as under contracts that are approved by a proposed regulator. The PDP Bill is currently being revised and while government statements indicate streamlining and limiting the data localization measures, it remains to be seen if this will be the case. Retention of the data localization mandates could seriously impede cross-border data flows and free trade.

In February 2021, MeitY released the 2021 Intermediary Guidelines and Digital Ethics Code (Guidelines), which impose significant and burdensome requirements on a wide range of internet-based service providers, particularly those that operate social media, messaging, and streaming news and entertainment services. The Guidelines were notified to the Gazette of India without public consultation and are significantly different from the version MeitY had initially released for public comment in December 2018. Many of the new requirements entered into effect immediately, while "significant social media intermediaries" (5 million or more registered users in India) were given only three months to comply with sweeping regulatory changes that in some cases require significant technical re-structuring of services. These changes include the appointment of a Chief Compliance Officer, who can be held legally liable if the intermediary fails to observe the "due diligence" requirements. In addition to concerns over the lack of comprehensive stakeholder engagement, the Guidelines contain many troubling elements that could undermine privacy, security, and freedoms of speech and expression. There are also concerns about whether the Guidelines force the localization of company operations and restrict market access for non-Indian companies through the imposition of burdensome regulatory requirements that erode safe harbor protections in India's Information Technology (IT) Act and significantly overstep international best practices. Additionally, the Indian government is reported to be currently working on a significant revision to the IT Act governing intermediary liability protections in India (the "Digital India Act")

E-Commerce Restrictions: Initially released in January 2019 for consultation, India's draft E-commerce Policy represents the GOI's official position on a host of digital economy issues. The 2019 draft was explicitly discriminatory and contemplated: (1) broad-based data localization requirements and restrictions on cross-border data flows; (2) expanded grounds for forced transfer of intellectual property and proprietary source code; (3) preferential treatment for domestic digital products and incentives for domestic data storage in India (e.g., provision of infrastructure, incentives to domestic data center operators). The policy also introduces the notion of community data as a "national resource" where countries are "custodians" over data. A revised draft of the E-Commerce Policy has been in the works

since the release of the draft. Media reports have suggested that: (i) certain categories of data such as defense, medical records, biological records, cartographic data, and genome mapping data should not be transferred outside India; and (ii) certain categories of e-commerce data should be mirrored/stored in India (with the government/a proposed e-commerce regulator deciding the categories). Such proposals, if implemented, would significantly affect cross-border flows of data and pose barriers to free trade. The rules also impose obligations on all e-commerce entities without regard to unique e-commerce models and relationships between the entities, buyers, and sellers. It is also unclear how the requirement for every e-commerce entity to register itself with the Department for Promotion of Industry and Internal Trade (DPIIT) is connected with protection against unfair trade practices by e-commerce entities and creates an arbitrary and artificial distinction between offline sellers and e-commerce entities as registration requirements do not apply to offline sellers. Such additional non-tariff barriers have a dampening impact on the market access of foreign players into the Indian e-commerce market.

Source Code Disclosure as Precondition for Product Certification: As a part of its Communication Security ("COMSEC") scheme, implemented pursuant to the India Telecom Security Assurance Requirements ("ITSAR"), India's Department of Telecom requires U.S. companies to disclose valuable U.S. source code as a condition for market access. USTR raised this issue via the U.S. Ambassador to India in January 2025. Submission of source code was originally mandated and then the Indian Government reformed the requirement via a notification in June 2025. OEMs are no longer required to submit source code for certification. Instead, they are now required to submit the following: 1/internal test report excluding IP information, including summary of security vulnerabilities/weaknesses classified by risk; and 2/ The "Self Declaration of Conformity" stating that the source code is free from specific vulnerabilities and an undertaking stating, in case of an attack due to product in question, source code will be submitted for testing.

This new requirement continues to be a challenge. The threshold and arbitration of attack or incidence is not defined. Source code includes algorithms, protocols, or defence-in-depth mechanisms that are export-controlled under US Law. The requirement to provide source code in the event of an attack/incident still remains. The threshold and arbitration of attack or incidence is not defined. Source code includes algorithms, protocols, or defense-in-depth mechanisms that are export-controlled under US law. The format proposed by the government for internal test reports is not relevant as they generate a lot of false positives. Vulnerabilities flagged under this tool do not always translate to actual threats in deployed environments. There is also an unrealistic expectation of the code being free from certain vulnerabilities. Industry recommends the following:

1. Security certifications must be based on international standards (e.g., Common Criteria, ISO/IEC 27001/62443).
2. Penetration testing and product-specific Vulnerability Assessment and Penetration Testing (VAPT) by certified labs under agreed scopes instead of source code testing.
3. Support for secure-by-design and secure development lifecycle processes.

The United States does not require the disclosure of source code as a precondition of market access. Second, U.S. companies cannot provide this source code without the appropriate U.S. export licenses issued by the Bureau of Industry and Security ("BIS") under the U.S. Department of Commerce. Third, the disclosure of source code creates an unacceptable risk that important intellectual property may be stolen. The ITSAR documents for LAN Switches are currently under consultation and are expected to be notified soon. India also requires that all OEMs change their source code to "clean up" security vulnerabilities across notified products, but a deeper understanding of the source code development cycle is required to adequately address the country's security concerns. Moreover, India is demanding that companies turn over internal test reports and testing algorithms, which are proprietary. Again, submitting such reports could constitute a technology transfer that would require a

U.S. export license.

Services Barriers - Telecommunications

Draft Telecom Bill: India has put out a draft telecom bill that significantly broadens the definitions of telecom services and telecom equipment to include almost all digital or telecommunications goods and services. Such services including email, messaging, machine-to-machine communications, cloud services will need to be licensed under this new law, and will be subject to onerous licensing, KYC conditions, and raises serious privacy concerns. **With the bill currently under consideration, NFTC urges USTR to take active steps to push back against its proposals.**

Other Non-Market Policies and Practices

Tax Issues: US multinationals continue to face a challenging tax environment in India. Systemic issues with India's tax system have been highlighted repeatedly during the last decade or so, and while the Indian government has recognized problems with its administrative practices, there has been only limited progress towards alleviating them. The poor success rate in India's courts by India's tax authorities is an indication of improper handling of these assessments. The situation is exacerbated by the backlog of tax appeals and litigation in India's overburdened courts, resulting in an extremely lengthy (often 15-20 years or longer) and costly process to resolve a tax controversy. Further, US companies have experienced that India's tax auditors quite often refuse to follow a controlling judicial decision or provide unsupported reasons not to refund taxes following an adverse court ruling.

NFTC urges USTR to insist that India implement reforms to its tax administration, including but not limited to: (1) assessing tax if and only to the extent supported by reasonable technical positions with a basis in the law and taking into account likelihood of success in the court system; (2) removing any incentive for tax auditors to take unsupported positions, such as by requiring for government budgeting purposes the inclusion of a fair estimate of refunds likely to be recovered by taxpayers; (3) creating an incentive structure for assessing officers to be measured based on making well-grounded assessments; and (4) promptly issuing refunds to taxpayers when they are appropriately due, particularly if required to do so by court decision. An additional step would be if USTR (in coordination with US Treasury) could convince India to accept binding arbitration in its tax treaty with the US, which arbitration could be initiated at the request of the taxpayer in the event that MAP does not lead to an agreed resolution.

Indonesia

Import Policies

WTO Information Technology Agreement Commitments: Indonesia continues to contravene its WTO binding tariff commitments by charging tariffs on a range of imported information technology (IT) products that are covered by Indonesia's commitments under the Information Technology Agreement (ITA) and should receive duty free treatment. Indonesia has only implemented ITA commitments that fall under 5 categories of goods/HS codes (Semiconductors, Semiconductors Equipment, Computers, Telecommunications Equipment and Software, and Electronic Consumer Goods). Further, Indonesian Customs has also sought to re-classify IT products into dutiable HS codes that are outside of the 5 categories as a means to raise revenue, but in most cases the reclassified dutiable HS codes are also themselves covered by Indonesia's ITA commitments. For example, Indonesia continues to impose duties on printers and related parts, data center and networking equipment (e.g., routers, switches, servers and server racks, optical modules, and optical cables), and other ICT products, such as solid state drives, that are covered by the ITA. This practice widely affects the IT industry and negatively impacts U.S. investors and their workers.

Restrictions on imports under $100: In September 2023, the Ministry of Trade ("MOT") issued Regulation No. 31/2023 ("Reg 2023"), which prohibits foreign merchants from selling any goods valued below $100 to Indonesian customers via online marketplaces and includes several other discriminatory requirements that will restrict imports and foreign investment in Indonesia, including a requirement for foreign ecommerce platforms to receive a permit from the Ministry of Trade in order to conduct business activities in Indonesia and mandates that platforms that meet certain criteria appoint a locally based representative. Additionally, it prohibits companies with a marketplace business model from acting as a manufacturer and selling their own branded products. Reg 2023 appears to violate Indonesia's international trade commitments, including under the WTO, and will directly affect U.S. exports and the ability of U.S. companies to operate in the country.

Import Restrictions - Survey Report (SR) Requirement: The Ministry of Trade ("MOT") Regulation No. 87/2015 ("Reg 2015") applies to imports of goods classified in specific HS codes including servers. The importer is required to appoint a company accredited by the Indonesian Government (known as the "Surveyor") to inspect its shipment in the origin prior to Customs clearance. The SR requirement was initially enforced by Indonesian Customs ("Customs"), until MOT Regulation No. 51/2020 ("Reg 2020") introduced a post-entry SR inspection process administered by the Directorate General of Consumer Protection and Trade Compliance of MOT, effective on August 28, 2020. Reg 2015 was repealed and replaced by MOT Regulation No. 20/2021 ("Reg 2021") effective on November 19, 2021 to introduce new HS codes requiring SR. The product scope covers imports including servers, cooling equipment, hard disk drives, network interface cards and battery back-up units. The SR can cost up to US$1,600 per shipment and significantly increase the supply chain costs. Although both Reg 2015 and Reg 2021 allow capital goods to be imported without SR if an exemption letter from the MOT is obtained, there has been limited transparency and timeline provided for applying for and issuing such exemption.

Prohibition on Import of Refurbished Products: Indonesia does not permit the import of refurbished products. This policy is unfair because refurbished products and components are essential to supporting customers with warrantied products that have reached end-of-sale without components available as new products. In particular, critical infrastructure customers are unable to obtain replacement parts to service and maintain important infrastructure without access to refurbished products.

Technical Barriers to Trade

Product Compliance Certification and Testing Requirements for Imports: Under Kominfo Regulation 3/2024, Indonesia requires the individual importer of a product to obtain a product compliance certificate for each product to be imported. A partner or distributor of U.S. products importing products for customers in Indonesia must obtain individual certificates for the products in its own name and cannot rely on certificates obtained by a U.S. company This means that the U.S company's contracted importer of record ("IOR") must obtain certificates held in its own name even when importing products for a company's own internal use.

Furthermore, Indonesia requires importers to acquire a separate certificate for the same product that is imported by different parties. A separate certificate is required for a product that has the same IOR but has a different country of origin. Such burdensome regulations deviate far from other countries' certification programs.

Indonesia also requires product labelling on both the chassis and the packaging. Because certification is tied to the IOR, this requires the IOR to open the package to relabel the product. However, an IOR does not have a legal right to open a package. Such impractical and contradictory regulations create high

compliance risks for U.S. suppliers.

Additionally, Indonesia requires in-country conformity assessment testing for many consumer goods, including ICT products. Such requirements are covered in various regulations, including Komdigi's Ministerial Regulation 12/2025 that requires a product compliance test report to be issued by a domestic telecommunications device testing center, or by testing centers in countries that have mutual recognition agreements ("MRA") on testing with Indonesia. Komdigi Ministerial Regulation 13/2025 was announced later to enforce the mandatory MRA requirement from Dec 31, 2026. The United States does not have such an MRA arrangement with Indonesia. South Korea remains the only country with an MRA with Indonesia, and there is no indication that Indonesia would negotiate MRAs with other countries.

Indonesia's Ministry of Trade is preparing to expand the scope of regulated goods required to obtain Safety, Security, Health and Environment (K3L) registration. The new proposed K3L obligations would cover a broader range of product categories, including electrical and electronic goods. The expanded scope of mandatory local testing is redundant and adds no extra safety value commensurate with additional burden, significantly delays market entry, and increases costs for both industry and consumers. The regulation's requirement for samples to be collected from warehouse through random sampling adds layers of logistical burden, as keeping products stored in-country until the K3L certification process is complete would disrupt supply chain and delay customer fulfillment delivery times. There should also be harmonization and recognition of test reports done by other agencies such as the Ministry of Communications and Digital Affairs. There is also a need to provide for enough transition period (at least 12-18 months) for vendors to manage the change of scope of products covered, with exemption for legal and existing products in the market.

Indonesia's certification and testing requirements are unfair, because they unduly increase costs for U.S. exporters. The tests are duplicative and burdensome for U.S. suppliers whose products have already bene tested for safety and conformity elsewhere. Such regulatory hurdles also result in delays and hurt the Indonesian customers' access to products.

Government Procurement

Hardware, Software, and Public Procurement: Local Content Requirements (LCR) create uncertainty and limit the ability of international service providers to serve local customers. The recently issued Ministry of Industry (MoI) Regulation 35/2025 ("Reg 35"), which replaces MoI Regulation 16/2011, regulates goods and services generally, absent specific LCR regulations. Reg 35 now explicitly governs certain categories of "Industrial Services", which include ten (10) business activities under the category of "Industry 4.0 Support Services", including software, cloud services, and data center (hosting) activities among others. However, similar to its predecessor, the prescribed calculation methods in Reg 35 still do not consider the unique nature of certain goods and services, such as cloud, which leads to uncertainty on the applicability and impact of this regulation on cloud and software businesses. Meanwhile, Presidential Instruction No. 2/2022 stipulates LCR thresholds in government procurement, resulting in uncertainty of the eligibility of cloud services to participate in government procurement given the unclear LCR calculation methods for cloud. The government's e-catalogue does not recognize cloud services as a separate category, complicating compliance as cloud is currently categorized under software in public procurement. Protectionist sentiment in the administration may drive stricter LCR enforcement for cloud service providers participating in government procurement, requiring certification by local assessors despite the absence of sectoral guidelines from the MoI. Following the negotiation on Framework for US-Indonesia Agreement on Reciprocal Trade earlier this year, Indonesia is expected to work on exempting U.S. companies and originating goods from LCR. However, enforcement is unclear, especially after the issuance of Reg 35 less than two months after the hand-shake trade deal was announced in July

2025. Indonesia needs to deliver on its commitment by effectively exempting US companies and originating goods from LCR.

Services Barriers

Localization under E-Commerce Regulations: Indonesia's Government Regulation No. 80/2019 (GR80) on E-Commerce draws a clear distinction between domestic and foreign e-commerce business actors, and prohibits personal data from being sent offshore unless otherwise approved by the Ministry of Trade through a list of countries which can store Indonesian e-commerce data. This effectively requires e-commerce business actors to locally reside personal data for e-commerce customers. GR80 poses *de facto* data localization measures and local content requirements, which increase overhead costs for foreign entities and create undue market barriers.

WTO E-Commerce Moratorium: Indonesia has long opposed U.S.-backed multilateral efforts to renew the WTO Moratorium on Customs Duties on Electronic Transmissions ("Moratorium"). The Moratorium reflects the WTO Members' longstanding commitment to avoid imposing customs duties on electronic transmissions, including software and other digital products. Despite the overwhelming global support to extend the Moratorium, beginning in 2022, Indonesia joined India, Sri Lanka, Pakistan, and South Africa to oppose renewal of the Moratorium at the 13th WTO Ministerial Conference ("MC13").

Similar to South Africa, recently, Indonesia has since indicated its intention to support the WTO Moratorium, though it remains to be seen if Indonesia will indeed do so. However, Indonesia has not yet removed rules under Ministry of Finance Regulation 26/2022 that established import categories for software downloads and digital products under Chapter 99 of its tariff schedule (and provide assurance that the digital products would remain duty-free), as well as Ministry of Finance Regulation No. 190/PMK.04/2022 that established a new import declaration procedure for intangible goods, which had paved the way for Indonesia to administer and collect duties on digital products should Indonesia decide to impose unilateral tariffs on digital products and electronic transmissions.

Import Duty on Electronic Transmission of Digital Goods: Throughout 2018-2022, Indonesia's Ministry of Finance (MoF) issued regulations that aim to collect duties on digital goods. MoF Regulation No. 17/PMK.010/2018 added software and other digital products transmitted electronically, including applications and multimedia products ("intangible goods"), to Indonesia's tariff schedule with import duty rate set at 0%. Later, MoF Regulation No. 190/PMK.04/2022 required an import declaration for intangible goods, which effectively established a customs administrative regime that would result in significant compliance costs and administrative burdens for businesses, such as a custom declaration within 30 days of paying for the intangible goods and import and custom duties, and enable Indonesia to collect duties on intangible goods if Indonesia decides to increase the applicable duty rate from the existing 0%. No other country in the world has similar regulations in place, and such imposition of digital duties is against the international agreement of the WTO Moratorium on Customs Duties on Electronic Transmissions, which Indonesia is a party to and has been in place since 1998. Following the bilateral negotiation on Framework for US-Indonesia Agreement on Reciprocal Trade earlier this year, Indonesia has committed to eliminate existing HTS tariff lines on "intangible products" and suspend related requirements on import declarations. Indonesia is also to support a permanent moratorium on customs duties on electronic transmissions at the WTO immediately and without conditions. It is imperative that the Indonesian government delivers on its commitments by removing intangible goods from its tariff schedules and eliminating the related import declaration requirement, as well as continuing to support the WTO Moratorium on customs duties for intangible goods.

Electronic Payment Services: Government of Indonesia should continue to provide a level playing field. Including by ensuring that:

- Bank Indonesia does not undertake regulatory requirements that hinder U.S. electronic payment services (EPS) companies from processing data internationally and introducing innovations in risk and security to the Indonesian market. Specifically, Under Article 71 (6) of Bank Indonesia Regulation (PBI) 23/7/2021, Bank Indonesia has the discretion to exempt transactions from onshore processing requirements. [Article 71 (6): "The payment transaction may be processed outside the territory of the Republic of Indonesia to the extent it has been approved by Bank Indonesia"] Therefore, Bank Indonesia should formalize the current market practice of allowing domestic credit card and e-commerce transactions to be processed offshore. This aligns with the Bank Indonesia (BI) Payment System Blueprint 2030's goal of enhancing transaction security and protecting the payments ecosystem and consumers.
- BI should amend regulations on card security to allow for use of internationally accepted chip standards for all domestic card transactions, including for contactless debit (tap-to-pay).

Specifically, current regulations related to card security for contactless (tap-to-pay) transactions require a separate domestic chip standard (NSICCS) that is NOT interoperable or compatible with international (EMVCo) standards [BI Regulation (PBI) 23/11/2021 and Board of Governors Regulation (PADG) 24/7/2022]. In practice, this has resulted in only the domestic chip standard (NSICCS) being used for routing/processing of domestic debit transactions, which in turn prevents Indonesian banks from enabling tap-to-pay features for domestic debit transactions. To facilitate greater participation of all networks and a wider range of choices for consumers, BI should amend the regulation to allow for use of the international standard, with interoperable EMVCo chips, to be used for contactless debit transactions. Both EMVCo and NSICCS standards are complementary and in alignment with BI's approach to developing the QR Indonesia Standard (QRIS), which leveraged internationally accepted EMVCo QR standards. Both standards, governed by PBI 23/11/2021 and PADG 24/7/2022, emphasize the use of standards to enhance payment security. Using national standards that are not interoperable with global standards contradicts the goal of creating a secure payments ecosystem.

Electronic Transaction Tax (ETT): Under Law 2/2020, Indonesia introduced a series of changes to its tax code, including an expansion of the definition of permanent establishment for purposes of Indonesia's corporate income tax and a new electronic transaction tax (ETT) that targets cross-border transactions where tax treaties prohibit Indonesia from taxing corporate income from the transaction. The ETT blatantly discriminates against foreign companies as it only applies to non-Indonesian operators. Its efforts to deem foreign companies with SEP (significant economic presence) as permanent establishments undermine the traditional definition of a permanent establishment and create a significant barrier to cross-border trade. MOF would need to issue additional legal measures for these new taxes to go into effect. Such proposals are based on an unprincipled and unsupported distinction between digital and non-digital companies.

Data Localization: Indonesia is currently planning to revise Government Regulation No. 71/2019 ("GR71") that, based on the 2024 draft, potentially includes the expansion of data localization mandate to include five (5) broadly defined categories of data: civil registration, immigration, health, financial and 'other' data as determined by relevant ministries or institutions. The 'other' category is intentionally vaguely defined to allow for practically unlimited scope of data that must be stored in Indonesia. Data localization requirements limit the ability of international service providers to serve Indonesian customers with features and services that may not be available locally, as well as potentially restrict Indonesian enterprises from providing their services to global customers. Expanding data localization requirements will also result in significant expenses that could otherwise be allocated to research and development to benefit Indonesian enterprises. Meanwhile, given the advances of technology and the cross-border nature

of cyber threats, such restrictive policy may not necessarily improve the security posture and sovereignty of data that the government wishes to achieve.

The Personal Data Protection Law (2020) includes a broad exterritorial scope provision that applies to organizations if their processing activities have legal consequences in Indonesia or cover Indonesian citizens outside of Indonesia. The law includes broad record-keeping obligations and the introduction of vague and novel categories of data, such as "specific personal data." Further, the draft Implementing Regulation of Law Number 27 of 2022 regarding Personal Data Protection introduces stringent cross-border data transfer requirements including strict conditions for relying on consent for such transfers (e.g. where such transfers are non-recurring and involves a limited number of data subjects). Transfers of personal data outside of Indonesia should be more permissive and less stringent to facilitate cross-border data flows/businesses.

Data Localization (Financial Services): Bank Indonesia (BI), especially through BI Regulation (PBI) No. 23/6/PBI/2021 on Payment System Providers and PBI No. 23/7/PBI/2022 on Payment System Infrastructure Providers, requires payment transactions to be processed domestically. Meanwhile, the Financial Services Authority (OJK) has gradually allowed certain financial services entities, such as insurance companies and non-bank financial institutions with specific asset thresholds, to use offshore electronic systems and data centers. Commercial banks may also use offshore electronic systems and data centers for non-core workloads, such as for risk and internal management purposes, but core banking workloads must still be stored and processed in Indonesia unless approved by OJK.

Access to Electronic Data and Systems: On top of data localization, the planned revision of GR 71 may also allow government and law enforcement greater access to electronic data and systems. This may lead to excessive government power in demanding data and system disclosure without due process. In practice, digital platforms and service providers have experienced challenges with addressing government data requests, as many are made without clear objectives and legal basis and with arbitrarily short timelines. GR71 revision may expand this authority even further, while unclear scope and mechanism of "access to electronic systems" will also increase cybersecurity risks and undue exposure of trade secret and proprietary information.

News Media-Related Digital Service Taxes: In February 2024, the government signed a Presidential Regulation directing specific digital platforms to pay news organizations for news content that appears on those platforms. This regulation, while seemingly neutral, primarily targets U.S. companies – the goal of extracting revenues from such companies and subsidizing local news outlets is evident from the explicit goal of the regulation, which states that digital services companies have a "responsibility" to support news organizations. The regulation mandates collaboration (paid licenses, profit sharing, data sharing) and empowers the Implementing Committee (the KTP2JB), comprising mostly media company members, to implement rules and oversee arbitration, creating a conflict of interest. The Regulation also allows for directing platforms to design algorithms supporting quality journalism, though it lacks clear mandates for disclosing algorithmic changes or user data to publishers.

Content Moderation: Indonesia is advancing a series of content moderation regulations that create significant uncertainty and operational risks for the digital ecosystem. Regulations such as GR No. 5/2020 and the Child Protection/PP Tunas regulation impose unworkable compliance demands on digital platforms. The regulations impose extremely short content removal deadlines (4-24 hours), use vague definitions of prohibited content, and require government access to systems and data without a robust legal process. Non-compliance carries severe penalties, including substantial fines and the blocking of access to services. Further, new regulations are on the horizon, including a leaked broadcasting bill and a planned revision to the Police Law, that could grant authorities expansive powers to censor content and

restrict internet access. Overall, Indonesia is creating a regulatory environment that trends backward for freedom of expression and predictable business operations.

Discriminatory Local Standards: Through various regulations, the government has been requiring service providers to possess Indonesian National Standard (SNI) certificates as part of the public procurement process, while not acknowledging the international equivalence (ISO). Most recently, the Ministry of Communications and Digital Decree No. 519/2024 requires public cloud providers to possess local certificates to pre-qualify to be part of the National Data Center Ecosystem. The standards listed are SNI ISO 9001, SNI ISO/IEC 27001, SNI ISO/IEC 27017, and SNI ISO/IEC 27018 – without accepting the international ISO equivalent. The requirements are designed to be more easily met by local providers, including by requiring a local entity and local presence, as well as local content, presenting an uneven playing field for international providers. Furthermore, some requirements are listed without further implementing guidelines, resulting in local certifiers incapable of issuing such certificates. The recent draft of cybersecurity law also suggests potential additional local standards and certifications for cybersecurity service and infrastructure providers. These requirements add to compliance costs and prevent international cloud providers from serving potential customers, especially in the public sector.

Cybersecurity Bill: Indonesia's proposed Cybersecurity Bill raises significant concerns for cloud service providers and data center operators due to its expansive scope and overlapping regulatory authority. The draft legislation creates regulatory uncertainty by distributing cybersecurity governance and incident response authority across multiple agencies - Kominfo (through Komdigi), BSSN (National Cyber and Crypto Agency), Police, and Military - without clear delineation of roles and responsibilities. This fragmented oversight structure could create significant operational complications for cloud and data center providers, particularly during security incidents where multiple agencies may issue conflicting directives.

The bill contains several provisions that could substantially impact data center operations, including new security requirements, certification processes, and compliance monitoring systems. Of particular concern is the potential expansion of government access requirements and unclear incident reporting mechanisms, which could conflict with global security standards and best practices. The legislation's current form suggests a move toward increased data localization and more stringent compliance requirements that could create unnecessary operational barriers for international service providers.

These requirements, combined with the overlapping regulatory authority, could lead to increased compliance costs, operational disruptions, and implementation challenges for U.S. cloud service providers and data center operators. The lack of clear authority delineation between agencies not only creates regulatory uncertainty but also raises concerns about the ability to maintain consistent security standards and operational efficiency. The bill's current structure appears to deviate from international best practices for cybersecurity governance and could create unnecessary market access barriers that may impact the quality and availability of cloud services in Indonesia.

MOCDA blocking Global Companies. Indonesia’s Ministry of Communication and Digital Affairs (MOCDA or Komdigi) has notified 36 global companies (including US-based companies) to register as electronic system operators (ESOs) with Komdigi. Several companies have had to block access to users due to a lack of ESO registration. Though some companies have been able to restore access to users following consultations with the Indonesian government, some may be required to establish a local entity in Indonesia. Further, Indonesia also announced that a 0.5% income tax on e-commerce transactions would take effect in February 2026, with major platforms designated as tax collectors, though implementation of this policy will be postponed until the economic growth achieves certain levels.

Services Barriers - Telecommunications

Submarine (Telecom) Cable Connectivity: Various measures create significant barriers for international operators to deploy and operate submarine cables in and around Indonesia. These include: Ministry of Fisheries and Marine Affairs Decree No. 14/2021, which limits all submarine cables in Indonesian waters to a limited number of prescribed routes and landing points that different ministries have different interpretations of; requirements for submarine cable operators to obtain overlapping licenses from multiple ministries; and requirements by the Ministry of Communication and Digital Affairs for international submarine cable operators to have minimum 5% ownership by local partners who must meet unreasonably stringent qualification criteria.

Other non-market policies and practices

Local Content Requirements: Local content requirements (LCR) are a growing concern for global industries, including the pharmaceutical industry. Recent developments include the issuance of Minister of Industry Regulation No. 35/2025, which introduces potential flexibility in local content calculations for global companies by formally recognizing "brainware" contributions. However, the certification process for product-based local content remains challenging, particularly for fully imported goods. Moreover, the regulation's mandate to prioritize products with local content may disadvantage those with minimal or no local input—regardless of their quality or performance. Articles 327 and 328 of the Omnibus Health Law (Law No. 17/2023) explicitly dictate that the government and healthcare facilities – both public and private – must prioritize the procurement and utilization of domestically produced and sourced pharmaceuticals and medical devices, imported products will only be used if there are availability or supply issues. This further escalates the aggressive import substitution policy pursued in recent years, which has centered around the imposition of local content requirements as well as the "freezing" of imported products from the public procurement catalog should local alternatives be available. Separately, Presidential Instruction No. 6/2016 mandates local content requirement calculation to be used as a criterion for government procurement of biopharmaceutical and medical device products. Finally, this trend was further bolstered by Presidential Decree 2/2022, which prioritizes government procurement of products with domestically produced raw materials, specifically those with a local content threshold of at least 25 percent. It is critical that these requirements are not applied in a manner that restricts patient access to innovative medicines in Indonesia and that greater recognition is given to biopharmaceutical innovators for their contribution in bringing innovative therapies to Indonesia.

Local Content Certification Requirements: Indonesia maintains several local content policies applicable to ICT equipment and is contemplating a range of other limitations. For example, the "Neraca Komoditas" (commodity balance) policy is intended to force domestic production by using trade imbalances as a rationale for quotas or outright bans. ICT and electronic devices could potentially be included in the scope of the policy. In addition, in September 2020, the Indonesian Ministry of Industry released Regulation No.22/2020 (IR22) on the Calculation of Local Content Requirements ("LCR") for Electronics and Telematics, with a government target to achieve 35% import substitution by 2022. Although it is unclear whether the government has achieved this target, the recent ban on imports of ICT goods suggests that this policy will continue to place an additional administrative burden on the production of physical ICT products that are indispensable for ICT companies to operate in Indonesia. Such onerous requirements cannot be met without vendors establishing a manufacturing presence in Indonesia.

These local content policies are unfair, because they discriminate against American companies in favor of local Indonesian companies, without any consideration of quality or security. In particular, electronic public sector bids require participating vendors to pre obtain a certificate demonstrating the vendor's qualification in meeting local content requirements, including having manufacturing facilities in Indonesia.

There is also a plan to revise the Ministry of Trade Regulation 08/2024 regarding the third Amendment to the Minister of Trade Regulation 36/2023 regarding Import Policies and Provisions. While the regulation aims to address container backlog at the port, the new revisions are likely to re-introduce additional hurdles to the import process and more restrictive technical consideration (Pertimbangan Teknis/Pertek), Import Approval (Perizinian Import/PI) and quota. These actions, aimed at protecting domestic markets, represent major non-tariff barriers for all products entering Indonesia. The regulatory changes would be graduated, with an initial focus on clothing goods and other commodities, including electronics, potentially at a later stage.

The ICT and electronics industry actively advocated for a higher allocation of non-physical product factors, such as R&D and training, in Indonesia's LCR calculation. While the Indonesian government has shown some receptiveness to these proposals, it remains unclear whether such inputs had been incorporated in the inter-ministerial discussions on the LCR regulation revision. The Indonesian government is currently considering a more streamlined and integrated method for calculating LCR. However, the LCR computations heavily rely on the cost of materials, labor and factory overhead, and the proposed revisions would still require the industry to invest and build manufacturing facilities in Indonesia.

Price Controls: Indonesia is moving in the direction of increased state control over drug and medical device prices under the pretext of ensuring equitable and affordable health access for patients, while in fact it could threaten patient access to innovative treatments. The Omnibus Health Law, which was issued in August 2023, gives the government authority to regulate and control the price of drugs and medical devices in the context of securing their accessibility for public health and making necessary interventions. It is yet unclear how controls will be implemented. The government is also developing an online "pharmaceutical and medical device dictionary" where the public can get access to information about the products, including their price. With this kind of price transparency policy, the government expects that hospitals and pharmacies will feel discouraged to set high drug prices so that people can buy drugs at affordable prices. In addition, listing decisions on the National Formulary (FORNAS) appear to be primarily based on price, whether the medicine and vaccine is locally produced, and the overall National Health Insurance (JKN) budget. It is important for the policymakers to start looking at value-based pricing to ensure that innovation is being valued.

Israel

Services Barriers

Investment Obligations: Under the draft bill released by the Israeli Ministry of Communications in 2022-23, international streaming services and domestic content providers classified as "medium" or "large" (e.g., those with annual revenues over NIS 300 million) would be required to invest in local productions at rates of 2 % of annual revenue for medium players and 4 % for large players. If enacted, proposed streaming content obligations would impose new financial and operational burdens on U.S. streaming platforms.

Japan

Import Policies

Express Delivery: U.S. operators remain concerned by unequal conditions of competition between Japan Post Co., Ltd. (Japan Post) and international express delivery suppliers. Private U.S. express carriers are required to declare all shipments for customs clearance and calculate duties and consumption taxes based on cost. Different procedures called a duty assessment system apply to Japan Post including their competitive product of Express Mail Service (EMS). **NFTC urges USTR to insist Japan to establish equivalent conditions of competition between Japan Post and international express delivery suppliers in terms of customs procedures and requirements.**

The customs issues came from the privatization process of Japan Post back to 2007. When the privatization was determined, the Ministry of Finance, in response to industry's strong push for equivalent conditions of competition, enacted a bill to revise customs clearance procedures for international postal mail. The bill requires Japan Post to adopt a duty declaration system for international postal import and export items with a value of more than JPY200,000. The threshold is very high and the imported items with a value of more than JPY200,000 in 2007 constituted only 0.06%. Thus, industry has been requesting GOJ to lower the threshold over the years, which GOJ explained to the industry as their plan in 2007. They still maintain the threshold and the issue remains heavily as a non-tariff barrier in Japan.

Security Clearance Requirements for Private Sector: Japan formulated security clearance requirements for private companies to handle confidential-level government information. The current rules require companies to have dedicated physical space, security measures such as fence and locks, storage containers with keys, and stand-alone computing system with no internet connection. Such requirements favor on-prem solutions and discriminate against the use of cloud services/solutions (e.g. access controls) to handle sensitive government workloads (e.g. in public sector procurement opportunities). A risk-based and technology neutral approach to security clearance would be a fair alternative.

Excessive Information required under Economic Security Scheme: Japan has introduced the Economic Security Scheme to ensure the protection of critical infrastructure. This regulation requires suppliers to submit an excessive amount of detailed, proprietary information for the government to evaluate made-in-China products. The United States and other similar economies do not require such information.

Technical Barriers to Trade

Repeated Price Cuts to Patented Medicines: Japan devalues new innovative medicines through draconian rules that set low prices for patented medicines at launch and then exacerbates this problem by aggressively cutting prices throughout the patent period. Following National Health Insurance price listing, Japan applies a growing number of re-pricing rules in a highly unpredictable and arbitrary manner that significantly erode prices and expected revenues of patented medicines. Overall, about half of patented medicines launched in Japan are subjected to annual price cuts.

Biased Health Technology Assessments: For new innovative medicines awarded a price premium at launch for demonstrating clinical superiority over a comparator, Japan conducts biased "cost-effectiveness" evaluations using low and outdated monetary thresholds per life year gained to cut these price premiums by up to 90%.

Government Procurement

Information System Security Management and Assessment Program: Japan's Information Security Management and Assessment Program ("ISMAP") is a security certification scheme that applies to

government procurement of cloud services. ISMAP has historically imposed significant compliance burdens and costs to service providers. Japan then expanded ISMAP to cover all key infrastructure, including telecommunications.

Most cloud and telecommunication service providers already have internationally accredited certifications (*e.g.*, ISMS-JISQ/ISO 27000 series, SOC2), but ISMAP requirements go above and beyond these certifications without providing any additional security. They create additional costs not imposed by U.S. authorities procuring similar services.

Intellectual Property Protection

Patent Term Restoration (PTR): Japan's PTR laws as currently interpreted by the Japanese Patent Office (JPO) often result in extensions for subsequent marketing approvals which are shorter in term than the extensions for the original approval and can thus act as a disincentive to conduct research on additional medical uses and indications, including new formulations for an approved product.

Patent Enforcement: Actions by the MHLW to approve generic versions of an innovative product, including during ongoing litigation, raises concerns for industry as to Japan's commitment to effectively enforce patents. While injunctive relief is typically available in Japan, such relief can take at least several months to secure, thereby frustrating the ability of the innovator to seek an injunction before potentially infringing products are allowed to enter the market. MHLW is considering reforms to Japan's early patent dispute resolution practice.

Services Barriers

Digital Platform Regulation: The Act on Improving Transparency and Fairness of Digital Platforms (the Digital Platform Act) imposes additional obligations on large companies designated by METI as "specified digital platform providers" for specific services, including "general online shopping malls selling goods," "application stores," "media-integrated digital ad platforms," and "ad intermediary digital platforms." The "specified digital platform providers" designated by METI have disproportionately captured U.S. firms compared to their Japanese and third country competitors and therefore undermine U.S. competitiveness in Japan by increasing the compliance costs on certain U.S. firms while not placing a similar burden on their competitors.

In a similar way, in 2024, Japan adopted the Smartphone Software Competition Promotion Act, modeled after the European DMA, targeting major mobile OS, app stores, browsers, and search engines of a certain size. In March 2025, the JFTC designated only two U.S. companies under this law, excluding domestic competitors based on their monthly active user calculation methods. As the law's subordinate guidelines are reviewed for final approval, there remains a risk that if not adjusted the guidelines will include overly prescriptive rules (with draft guidelines exceeding 100 pages) and lack the incorporation of crucial concepts like "user convenience" despite a Diet resolution emphasizing its importance, placing significant compliance costs and prohibitions on certain U.S. firms without placing a similar burden on their Japanese or third country competitors.

De Minimis Threshold for Consumption Tax on Imported Goods. Starting in April 2025, certain online providers assumed responsibility to collect and remit consumption taxes on behalf of non-Japanese businesses providing digital services to consumers in Japan. The current transaction threshold is JPY 5 billion. There have since been discussions about expanding these policies to include additional cross-border e-commerce transactions. This higher threshold could potentially create disparities in the broader market. In short, a lower threshold would help ensure a level playing field among all platforms. In tandem, it is also important to evaluate de minimis import thresholds, in addition to the lens of taxing

online platforms. Furthermore, as Japan refines its digital platform taxation framework, it is important to further promote the digitalization of administrative procedures to ensure the system's effectiveness. Fully digitizing tax and customs-related procedures and additionally making them accessible in English will help reduce compliance costs for U.S. companies.

Economic Security Promotion Act: Subsidies for the provision of Cloud services/GPUs under the Economic Security Promotion Act have distorted the level playing field for US cloud service providers in Japan. Japan service providers benefiting from subsidies have an unfair advantage, winning government procurement contracts with bids that are significantly lower than comparable market prices.

Policy Barriers for Cloud Adoption in National Security and Defense: The government's information security guidelines restrict the use of public cloud by requiring a stand-alone system, on-site inspection, and installation of physical facilities for restricted and classified information in national security and defense areas. Such requirements favor on-prem solutions and limit use of cloud services, hindering interoperability with allies including the U.S. in national security, cyber, and defense areas. While the Ministry of Defense announced its plan to adopt "hybrid cloud" approach for its next-generation of telecommunication infrastructure by FY2029, cloud adoption would still be limited and most of the critical workloads would remain at on-premise system without amending the security guidelines.

Subsidies

GPU purchase subsidy for frontier AI: The government plans to support the development of frontier AI models by providing a subsidy to select local businesses for their GPU purchase. The government budget for this project is expected to be billions USD. Such an arrangement favors on-premise solutions and excludes cloud service providers from supporting the project. Massive GPUs purchased by local entities could entail the risk of transshipment of computing resources to third countries including adversaries.

Kenya

Services Barriers

Data Localization: While Kenya's 2019 Data Protection Act allows for cross-border data transfers (subject to certain safeguards), the Cabinet Secretary is empowered to decide the types of personal data that must be stored and processed in Kenya to protect the strategic interests of the state and/or revenue, stricter data localization requirements have been layered in through other regulations and policies including:

- The Data Protection Regulations of 2020, which mandate the localization of a broad set of data – including national civil registration systems, population register and identity management, primary and secondary education, electronic payment systems, revenue administration, health data, and critical infrastructure – requiring that a copy of the data falling under these categories to be stored in a data center located in-country;
- The Computer Misuse and Cybercrimes Act of 2018, and the Critical Information Infrastructure Regulations of 2024, mandate localization for information classified as Critical Information Infrastructure (CII). Operators in the CII space require approvals for offshore hosting; and
- The 2020 ICT Policy, which requires that Kenyan data remains in Kenya, and that it is stored safely and in a manner that protects the privacy of citizens.

Cloud Policy: Kenya's 2025 National Cloud Policy requires sensitive categories of data to be hosted locally through local accredited providers or government cloud. While framed as a measure to strengthen national infrastructure, the preference for local storage and local providers risks excluding or disadvantaging foreign suppliers, creating discriminatory barriers to market access that conflict with

Kenya's trade commitments and undermine the competitiveness of U.S. cloud and digital service providers.

Digital Services Tax: In 2020, Kenya implemented tax laws imposing a 20% withholding tax on "marketing, sales promotion and advertising services" provided by non-resident persons, and a 1.5% Digital Services Tax (DST) on income from services derived from or accruing in Kenya through a digital marketplace. In December 2024, the DST was repealed and replaced by the Significant Economic Presence (SEP) Tax through the Tax Laws (Amendment) Act, 2024. The SEP Tax is a 3% tax on gross turnover imposed on non-resident companies that earn income derived or accrued in Kenya through services provided over the internet or any electronic network. In addition, the Tax Laws (Amendment) Act broadened the definition of "royalty" to include nearly all software-related payments, subjecting licensing, development, training, and support fees to withholding tax in a departure from international norms. Non-resident providers must also contend with new obligations, including a 20% withholding tax on digital marketplace payments and excise duty on services delivered through digital platforms, adding multiple layers of taxation that increase compliance costs and reduce profitability. Kenya Revenue Authority (KRA) published draft SEP tax regulations on 22nd Sept 2025 which are the subject of public consultation. SEP tax may increase tax burden for consumers, slow down card penetration where an exemption clause is not applicable. While the replacement of the DST was a welcome development, we urge the USTR to continue to press the Kenyan government to remove overlapping and burdensome taxation regimes that disproportionately penalize cross-border services providers and, at times, are inconsistent with international tax norms.

Content Moderation: Industry remains concerned about overbroad content moderation in Kenya, risking the stifling of innovation and free speech. In June-July 2024, the Kenyan government severely restricted internet access during protests, causing a 40% connectivity drop and costing the economy approximately US$6.3 million daily, despite prior commitments against such actions. On September 18, 2024, the Computer Misuse and Cybercrime Bill was introduced to the National Assembly, which would grant the National Computer and Cybercrimes Coordination Committee authority to block websites and apps for promoting "illegal activities" and "extreme religious and cultic practices". The Bill is still under consideration, but, due to vague definitions in the Bill, there is a significant risk of abuse were the Bill to pass. More recently, in June, 2025, amid nationwide protests marking the anniversary of the previous year's controversial Finance Bill, the Communications Authority of Kenya (CA) ordered TV and radio stations to stop live broadcasts of demonstrations. Several major stations were taken off air for non-compliance.

Jordan

Services Barriers

Electronic Payment Systems: CBJ's 2019 Circular No. 3/10/6474 aims to empower banks to make risk-based decisions under AML/CFT rules. However, its misinterpretation has delayed key global updates and innovations, harming Jordan's financial sector. An amendment to the circular is needed to exclude global payment network updates and technological advancements, ensuring seamless, secure connections to global payment systems.

Korea

Import Policies

Customs: Onerous new requirements starting from January 2026, Korean Customs Service will require enhanced data elements, like purchase order details, order numbers and website addresses. Guidelines are unclear on who is responsible for providing and for validating.

Technical Barriers to Trade

Market Access (Pharmaceuticals): Korea sets prices of new innovative medicines through a combination of referencing the lowest price among OECD countries and using low and outdated monetary thresholds per life year gained from clinically proven treatments. Two government agencies, the Health Insurance Review and Assessment (HIRA) service and the National Health Insurance Service (NHIS), force companies through a gauntlet of assessments to access the market, resulting in lengthy patient access delays following marketing authorization from the Ministry of Food and Drug Safety (MFDS). The monetary threshold per life year gained from clinically proven treatments was set equal to Korea's GDP per capita in 2007 but has not been updated even though Korea's GDP per capita has since more than doubled.

Government Procurement

CSAP: South Korea's Cloud Security Assurance Program ("CSAP") provides stringent certification requirements for foreign CSPs. The regulation directs CSPs to create Korea specific products to sell to Korean central, local, and provincial agencies and public sector institutions. In 2023, South Korea amended the CSAP and established a three-tier classification of the public institution data systems based on risk levels. Under the amended CSAP, CSPs must meet physical data segregation requirements to obtain the medium and high-risk tier certifications. Foreign cloud service providers and cloud-based services cannot meet these Korea-specific requirements. As of 2025, the CSAP certification remains valid through March 27, 2030, and continues to be administered by KISA under MSIT supervision. U.S. CSPs remain effectively excluded from nearly all of Korea's public sector market, as they are unlikely to qualify for the Moderate and High tier certifications that represent the majority of government procurement opportunities. Only those CSPs that have at least the Moderate CSAP certification can effectively participate in the government's digital transformation initiative. The United States has urged Korea to align its cloud security certification requirements with other internationally accepted standards.

Government Procurement Requirements in AI: In February 2025, the Ministry of Science and ICT (MSIT) of the Republic of Korea announced a comprehensive National AI Initiative with the strategic objective of positioning the nation among the world's top three AI leaders. This initiative encompasses critical projects, including the development of a world-class Large Language Model (LLM) and the establishment of the National AI Computing Center. However, the subsequent Request for Proposal (RFP) issued by MSIT in May 2025 incorporated a restrictive "domestic companies only" clause, effectively excluding U.S.-based CSPs from accessing a potential market valued at KRW 1.5 trillion (USD 1.1 billion).

This development has raised significant concerns among U.S. stakeholders, as several U.S. CSPs had already made substantial investments in infrastructure preparation based on preliminary discussions with MSIT. The unexpected implementation of exclusionary criteria without prior consultation not only compromises the principles of transparent government procurement but could also set a precedent for similar restrictive practices in other government AI initiatives and technology sectors. In the interest of maintaining fair competition and fostering international cooperation, it is recommended that the "domestic companies only" requirement be removed from the RFP, thereby enabling U.S. CSPs to participate in an open and equitable procurement process.

Intellectual Property Protection

Patent Term Extension (PTE) System: In December 2024, the Korean National Assembly passed the Patent Act Amendment Bill, which revises the patent term extension (PTE) system to limit the number of patents eligible for PTE based on a single drug approval, as well as setting a maximum cap on patent term including PTE (previously no cap, now the maximum cap of 14 years from the product approval date). The current PTE system also lacks due process in the PTE procedures and imposes a high-stakes, all-or-nothing approach to appeals. If the Patent Office determines a certain duration of PTE that is less than the full amount originally requested by the patentee and the patentee challenges that determination and subsequently loses the challenge, no PTE is granted; even the duration previously determined by the Patent Office is lost. This all-or-nothing approach significantly undermines a patentee's right to appeal, effectively deterring appeals of erroneous calculations, and undermines the patentee's rights.

Services Barriers

Network Usage Fees: South Korea's "sender party pays" (SPP) framework, established under the Telecommunications Business Act (TBA), requires content providers to bear the costs associated with delivering data over networks. This system has been in effect since 2016 and has been a subject of ongoing legislative discussions. In 2020, the National Assembly passed the "Content Providers' Traffic Stabilization Law," amending the TBA to mandate that large content providers ensure stable services, effectively compelling them to negotiate network usage fees with Internet Service Providers (ISPs). As of 2024, additional legislative efforts are underway to further formalize and expand these obligations, potentially imposing mandatory network usage fees on both domestic and foreign content providers. These regulations present significant challenges. The requirement to pay network usage fees can substantially increase operational costs, potentially leading to higher prices for consumers or reduced service quality. This anti-competitive environment has forced one of major U.S. companies to exit the market in February 2024, citing prohibitively expensive network costs. The United States has repeatedly raised concerns with Korea throughout 2024. **NFTC encourages USTR to recommend that the Ministry of Science and ICT to abolish the SPNP framework and return to the global standard of settlement-free peering for same-tier ISPs.**

Discriminatory Digital Trade Policies: Multiple proposed platform regulation laws (such as the Online Platform Monopoly Act, the Platform Fairness Act, and related bills) would disproportionately impact U.S. firms, and in many cases put U.S. firms at a disadvantage to other competitors, both those based in Korea and in third countries, including China. Korea has also adopted or proposed: discriminatory limitations on U.S. maps providers and geospatial data export prohibitions; discriminatory cybersecurity certifications and mandated network segregation; requirements that effectively lock out U.S. cloud service suppliers from Korea's public procurement and limit cloud usage in the financial service sector; data localization mandates, including for reinsurers; and EU-inspired AI Act that would put significant restrictions and obligations on American AI models and services.

Restrictions on Mobile Application Marketplaces: In August 2021, South Korea enacted legislation compelling mobile app marketplaces to permit in-app purchases via third-party payment systems, directly prohibiting app stores from requiring exclusive use of their own payment system, and specifically targeting U.S. companies. The Korea Communications Commission (KCC) approved implementing rules on March 8, 2022, and initiated investigations into Google, Apple, and SK Group's OneStore on August 16, 2022, for potential violations concerning in-app payments. The KCC specifically warned Google and Apple against imposing discriminatory conditions or inconvenient usage processes for third-party payments. In October 2023, the KCC proposed fines of KRW 68 billion (approximately $52 million) against two U.S. companies for alleged breaches, a decision both firms are currently still contesting. The lack of clear implementation procedures and stakeholder input has created uncertainty for businesses and risks harming Korea's burgeoning developer ecosystem. Further, the discriminatory nature in which the rules are being applied, particularly the ban on specific payment mechanisms solely for app stores, poses fundamental questions of fairness, and raises concerns about potential conflicts with Korea's trade

commitments under the KORUS and Article XVII of the WTO General Agreement on Trade in Services (GATS), which prohibit discriminatory treatment against foreign service suppliers.

Targeted enforcement: The KFTC continues to unfairly target U.S. companies with unprecedented fines, office raids, threats of prosecution, and attempts to harass American companies with criminal allegations and erroneous investigations. This enforcement culture in Korea is a troubling anomaly for a closely allied U.S. trading partner and could represent "unfair or harmful acts, policies, or practices" that present a "structural impediment to fair competition" per the Trump administration's recent Reciprocal Trade Memo.

Cloud Services: The Cloud Security Assurance Program (CSAP) was established by the Ministry of Science and ICT (MSIT) in 2016 and elevated from administrative guidance to a legal requirement through a March 2022 revision to the Cloud Computing Promotion Act. The CSAP, which applies to Korea's central, provincial, and local public sector with very limited exceptions, creates significant barriers to foreign cloud service providers (CSPs) seeking to sell to Korea's public sector. CSPs are required to comply with data localization of cloud systems, backup systems and data, and ensure that operations and management personnel of CSPs are located within the territory of Korea. CSPs must also use only National Intelligence Service (NIS) certified domestic encryption algorithms (ARIA, SEED, LEA or HIGHT), and information security systems and network equipment deployed for cloud service provision must use products verified for stability by NIS, such as those with Common Criteria (CC) certification or security function verification. Moreover, to obtain the CSAP Moderate tier certification, CSPs must build physically segregated facilities for exclusive use by public sector customers. These requirements differ significantly from internationally accepted standards and create significant barriers to U.S. CSPs seeking to sell to Korea's public sector. As of 2025, the CSAP certification remains valid through March 27, 2030, and continues to be administered by KISA under MSIT supervision. U.S. CSPs remain effectively excluded from nearly all of Korea's public sector market, as they are unlikely to qualify for the Moderate and High tier certifications that represent the majority of government procurement opportunities. Only those CSPs that have at least the Moderate CSAP certification can effectively participate in the government's digital transformation initiative. The United States has urged Korea to align its cloud security certification requirements with other internationally accepted standards.

New PIPC Personal Data Guidelines for Foreign Companies. The Personal Information Protection Commission of South Korea (PIPC) published explanatory guidelines in July to help foreign companies comply with the South Korean personal data protection law. When a foreign company processes data of South Korean citizens or carries out personal data processing on South Korean territory, it is subject to Korean legislation. The guidelines specify the main legal provisions in force, as well as some decisions taken by the PIPC or by local courts to clarify the applicable legislation for companies. This is a complex and challenging task for both domestic and multinational corporations in Korea, as there is presently no industry benchmark.

Content Moderation: Korea's *Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.* (Network Act) regulates how information and communications networks are used and policed. A new Article 44-7(5), added in January 2024, creates new content moderation burdens for providers that operate domestic servers of a certain type or scale. These providers must implement measures to identify and restrict access to unlawful information, subject to review by the Korea Communications Standards Commission. They are also required to request uploaders to halt further distribution, record and store logs of enforcement actions, and adopt additional preventive measures as mandated. For cross-border service suppliers, this provision creates significant concerns by potentially pressuring foreign companies to maintain local servers in Korea, acting as a de facto data localization requirement. It also expands liability by obligating providers to monitor, restrict,

and document user content in ways that may conflict with global business models and international trade commitments.

Furthermore, the Korea Communications Commission (KCC) is reportedly working on additional amendments to the Network Act aimed at introducing new digital content censorship. These measures would require large online platforms, primarily those based in the U.S., to censor vaguely defined "False Manipulated Information" under threat of government investigations and substantial fines. Modeled after the European Union's Digital Services Act (DSA), these proposed measures are expected to replicate the DSA's risks, including discriminatory burdens on U.S. firms and vague, onerous content regulation that may target lawful political speech. The KCC would have the power to investigate platforms' censorship systems and impose administrative fines of up to 4% of domestic sales for non-compliance, creating an incentive for platforms to over-censor and remove vast amounts of content to avoid penalties. The proposed measures also include a local agent requirement for "Large-scale" platforms without a domestic business establishment, which could violate Korea's market access obligations under the Korea-U.S. Free Trade Agreement. This pattern of discriminatory digital policies and aggressive enforcement actions against U.S. firms is troubling.

Overall, these content moderation measures are part of a troubling pattern of discriminatory digital policies in Korea, similar to other platform regulations identified above, as well as a track record of aggressive enforcement action against U.S. firms. By importing the DSA model through, Korea would be imposing similar unwarranted economic burdens on U.S. service providers, and embracing a regulatory philosophy fundamentally at odds with shared U.S.-Korea democratic values and free speech.

Artificial Intelligence: South Korea's AI Basic Act, effective January 1, 2026, broadly regulates AI business entities, including developers and deployers, without clear distinctions in obligations or liability. This creates significant uncertainty for large, often U.S.-based, AI developers who could be held liable for uncontrolled downstream uses. Concerns for cross-border service suppliers include: unsupported compute-based thresholds for "high-impact" AI, potentially targeting U.S. firms and conflicting with trade commitments; mandated public disclosures and labelling of AI outputs, risking commercially sensitive information; the requirement for foreign providers to designate a domestic agent, which could act as a disguised local presence mandate; and low thresholds for intrusive fact-finding investigations. Unless clarified, these provisions could hinder market access, impose disproportionate compliance costs, and raise trade law concerns for international AI suppliers.

Kuwait

Services Barriers

Electronic Payment Services: The Central Bank of Kuwait (CBK) is currently developing its domestic payment scheme, with potential implications for international card schemes (ICS). While no formal guidance has been issued regarding adoption or implementation, past experiences in other markets suggest that central banks may opt for models that disintermediate ICS from domestic transactions. Such approaches can create a non-level playing field and put U.S. providers on an unlevel playing field.

Malaysia

Import Policies

Refurbished Products: Malaysia requires importers to obtain a certificate of approval issued by the

Standard and Industrial Research Institute of Malaysia ("SIRIM") to import communications equipment. However, SIRIM does not undertake testing of refurbished products as import of refurbished equipment is prohibited in Malaysia. This ban on refurbished products limits U.S. suppliers' ability to support customers in Malaysia. For products still in production, new components must be sourced to support customers. For products that are no longer in production, such products cannot be supported or replaced with available refurbished parts, meaning that U.S. suppliers are forced to stop customer support or the customer is forced to upgrade to a newer version of the product.

Additionally, SIRIM requires Internet Protocol Version 6 ("IPv6") certification at the level of "IPv6 Ready Logo" for all products imported into Malaysia. While the "IPv6 Ready Logo" is a voluntary certification led by the IPv6 Forum, the certification is mandated in Malaysia. This requirement is unfair because, in the United States, this requirement only applies to government procurement. Malaysia's unique practice of specifically requiring MalaysiaIPv6 compliance for market entry is excessively burdensome and out-of-step with other countries' practices.

Charges: USD 1/RM5 charge on per shipment basis for export import in Kuala Lumpur and Penang. Collected by the airport operator Malaysia Airport Holding Berhad. The fee collected was meant to be reinvested for infrastructure development and security of the complex. After more than two decades of contribution we have seen minimum improvement.

Local Ownership: The Malaysian Ministry of Finance requires companies wanting to operate public bonded warehouses to at least have 30% ethnic Malaysian ownership and board structure. This contradicts with Malaysia Investment and Development Agency's incentives of 100% ownership through the Integrated International Logistics Status (IILS).

Services Barriers

AI Sovereignty: In recent developments, Malaysia's National AI Office (NAIO) has outlined a Sovereign AI Strategy, introducing a tiered approach to AI governance with implications for international technology providers. The strategy establishes strict requirements for compute infrastructure, data residency, and operational flows, particularly for highly sensitive government workloads. Of note, NAIO is proposing the implementation of government-owned cloud/compute capabilities for top-tier (L3) workloads and introduces new sovereignty certification requirements, even when engaging with global companies. While NAIO maintains an "ecosystem-supportive" stance open to both foreign and local providers, the strategy raises concerns about potential market access barriers and preferential treatment for domestic companies. The introduction of mandatory requirements for handling sensitive government data, coupled with new certification and auditability standards, could result in increased operational complexity and compliance costs for US companies operating in Malaysia. This evolving regulatory landscape warrants close monitoring, as it may establish precedents that significantly impact the ability of international technology firms to operate effectively in the Malaysian market.

Social Media Licensing: In 2024, the Malaysian government established a Social Media Licensing (SML) regime on social media and internet messaging platforms, imposing local registration requirements and criminal liability for local employees, as well as financial penalties. With no US company having registered to date, the government has given itself powers to "deem" US companies as licensees to place them under the regime. The government is prone to censoring political speech and content on royalty, race and religion and has arrested political opponents as well as members of the public for offences related to online speech. The SML regime gives it greater powers to censor online speech and heighten the chilling effect on US companies.

Law Enforcement Access Powers: Recent amendments to the Communications and Multimedia Act, passed with minimal consultation, grant law enforcement enhanced powers for data access and

interception, which create significant operational and compliance risks for global service providers. The new provisions empower law enforcement authorities to compel the warrantless disclosure of broadly defined "communications data", potentially placing U.S. companies in a position of legal conflict – compliance with this mandate to avoid penalties up to RM1 million (approx. US$236,000) and/or up to five years in prison could necessitate a breach of strict U.S. legal requirements that limit such disclosures. The amendments also empower law enforcement officers to enter any premises without a warrant to install interception devices which would be a red-line critical security risk for U.S. service providers, as it jeopardizes the integrity and security of communications networks; interference with this entry carries potential severe penalties of RM1 million (approx. US$236,000) and/or up to 10 years imprisonment. Given these concerns, the U.S. government should insist that Malaysia use the U.S.-Malaysia Mutual Legal Assistance Treaty (MLAT) as the sole and standard legal mechanism for requesting data from U.S.-based service providers, and concurrently seek the repeal of the intrusive power that permits warrantless entry for interception as it poses a direct threat to service integrity and security.

Other non-market policies and practices

Local Content Requirements: Local content requirements being proposed by both State and Federal authorities in Malaysia. Malaysia is moving toward imposing a Local Content Requirement (LCR), with Selangor sets to apply 30% LCR for hardware as a condition for business licenses. Federal agencies such as MITI and MDEC are advancing parallel measures, including possible reductions in import duty incentives to spur local supply chains. The government is also linking electricity tariff rebates to local purchases. Selangor's move is expected to set a precedent for other states, and the initiative is being framed as a national strategy to strengthen Malaysian semiconductor firms' access to domestic and global markets, modeled after localization policies in India and Indonesia.

Mexico

Import Policies

Shipments Valued Under 2,500: On December 30, 2024, Mexico's Tax Administration Service (SAT) published amendments to the regulations governing the clearance of express shipments, which took effect on January 1, 2025 (less than 48 hours later). This created operational havoc, widespread confusion, etc. The new regulations included a host of additional information requirements, including some that Mexico has since relaxed. Furthermore, the regulations now disqualify from express clearance procedures any shipments due ADCVD duties. Without an exemption for USMCA partners, shipments valued between US$50 and US$2,500 will likely incur higher duties than the current flat rates of 17-19%. This change not only increases operational burden but also introduces new risks related to misclassification and heightened regulatory scrutiny. Overall, these changes are yet another example of Mexico's failure to provide sufficient prior notification of changes to the trading public. On substance, these changes continue to degrade the simplified clearance channeled set out in USMCA article 7.8.2.

Shipments Valued $2,500 and Over: In a recent regulatory change, Mexico modified its regulations to disqualify all shipments valued at $2,500 and above from the simplified express clearance process. However, the USMCA requires in article 7.8.1 that Mexico maintain such a process regardless of value.

Cargo Security: The high levels of cargo theft is a critical security and safety concern spanning every NFTC member that trades in the region. The security environment in Mexico is being prioritized in bilateral discussions, but cargo security needs special attention as the risks extend far beyond the border, translating into significant costs, supply chain disruptions, and investment risks for Mexico. These costs and disruptions affect both U.S. exports and imports, and where imports are inputs destined for further processing can lead to manufacturing disruptions. **In addition to Mexico's commitments on border**

security that are being prioritized in bilateral negotiations, NFTC urges USTR to obtain commitments from Mexico of additional resources and actionable security measures to prioritize cargo safety and theft. This cooperation could be a pillar under the recently launched U.S.-Mexico Security Implementation Group, where, as appropriate, the United States can offer technical assistance, intelligence sharing and resources to support cargo safety and security.

Customs facilitation: In establishing the Agencia Nacional de Aduanas de Mexico (ANAM) as an independent customs agency separate from its tax authority, Servicio de Administracion Tributaria (SAT), industry and freight operators are experiencing significant clearance delays at the U.S.-Mexico border. In 2022, career customs officials have been replaced with military personnel who are not experts in trade facilitation, and created a fragmented border clearance with responsibilities diffused between the Army at land ports, the Navy at seaports, and the Air Force and private actors at airports. As a result, in 2025, industry is experiencing significant pain points in cargo movements, and technical and regulatory challenges in the coordination between SAT and ANAM.

Technical Barriers to Trade

Adhering to National Treatment in MA Procedures (Pharmaceuticals): Proposed amendments to Mexico's marketing authorization procedures appear to undermine its national treatment obligations under the USMCA. Under the draft legislation, companies holding a sanitary license for a domestic manufacturing facility producing generic or biological medicines would be granted access to an expedited marketing authorization process. By limiting this streamlined pathway exclusively to manufacturers that meet these criteria, the proposal introduces a discriminatory measure that undermines the principle of national treatment enshrined in the USMCA; specifically, Annex 12-F.5, which governs the application of regulatory controls. The legislation was published in the Gaceta Parlamentaria on September 26, 2025. USTR should urge the Mexican government to ensure marketing authorizations, recognition letters, and regulatory controls are administered equitably and without discrimination based on origin, in line with national treatment obligations.

Delays in Regulatory Approval & Market Access (Pharmaceuticals): Under Mexican law, products approved by the FDA, should receive an expedited review by COFEPRIS within 90 days. COFEPRIS has been inconsistent in its use of this review pathway, resulting in long approval delays that prevent market access. These delays are inconsistent with Mexican law and USMCA (Annex 12-F).

Services Barriers

Mexico's "Kill-switch" and Article 30-B in the 2026 Economic Package: A proposal in Mexico's Economic Package would require digital service providers to grant the Tax Administration Service (the Servicio de Administración Tributaria or SAT) permanent, real-time online access to their systems and records related to operations in Mexico. Mexico's Senate passed the 2026 Economic Package in October, 2025, including Article 30B (kill switch), and the tax is set to take effect April 1, 2026, pending publication in Mexico's Official Gazette later this year.

Non-compliance could result in the temporary blocking of digital – widely referred to as the "kill-switch" - as outlined under the Value-Added Tax Law (LIVA). Additionally, the SAT would coordinate with the newly created National Agency for Digital Transformation and Telecommunications to manage the technological infrastructure and data analysis associated with this obligation. These authorities have stated that the intention of this proposal is to capture Chinese e-commerce companies, but the language is broad and captures all providers. Both the new provision and the existing "kill-switch" provision raise serious concerns regarding Mexico's USMCA commitments. These measures would create extreme risks for U.S. firms, threatening the security of user data, proprietary intellectual property, and trade secrets, while

placing companies in an impossible conflict with U.S. and global data privacy laws. USTR should seek assurances that the "kill switch" mechanism will not be activated, as its use would raise immediate USMCA compliance concerns.

Electronic Payment Services: In the historic U.S.-Mexico-Canada Agreement (USMCA)'s Chapter 17 (Annex 17-A), Mexico adopted new high-standard Financial Services commitments related to cross-border trade, including application of the national treatment and market access obligations for electronic payment services (EPS). Since the Agreement's entering into force, Mexico has failed to comply with these commitments, maintaining significant barriers for U.S. EPS suppliers that effectively prevent them from fully participating in Mexico's domestic payments market. Mexico should take all necessary steps to finalize, publish, and implement regulations that enable U.S. EPS suppliers to process domestic transactions using their own attributes to differentiate their value proposition and compete fairly, in accordance with USMCA's commitments as soon as possible, specifically the draft regulation on retail payment networks led by Comision Nacional Bancaria y Valores (CNBV) and the Central Bank (Banxico) and draft regulation on clearinghouses led by Banxico. The absence of effective competition is restricting U.S. commerce in the digital services sector, as U.S. EPS providers are unable to expand their operations in Mexico unless they adapt their services to rules established by local participants, including potential competitors. The existing regulatory framework in Mexico gives preferential treatment to domestic companies, establishing obstacles that hinder fair competition for new market entrants.

The Office of the United States Trade Representative (USTR) and the U.S. Department of the Treasury have repeatedly urged the Mexican Government to ensure that U.S. EPS suppliers can effectively compete in the Mexican market, in line with the commitments in the USMCA. For example, in the 2025 National Trade Estimate Report, USTR highlighted that the current regulatory framework in Mexico limits the ability of U.S. EPS suppliers to offer their full range of value-added services and differentiate themselves in the market. Therefore, the current regulations limit the availability of new services and innovations for financial institutions and their users. In 2023, the Mexican Economic Competition Authority (COFECE) confirmed the existence of barriers to competition and free market access in the card payments market in Mexico and recommended that Banxico and CNBV amend the regulations to eliminate these barriers and guarantee interoperability of card payment networks. Mexican Financial regulators have also acknowledged the need to modify the regulations in this regard.

Barriers for cloud in financial services: Mexico continues to enforce 2021 regulation which requires electronic payment fund institutions to maintain a business continuity plan in the case of disaster recovery that relies on either 1) a multi-cloud approach with at least two cloud service providers from two different jurisdictions, or 2) an on-premise data center in country that doesn't depend on the primary (foreign) cloud provider. The approvals process run by the National Banking and Securities Commission (CNBV) that is required for financial services companies to use cloud services is resource intensive and is discriminatory towards foreign cloud providers, whereas existing local on-premise data centers need to complete a shorter notification process. This de facto data localization requirement is in addition to an already complex and time-consuming process that electronic payment fund institutions face in order to gain regulatory approval to use offshore cloud infrastructure whereas in-country infrastructure enjoys a more expedited process. The United States has raised concerns with the Mexican government that the requirements relating to use of cloud service suppliers by electronic payment fund institutions have a negative competitive impact on the business of U.S. service suppliers.

Mexico 8% excise tax on violent video games: Mexico's 2026 Economic Package (budget) Article 2 - I-K, II-D from the IEPS Bill would, for the first time, impose an 8 percent tax under the Special Tax on Production and Services (IEPS) on video games determined to have violent content. Policymakers have signaled an intent to focus the measure on foreign-based game providers. The tax would cover both paid and free-to-play games, including those without microtransactions or other revenue streams, and would be

assessed on the game's value or, for subscription services, on 70% of the total subscription price in Mexico. The tax, as proposed, would, at a minimum, be *de facto* discriminatory against U.S. and Canadian gaming services, given the nature of the global games industry and the digital services obligations established at the USMCA.

Intermediary Liability: Mexico made reforms to its Federal Copyright Law in 2020 in an attempt to bring its law in compliance with commitments under USMCA. However, the provisions implementing Article 20.87-88 of the USMCA Intellectual Property Rights Chapter inappropriately narrows the application of this framework for internet services. Likewise, the provision implemented through the amendment of Article 232 Quinquies fr. II of the Copyright Law establishes administrative offenses fines when ISPs fail to remove, take down, eliminate, or disable access to content upon obtaining a notice from the right holder; or do not provide to a judicial or administrative authority information that identifies the alleged offender.

Services Barriers - Telecommunications

6 GHz Spectrum Restrictions and Telecommunications Policy: In contrast to U.S. actions to expand 6 GHz spectrum, Mexico has engaged in unfair trade practices by restricting the 6 GHz band allocation and dissolving the telecommunications regulatory agency in violation of the Telecommunications Chapter of the USMCA. Mexico has also worked to undermine U.S. leadership in promoting 6 GHz and cutting-edge telecommunications technologies, including 5G and Wi-Fi.

Since 2020, the United States has allocated the 6 GHz band (5925-7125 MHz) for unlicensed use, which includes the use for technologies such as Wi-Fi and Bluetooth. By making the entire 6 GHz band available, the United States has enabled Wi-Fi to support new applications such as high-definition video, artificial and virtual reality, and haptic technologies. Most of the countries in the Western Hemisphere have adopted the same spectrum model as the United States, including Canada, Colombia, Argentina, and Peru. Mexico, however, has only allocated the lower portion of the band– 5925-6425 MHz – for unlicensed use. Although it has held multiple proceedings examining the possible future use of the upper portion of the band, Mexico has deferred its consideration of the issue for the last two years. These delays have been exacerbated by the recent dissolution of Mexico's telecommunications regulatory agency, the Federal Telecommunications Institute ("IFT"). Since its dissolution last year, Mexico's telecommunications policymaking has been largely on hold, as these regulatory responsibilities were moved to the nascent Agency of Digital Transformation and Telecommunications Mexico's dissolution of the IFT is in direct violation of the USMCA that requires signatory countries to maintain an independent telecommunications regulatory agency.

More importantly, the prior and current Mexican administrations have sought to undermine U.S. positions on 6 GHz issues. For example, the use of the upper 6 GHz band in the Americas was not on the agenda at the World Radiocommunication Conference in late 2023 ("WRC-23"). Nevertheless, Mexico sought to initiate a regional study of the issue that would have undermined Wi-Fi operations in the band throughout the region, including the United States. Backed by a strong opposition from the Wi-Fi industry, the United States blocked Mexico's proposal. Unfortunately, this did not stop Mexico from joining with Brazil to add a footnote to the final WRC-23 resolutions that allocated the upper part of the band for International Mobile Telecommunications ("IMT," i.e., 5G) for their respective countries. Since then, Mexico has exploited the International Telecommunication Union ("ITU") process to create further uncertainty about the future of Wi-Fi in the upper 6 GHz band in the Americas. For example, Mexico has sponsored an effort at the Inter-American Telecommunication Commission ("CITEL") to gather Member Countries' input about present and planned use of the upper 6 GHz band via wireless technologies, including 5G and Wi-Fi. Mexico's intent behind this effort was to suggest that Wi-Fi is not the preferred

technology for the band. With Brazil, Mexico has also sought to delay the CITEL action on resolutions providing technical guidance about how unlicensed technologies, like Wi-Fi, would operate in the upper 6 GHz band. This effort seems intended to delay progress on establishing Wi-Fi in the band and create uncertainty that would discourage other countries from following the U.S. lead on 6 GHz policy.

Investment Barriers

Investment Climate: It is essential to provide certainty to investments through expedited authorization procedures, including approvals for acquisitions and mergers. The ongoing transition from the former Federal Economic Competition Commission (COFECE) to the National Antimonopoly Commission (CNA) may undermine confidence in the criteria that will be applied to cases currently under review. It could also delay their resolution. The new Competition Law shortened the timeframes for reviewing and resolving merger authorization requests, in part as a recognition by the legislature that lengthy procedures delay investment in the country. However, merger authorization requests filed prior to the reform will remain subject to the timelines set forth in the former legal framework. As of June 2025, COFECE reported having 31 mergers and acquisitions pending authorization.1 This situation creates uncertainty for investors, potentially affecting decision-making and long-term planning.

Government Procurement

Proposed Offset Requirements: In addition to numerous changes to government procurement rules for medicines in recent years, the Mexican government issued a decree in June 2025 linking public sector pharmaceutical purchases to domestic production and/or investment. The proposal was also included in the draft revision to the General Health Law published in the Gaceta Parlamentaria on September 26, 2025. This policy, commonly referred to as an offset or performance requirement, also introduced a points-and-percentages system for evaluating bids in public tenders. This is inconsistent with several of its international trade obligations related to procurement.

Telecommunications Procurement: Mexico made commitments related to government procurement to which it no longer adheres. Specifically, the Comisión Federal de Electricidad's ("CFE") Telecomunicaciones y Internet Para Todos program is not explicitly covered under CFE's listing. Although the Mexican Secretariat of Economy confirmed that the 'Telecomunicaciones y Internet Para Todos' program would be covered under Mexico's existing government procurement commitments, the Mexican government has not confirmed this commitment in writing to date. CFE's failure to list the program violates its USMCA obligations, and CFE's discriminatory treatment of U.S. suppliers violates its USMCA commitments, especially notices of intended procurement (Article 13.6), qualification of suppliers, (Article 13.8), technical specifications (Article 13.11), time periods (Article 13.13), and compliance commitment (Article 13.2). Moreover, CFE issues procurement notices that are designed in such a way that the only products that qualify are from Chinese suppliers. This unfair practice discriminates against U.S. suppliers.

Government Procurement / Cybersecurity: The Government of Mexico is updating its cloud services framework agreement for public procurement, and there are indications that Mexico will be lowering the cybersecurity standards required to provide cloud services to the Mexican government and other public sector entities. The Secretariat of Finance is currently undergoing a market study that started at the end of September and will conclude by the end of November. It is anticipated that key international certifications such as ISO 27017, ISO 22301, SOC 1, 2, and 3, Cloud Security Alliance (CSA) STAR Level 2, FedRAMP, and FIPS 140-2 Level 3 or higher will no longer be required. This development means that leading Chinese cloud providers that previously did not meet the requirements will now be able to provide cloud services to some of Mexico's most critical public sector workloads.

Intellectual Property Protection

Lack of implementing regulations and patent linkage (Pharmaceuticals): The Mexican Institute of Industrial Property (IMPI) has not yet issued the necessary regulations to implement key provisions of the Federal Law for the Protection of Industrial Property (LFPPI), such as patent linkage. Additionally, recent court precedents have undermined patent usage by preventing their publication in the linkage gazette. All of these issues are in direct violation of Mexico's IP commitments under the USMCA. As a result, COFEPRIS has issued numerous marketing authorizations for generic versions of patented protected products, occurring at least 10 times in 2023 and 2024 alone (PhRMA, 2025). This harms innovation and allows generics in China to take market share away from U.S. companies operating in Mexico.

Lifting injunctions without sufficient legal justification: The Mexican government, including IMPI, has adopted the practice of lifting injunctions against products that infringe industrial property rights under the justification of access to medicines and the right to health. Although the protection of public health is a constitutional principle, this practice affects legal certainty and the protection of industrial property rights. The right to health cannot be interpreted absolutely when it affects constitutionally protected industrial property rights – fundamental rights must be harmonized and are not mutually exclusive. Preliminary injunctions should be maintained valid and should not be lifted unless compelling evidence of lack of access and/or non-infringing evidence is filed by the defendant.

Other Barriers

Tax ID registration affecting US SMEs: In 2020, Mexico passed legislation requiring U.S. businesses that store inventory in Mexico to register for a local tax ID with the Tax Administration Service (SAT) and file monthly tax reports. While this process alone is not novel, the process to obtain this tax ID, known as a *Registro Federal de Contribuyentes* (RFC), is extremely complicated and costly. This process alone has become the primary barrier for U.S. small and medium-sized enterprises (SMEs) that seek to sell their products to Mexican consumers and businesses. To receive an RFC, U.S. businesses are required to have a local Mexican address and a local Mexican legal representative that shares 50% of the company's tax liability, as well as pay income tax on all income generated in Mexico. The registration process is slow and bureaucratic, and involves 1) apostilling of documentation in the U.S., 2) translating all documentation to Spanish by a certified translator, 3) legalizing documentation with a Mexican Notary, 4) obtaining a SAT appointment (which can take one to four months due to limited availability), and 5) registering the RFC in SAT's offices. All of these steps are offline and in-person and can take over five months, costing over $5,000, in addition to the costs of complying with income tax obligations.

Tax Audits: The broader investment climate for established U.S. multinationals is deteriorating due to a systemic and punitive tax audit regime. Over the past few years, the SAT and related agencies have increasingly targeted U.S. multinational companies with extensive tax audits and assessments. While tax disputes are expected, U.S. companies have been assessed unreasonable tax charges, often based on new audits of previously closed tax filings. The targeting of U.S. MNCs suggests that some of these tax assessments are not based on Mexican accounting rules but are rather an attempt to secure additional corporate tax revenue. SAT's own data reveals a 367% increase in revenue collected from transfer pricing audits of large multinationals in the 2019-2024 period, suggesting audits are in fact used as a *de facto* revenue-extraction tool rather than for routine compliance. Unfortunately, the ability to resolve these tax assessments is difficult given an opaque and costly appeals process. This aggressive posture now also targets U.S. manufacturing supply chains, with SAT announcing its intent to audit 100% of companies in the VAT Certification program, a program essential for IMMEX operations. The targeting of U.S. companies in such a discriminatory and arbitrary manner raises the costs of doing business and undermines the stability pledged under the USMCA.

Barriers to access energy: In March 2025, Mexico concluded the approval process of its comprehensive energy reform with the publication of secondary laws, following the constitutional reforms approved in October 2024. This reform package returned control of the energy sector to the State, giving prevalence to state-owned companies Mexican Petroleum (PEMEX) and the Federal Electricity Commission (CFE), while establishing new schemes for private sector participation under state supervision. These new regulatory changes continue to create hurdles for companies seeking to connect to the electricity grid and purchase clean and reliable energy. These hurdles now include the establishment of CFE's dominance, requiring it to maintain at least 54% of grid-injected energy annually, and the implementation of "binding planning" requirements that give preference to state-owned CFE in generation and marketing activities. The creation of a new centralized regulatory body (CNE) replacing independent regulators potentially reduces transparency and regulatory independence. Additionally, the reform restricts self-supply arrangements, eliminates partial permit migrations, adds new requirements for electricity storage systems, and implements stricter controls on grid interconnection. As a result, U.S. companies face significant challenges in adequately sourcing their energy needs in Mexico, compromising their clean energy targets and operational efficiency. While the United States has already requested dispute settlement consultations with Mexico under the USMCA, the 2025 reforms appear to further entrench state control over the electricity sector, exacerbating existing concerns.

Constitutional reforms on independent regulatory bodies: In July 2025, Mexico published comprehensive reforms that fundamentally restructured key regulatory bodies. The reforms eliminated the autonomy of antitrust regulators, the Federal Economic Competition Commission (COFECE) and the Federal Telecommunications Institute (IFT). COFECE was replaced by the National Antimonopoly Commission, now a decentralized public agency under the Secretariat of Economy, while IFT's functions were transferred to the new Telecommunications Regulatory Commission (CRT) under executive branch control. The reforms altered the regulatory telecommunications landscape by reducing commissioner numbers from seven to five, eliminating independent selection mechanisms, and transferring removal power from the Senate to the Executive. These changes, combined with the first judicial election in Mexico following the judicial reform approved in the previous administration, represent a fundamental shift toward centralized executive authority over key regulatory and judicial institutions. The election, held on June 1, involved selecting 881 federal positions and 1,800 state magistrates and judges through popular vote. Voter turnout was low (approximately 13%), and most winning candidates were publicly aligned with the ruling political coalition. The new judicial leadership took office on September 1, 2025. These reforms raise significant concerns about regulatory independence and institutional consistency, particularly regarding competition enforcement and telecommunications oversight.

Nepal

Services Barriers

Digital Services Taxes: Nepal passed legislation on May 29, 2022 to adopt a 2% DST on a special list of digital services provided by non-residents to consumers in Nepal. The DST took effect on July 17, 2022, without any public consultation on the law or the implementing procedures. The DST: (i) only applies to non-resident companies; (ii) is inconsistent with existing international tax principles; (iii) imposes an additional tax burden and potential double taxation on non-resident companies; and (iv) creates a disproportionate compliance burden as additional resources are required to comply with the DST's payment and reporting requirements.

Data Localization: In March 2024, the Ministry of Communication and Information Technology introduced the draft Information Technology and Cyber Security Bill 2080 to regulate activities related to

information technology and cyber security. As written, the Bill would require data centers and cloud service providers to obtain licenses subject to yearly renewal and would require health and financial organizations to store all data domestically. The USTR should continue to track the development of this legislation and its discriminatory impact on foreign data centers and cloud service providers.

Content Moderation: The Nepalese government has progressively introduced measures to increase control over online content, creating significant operational and human rights concerns. Starting in August 2023 with the National Cyber Security Policy , which proposed a centralized "National Internet Gateway" for filtering and monitoring traffic, the government has pursued greater regulatory power. This was followed by a November 2023 Social Media Directive requiring local platform registration, and escalated with the January 2025 introduction of a Social Media Act Bill, which grants authorities broad powers to remove content deemed "indecent" or "misleading" and imposes severe penalties . In 2025, Nepal temporarily blocked 26 unregistered social media platforms in September 2025. These actions, which critics argue threaten free expression and create barriers for foreign companies, underscore the uncertain and challenging regulatory environment in the country.

OTT Licensing: Nepal has enacted a series of regulations that impose significant local compliance burdens on foreign digital service providers. Starting in March 2022, under amendments to Nepal's National Broadcasting Rules 2052 , broadcast and video-on-demand OTT services were required to obtain local licenses and maintain local data servers. Subsequently, a draft framework from April 2023 proposed that communications OTT providers must also register a local office or appoint a local intermediary. This regulatory trend has continued with the E-Commerce Act of 2025, which establishes broad extraterritorial jurisdiction, forcing foreign digital platforms to register locally, comply with Nepali laws, and assume liability as intermediaries for third-party activities, thereby creating substantial regulatory and financial hurdles for international firms operating in the market.

New Zealand

Services Barriers

News Media-Related Digital Service Taxes: In August 2023, the New Zealand government introduced the "Fair Digital News Bargaining" Bill, modeled on similar laws in Australia and Canada, and designed to make large digital platforms like Google and Meta pay for hosting local news content. The Bill aimed to generate NZD 40-60 million annually for New Zealand's news businesses. New Zealand's version, as compared with the Australia and Canada counterparts, includes more specific parameters for designating digital platforms. However, it empowers news businesses to themselves apply to have a digital platform registered to be subjected to the mandatory bargaining code. This power undermines any incentive of platforms to negotiate deals to obtain exemptions, as any disgruntled news businesses could seek designation regardless of whether they have bargained in good faith with the digital services providers. While the New Zealand government has since put the bill on hold, deeming it "not ready", the U.S. government should continue to monitor and ensure that this discriminatory tax on U.S. platforms does not proceed.

Nigeria

Services Barriers

Data Localization: Under the Content Guidelines developed by Nigeria's National Information Technology Development Agency (NITDA) in 2019-20, all "sovereign data" is required to be stored within Nigerian territory. While the scope of "sovereign data" remains undefined, it is generally interpreted to include all government and public sector data. A Data Classification Framework is currently being developed to define the categories of data which must be locally hosted, and NITDA has committed to full local hosting for classified data by end-2026. Moreover, Nigeria's draft 2025 National Cloud Policy, due to replace the 2023 version, emphasizes data localization, requiring foreign cloud service providers to invest locally or partner with local service integrators to win business and participate in government procurement.

Levy on Foreign Digital Platforms: The 2021 Finance Act introduced a tax regime for non-resident companies providing digital services and products to persons in Nigeria, including both income and VAT taxes. The 2020 Finance Act first introduced income tax obligations for non-resident companies providing digital goods and services in Nigeria. While the law applies to all non-resident companies earning above a certain threshold, extensive media coverage and analysis by experts has repeatedly mentioned the targeting of US multinationals. The law specifically references non-resident companies with a "significant economic presence" (SEP) in the country which is defined by a number of factors including: a minimum amount of revenue generated from users in Nigeria, transmitting data about Nigerian users, or the availability of local websites or local payment options. Under Nigeria's SEP regime, non-resident digital services firms may be taxed on a deemed profit basis, often resulting in an effective 6% rate on turnover where SEP criteria are met. Additionally, a 1% levy on foreign digital platforms was proposed in 2023, but has not yet been enacted.

Content Moderation: In September 2022, the NITDA issued a Code of Practice for Interactive Computer Service Platforms and Internet Intermediaries. Under the Code, digital service platforms with more than one million users must incorporate and maintain a physical presence in Nigeria and appoint a liaison officer, obligations that may limit cross-border operations. The Code contains requirements that create risks for free expression, user privacy, and business operations. The Code's vague definitions of "unlawful content", coupled with aggressive 24-hour takedown mandates, could be used to suppress legitimate speech critical of the government. Furthermore, requirements for proactive content monitoring and "stay-down" obligations effectively erode crucial intermediary liability protections, forcing companies to act as censors. These issues are compounded by rules that allow the government to demand user data under broad pretexts like "public order" and impose burdensome operational requirements, such as mandating local incorporation, which collectively create a high-risk and uncertain regulatory environment for U.S. platforms.

Further, under Nigerian law, all advertising of any kind needed to be pre-approved by the Advertising Regulatory Council of Nigeria (ARCON), a problematic requirement for online platforms, which are disproportionately U.S. firms. In October 2022, ARCON fined Meta $70 million for allegedly running advertisements without prior vetting and filed a lawsuit, which it withdrew nearly three years later after little progress. ARCON has since issued similar, largely unenforceable fines to TikTok and Google.

FX Controls: In June 2023, the Central Bank of Nigeria (CBN) announced the removal of the exchange rate peg and the introduction of the "Willing Buyer, Willing Seller" model. Despite the liberalization of the foreign exchange market, CBN maintains stringent controls over the repatriation of funds, which are inconsistent with a willing buyer willing seller market. These controls include the requirement for CBN approval to purchase foreign exchange using funds in Non-Resident local currency accounts, despite such accounts being pre-approved by the CBN for the collection of local currency funds by foreign companies. The approval process for the repatriation of funds remains a significant barrier to investment by U.S. entities, as it is frequently subject to delays and denials. It is recommended that the CBN abolish the approval requirement for the repatriation of funds in Non-Resident accounts.

Norway

Services Barriers

Digital Sovereignty and Ownership Requirements: The Norwegian Government plans to create a national cloud solution for a broad range of critical entities, requiring public sector companies to store over 60% of data using this national service. The government is also applying pressure to extend this to sectors such as energy, telecoms and financial services. The national cloud solution can only be developed by Norwegian providers within Norwegian borders.

Oman

Services Barriers

Electronic Payment Services: The Central Bank of Oman (CBO) launched the domestic payment scheme ALMAL in September 2025 to reduce issuing and processing costs and promote financial inclusion, particularly for SMEs. We urge USTR to encourage a level playing field for U.S. companies. Oman is currently considered a high-risk market for a co-badge mandate, however, there have been no official mandate or circular in place detailing the rollout plan.

Panama

Services Barriers

Data Localization: Resolutions 52 and 03 of the Government Innovation Authority AIG (former Government, 2021 and 2024) order that any government entity that uses cloud services for critical mission or state security platforms or sensitive institutional data hosted on servers outside the Republic of Panama must make the necessary adjustments and change the location to the Republic of Panama before 31 December 2024. In order to continue to support the government in serving its citizens and businesses, these resolutions should be removed. In an increasingly globalised world, and one in which Panama seeks to become a regional hub, data localisation could inhibit open data flows and new innovations such as generative AI, and create cybersecurity risks.

Pakistan

Import Policies

New Seller Registration Obligation. The Finance Act 2025 requires non-resident online marketplaces to ensure only sales tax–registered sellers can operate on their platforms starting July 1, 2025, effectively making online platforms liable for blocking unregistered sellers. This specific platform liability is affecting multiple US firms and there are still gray areas on how cross-border sellers are treated, especially when goods transit via local logistics partners. The courier-based enforcement and lack of clarity in application remain important factors to monitor.

Services Barriers

Data Localization: Pakistan launched a Cloud First Policy in 2022. This policy imposes data localization requirements on wide and open-ended classes of data ("restricted", "sensitive", and "secret"). In the financial sector, the State Bank of Pakistan (SBP) prohibits financial sector institutions from storing and processing core workloads on offshore cloud. Pakistan has been considering a "Personal Data Protection

Bill". The bill has a broad scope, applying to both digital and non-digital operators, and includes extraterritorial applications. The bill empowers the federal government to restrict cross-border transfer of "certain personal data". It also conditions export of personal data on explicit consent by the data subject and non-conflict with Pakistan's public interest or national security. Such broad language, combined with the regulator's lack of independence from the federal government, raises the risk that the proposed law could be weaponized, with potential harms to civil liberties and industry. The bill also includes a sweeping mandate for defining "sensitive personal data" that explicitly includes financial data, which may have broad implications for online services. Additionally, the bill includes burdensome requirements for data processing as well as a grant of broad powers to the regulator, with few guardrails. The bill also proposes a National Commission for Personal Data Protection which has extensive powers to introduce new regulatory frameworks and access data. In addition, several sectoral regulators have imposed restrictions on cross-border data flows for regulated entities: the Pakistan Telecommunication Authority (PTA) requires its licensees to obtain prior approval before transferring any data outside Pakistan; the Securities and Exchange Commission of Pakistan (SECP) prohibits licensed digital lenders from storing data on cloud infrastructure located abroad; and the SBP similarly requires licensed exchange companies to maintain both their primary and secondary data centers within Pakistan and permits outsourcing only to local cloud service providers. These data localization requirements are ineffective at enhancing data protection, and significantly increase costs for U.S. firms, potentially deterring market entry.

Digital Taxation: In 2025, Pakistan introduced a digital services tax applicable to the sale of goods and services by offshore platforms with a "significant digital presence" (SDP) in Pakistan. However, before the tax came into force, the Federal Board of Revenue (FBR) issued a blanket exemption on its implementation, leaving uncertainty about its future application. Despite this exemption, Pakistan continues to maintain several overlapping taxation measures on digital products and services. Provincial service tax laws extend their reach to companies without a physical place of business in Pakistan, effectively taxing offshore entities providing services into the country. At the federal level, income tax laws are also applied extraterritorially to offshore companies. In 2023, the definition of "permanent establishment" (PE) was also broadened to cover entities with no physical presence in Pakistan but a virtual business presence, including where transactions are carried out through the internet or other electronic means. While the U.S.-Pakistan Income Tax Convention should protect U.S.-located operations from the imposition of the "virtual PE" and the SDP measure, companies face challenges in practice due to inconsistent application of the bilateral tax treaty in Pakistan. The U.S. government should encourage Pakistan to withdraw both expanded definitions.

Content Moderation: Pakistan's *Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules 2021* grants the government power to order online service providers to remove content deemed harmful to "Islam", "security", "public order", "decency", and "integrity". Providers face 48-hour (12-hour in emergencies) compliance deadlines, or risk service degradation, blocking, or fines up to PKR 500 million ($1.76 million). Additional requirements include: mandatory local offices if required by the PTA; registration by the entity providing the service within three months; appointment of a local "compliance officer" and a local "grievance officer" (the grievance officer would be required to redress complaints from the public within 7 working days of receipt); intrusive content moderation and monitoring; and providing user data in a decryptable and readable format to investigative authorities in accordance with existing federal law. These rules greatly jeopardize the ability of U.S. firms to operate in Pakistan and undermine freedom of expression in what is a sizable market.

In 2025, Pakistan amended its Prevention of Electronic Crimes Act, creating the Social Media Protection and Regulatory Authority (SMPRA). The SMPRA has broad powers, including over platform registration, fines, and content removal. These amendments have significantly expanded the categories of content subject to takedown, covering material that SMPRA deems contrary to the "ideology of Pakistan", that it has "reason to believe" is false, or that contains aspersions against any person, including

public officials. Government-imposed internet shutdowns during protests and elections have led to substantial economic losses and human rights violations. Industry reports indicate these shutdowns cause uncertainty and encourage investment flight. Recent shutdowns have cost Pakistan an estimated $892 million to $1.6 billion. A new internet firewall implemented in August 2024 has already cost the economy $300 million and is expected to cause further harm.These content moderation measures, including broad takedown requirements and data disclosure obligations, would severely hinder the ability of U.S. firms to operate in Pakistan and undermine freedom of expression within a significant market.

Internet Services: In October 2021, Pakistan issued the Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards), Rules 2021" (Rules) which superseded the 2020 version of the Rules. The Rules apply to the removal and/or blocking of online content that is deemed unlawful on any "information system". Local and international industry players have expressed concerns regarding provisions that would pose significant barriers to operating in Pakistan, including requirements to deploy mechanisms to monitor and block livestreaming content, remove content within short timeframes when ordered by the authorities, and provide data to authorities in decrypted and readable format.

Electronic Payment Systems: The State Bank of Pakistan (SBP) is pushing to have its domestic payment system, 1LINK, process domestic transactions despite no regulatory mandate or circular in place. The SBP is driving this through an Industry-Led Steering Committee, which comprises issuing banks, 1LINK, fintech, and the Pakistan Banks Association. This is a marked change from when the SBP was previously allowing banks to choose their payment network rather than be pushed to use one domestic network only. This represents a trade barrier to processing domestic transactions in Pakistan for international payment networks.

Peru

Import Policies

Trade Facilitation: Under Article 5.7(g) of the U.S.-Peru Trade Promotion Agreement (the "Agreement"), the parties established a de minimis, the value threshold below which no customs duties or taxes are charged on imported goods. The Agreement's de minimis threshold is set at $200. However, the Peruvian government has implemented limitations to the number of shipments (three maximum) under the express delivery shipments that an individual without tax number (RUC) can do per year. Also, for individuals, it is uncertain if above the three shipments these personal imports would be considered commercial and create new income tax obligations. Thus, this RUC requirement limits the ability for individuals to import goods for personal use, which constitutes a trade barrier and a limitation to the use of express delivery shipments in Peru.

Services Barriers

Data Localization: In January 2020, Peru's Digital Trust Framework (Decree 007) raised significant industry concerns by giving preferential treatment to domestic data storage and service providers. The decree introduced potential trade barriers, including the creation of a whitelist for cross-border data transfers (even though the Peruvian Data Protection Law does not include such restrictions), the establishment of mandatory domestic cybersecurity certifications for private companies, and the creation of a national data center for hosting data provided by public sector entities. While an April 2025 draft regulation has addressed some concerns, making cybersecurity certifications voluntary for the private sector and limiting other measures to critical industries, significant issues persist. The draft fails to clearly define key terms like "internet intermediaries", creating legal uncertainty and potential enforcement risks, for a wide range of US digital service providers, who could be inadvertently captured by obligations not

intended for them. Critically, it has not clarified the original decree's provisions on cross-border data flows or data localization mandates, leaving businesses facing continued regulatory uncertainty in Peru.

Content Moderation: In 2025, the Peruvian Congress began debating Bill 10880, which seeks to establish a regulatory framework for the protection of children and adolescents in the digital environment. A key concern for U.S. industry is a provision in the Bill which would raise the digital age of consent for personal data processing from 14 to 16, potentially requiring burdensome age verification and parental consent for more teenagers. While the bill references using "reasonable efforts" and "available technology" for age verification, the higher age of consent itself represents a significant shift in the data protection landscape and could create new compliance burdens for a wide range of online services, from social media and gaming to educational platforms.

Intermediary Liability: Peru remains out of compliance with key provisions under the U.S.-Peru Trade Promotion Agreement (PTPA). Article 16.11, para. 29 of the PTPA requires certain protections for online intermediaries against copyright infringement claims arising out of user activities. USTR cited this discrepancy in its inclusion of Peru in the 2018 Special 301 Report, and we support its inclusion in the 2026 NTE report.

The Philippines

Import Policies

Pre-Border Technical Verification and E-invoice Submission: Background: Issued in late May 2024, Administrative Order No. 23-2024 implements pre-border technical verification and cross-border electronic invoicing for commodities bound for export to the Philippines. As defined in the AO, pre-border technical verification involves the testing and inspection of commodities by accredited Testing, Inspection, and Certification (TIC) companies prior to export. Cross-border electronic invoicing requires registered foreign exporters to create export invoices on a single electronic platform managed by the Philippine government.

Technical Barriers to Trade

Internet Transactions Act of 2023. The Philippines' E-Commerce Bureau (ECB) of the Department of Trade and Industry (DTI) distributed communications to online marketplaces regarding their obligations under Republic Act No. 11967, also known as the Internet Transactions Act of 2023 (ITA). The transitory period for compliance of ITA ended on June 20, 2025. Specific obligations include requiring online merchants to submit necessary information, maintaining updated lists of merchants, prohibiting the sale of regulated goods without permits, providing effective consumer redress mechanisms, and clearly indicating merchant information in product listings. The DTI emphasizes that failure to comply may result in penalties.

Inconsistent Incentive Regimes: Various laws in the Philippines impose inconsistent and burdensome regulatory requirements on businesses operating in its Special Economic Zones. Specifically, the Business Process Outsourcing (BPO) and related services industries are often subjected to the same obligations as export manufacturing firms, ignoring the fundamental operational differences between them. This regulatory mismatch, coupled with outdated and uncompetitive incentive packages, creates regulatory risk and uncertainty for foreign investors, making the Philippines a less attractive investment destination compared to other outsourcing locations.

Services Barriers

Data localization: The Philippines is experiencing increased pressure for data localization, driven by several key developments. The recent appointment of a new Department of Information and Communications Technology (DICT) Secretary, who previously campaigned for data localization during his tenure on the President's Private Sector Advisory Council (PSAC), has intensified this push. Additional factors include the end of the telecommunications duopoly, which has forced providers to seek new revenue streams, and investments in data centers by local conglomerates. Recent regulatory developments, from the passage of the Open Access Act to the publication of its subsequent Implementing Rules and Regulations (IRR), and draft Executive Order (EO) have suggested that there is significant momentum building for formal data localization requirements in the Philippines

The primary beneficiaries of this initiative would be local conglomerates, local telecommunications companies, and Chinese Cloud Service Providers (CSPs). Currently, Huawei operates three Availability Zones (AZ) in the Philippines, while AliCloud will open its second AZ in October 2025. Proponents argue that data localization will stimulate investment in Philippines-based data centers and the country's digital economy. They claim that data localization is essential to boost the country's national security, and cybersecurity posture. The proposal faces strong opposition, particularly from the influential Business Process Outsourcing (BPO) industry. The Joint Foreign Chambers of Commerce, including the American Chamber of Commerce and US-ASEAN Business Council, have formally expressed their opposition through position papers.

Recent legislative developments have accelerated the data localization drive. Proponents succeeded in inserting a last-minute provision into the Open Access in Data Transmission Act (2025), empowering the DICT to "formulate policies to safeguard local data, when necessary to advance national security and public interest**"**. Informal copies of a new draft "data sovereignty" bill and a draft presidential "Executive Order (EO)" were circulated to the business community, but their authenticity could not be verified. The "EO" would require data localization in multiple sectors, including FSI, healthcare, subscriber information, national security data, and sensitive personal information. Additionally, it would exclude US CSPs from three of the four tiers of public sector data - the draft EO mandates that only "Non-Sensitive Government Data" can be stored in off-shore infrastructure. The EO has yet to be published by the Office of the President. Such legislation/regulations would severely limit the services that US CSPs could provide to Philippines private and public sector customers and also impose onerous new compliance requirements on US CSPs.

Additionally, foreign providers are subjected to a mandated licensing process administered by the Securities and Exchange Commission (SEC) in the country as a condition for providing cloud services to the public sector. Without an SEC license, entities seeking public sector procurement are forced to work with domestic entities, reflecting a *de facto* localization obligation.

The Konektadong Pinoy Act aims to remove the outdated legislative franchise requirement for certain segments of the data transmission infrastructure (middle and last mile). This liberalization is a substantial step toward lowering entry barriers and increasing competition, creating significant market opportunity for U.S. digital services and technology providers. However, this positive market opening is jeopardized by several provisions, particularly Section 6(j), which grants broad authority to the DICT to "formulate policies to safeguard local data, when necessary to advance national security and public interest." The forthcoming Implementing Rules and Regulations (IRR) currently being drafted could introduce discriminatory requirements, including mandatory data localization or overly broad national security vetting of foreign entities, thereby creating an asymmetric regulatory environment that unfairly disadvantages U.S. digital services providers and undermines the Act's intended liberalization.

Services Barriers - Telecommunications

Telecommunications: Under the amended Public Services Act (PSA) which took effect in April 2022, public services engaged in the provision of telecommunications services are considered critical infrastructure. Foreign nationals may only own more than 50 percent of public services engaged in the operation and management of critical infrastructure, subject to reciprocity requirements i.e. if the country of the foreign national allows reciprocal rights to Filipinos, as defined by foreign law, treaty, or international agreement. Reciprocity may be satisfied by according rights of similar value in other economic sectors.

The Philippines allocates and manages spectrum through the Radio Control Law of 1931 (RA 3846 and its amendment, RA 584), Executive Order No. 546 1979, and the Public Telecommunications Policy Act of 1995 (RA 7925). These laws and directives provide the country's legal framework for spectrum enfranchisement, operation, and permitting in line with International Telecommunication Union requirements, and general provisions on the allocation and assignment of radio spectrum. While RA 7925 requires the conduct of open tenders in allocating spectrum, no public bidding has ever been carried out to allocate spectrum (e.g., spectrum auctions). Evaluation of applications typically involves submission by an applicant of a letter of request to the National Telecommunications Commission for its spectrum needs. This model is inherently non-transparent, constituting an administrative approach by which applicants are chosen based on the government's prioritization of certain criteria (like financial or technical capacity).

Government Procurement

Government Procurement: The government procurement system in the Philippines generally favors Philippine nationals or Filipino controlled enterprises for procurement contracts. Republic Act No. 9184 or the Government Procurement Reform Act, specifies a minimum Filipino ownership requirement of at least 60 percent in the procurement of goods, consulting services, and infrastructure projects. Domestic goods are also given preferential treatment over imported products in the bid evaluation process. The New Government Procurement Act (NGPA), which was signed into law on July 20, 2024, looks to enhance the existing procurement systems implemented by the 21-year-old Republic Act (RA) No. 9184. The new law states that preference and priority are given to Philippine products. As per Section 79, "The procuring Entity shall award the domestic bidder if the bid is not more than twenty-five (25%) in excess of the lowest foreign bid. The margin of preference provided herein shall be subject to a periodic review and adjustment by the GPPB, as may be necessary." However, the domestic preference can be waived if specific conditions are met, such as if the priority and preference will result in inconsistencies with obligations under international agreements.

While U.S. cloud service providers are active in the Philippine market, they continue to face constraints that limit their participation, particularly in competing for government projects. The Philippines requires government agencies to procure cloud computing services from the Government Cloud (also known as GovCloud), a cloud infrastructure set up by the Department of Information and Communications Technology.In 2024, CSPs were invited to participate in a new government procurement catalogue (eMarketplace of the Modernized Philippine Government Electronic Procurement System) run by the Procurement Service of the Department of Budget and Management (PS-DBM). This will include cloud as Common-Use Supplies and Equipment (CSE). The launch of cloud services in eMarketplace is expected to go live before end-2025. As part of the onboarding process U.S. CSPs are required to furnish a Certificate of Reciprocity confirming that Philippine companies may compete, with limited exceptions, on an equal basis with U.S. suppliers in U.S. government procurement. The Philippines is not a Party to the WTO Agreement on Government Procurement, but has been an observer to the WTO Committee on Government Procurement since June 2019.

South Africa

Services Barriers

Data Localization: South Africa's National Data and Cloud Computing Policy, published in May 2024 by the Department of Communications and Digital Technologies (DCDT), contains data sovereignty provisions. The Policy states that "data that incorporates content pertaining to the protection and preservation of national security and sovereignty of the Republic shall be stored only in digital infrastructure located within the borders of the Republic." The scope of covered data remains unclear.

Additionally, the Public Procurement Act was signed into law in 2024, but has yet to be brought into effect. Implementing regulations are being drafted, which will bring the new framework into effect. Currently, the procurement regime is not streamlined and is largely hardware-driven, without nuanced and context specific procurement frameworks for other industries including cloud. RFPs are issued with limited participation to specific vendors, which is an issue that is currently being investigated by the South African Competition Commission.

News Media-Related Digital Service Taxes: The South African government is advancing new regulations to force revenue transfer from online platforms through two key initiatives. A draft White Paper on Audio and Audiovisual Media Services proposes introducing a licensing fee for platforms and considering local content quotas. Separately, a February 2025 provisional report from the South Africa Competition Commission on its Media and Digital Platforms Market Inquiry recommends more drastic measures, including a 1% copyright levy, mandatory payments to publishers for news links, and a 5-10% digital advertising levy. Overall, the report significantly distorts the business model of online news and the role digital services play in the online information ecosystem. Given the focus of the report and in anticipation of the release of the finalized proposed remedies, industry remains concerned and urges the U.S. government to continue to push back on the report and future action.

Online VAT: South Africa currently levies a 15% VAT on the online selling of content, including films and television programming. As of 2019, income on services provided to South African businesses by foreign businesses is also subject to VAT.

Electronic Payment Systems: Foreign payment system operators were required to localize domestic processing infrastructure to comply with the amendments of the Payment Association of South Africa (PASA) Payment Clearing House (PCH) System Operator Criteria (focusing on domestic processing) effective from August 1, 2025. The policy requires that, for domestic transactions, payment service operators must authorize, clear and settle transactions through infrastructure that is established and maintained in South Africa. In 2025 the South African Reserve Bank (SARB) announced its intention to establish a domestic scheme. This will impact international schemes, who have made significant investments in localizing infrastructure, and NFTC urges USTR to work to assure a level playing field for U.S. companies.

Switzerland

Services Barriers

Surveillance Law: In January 2025, the Swiss Federal Council opened a consultation on a partial revision of the Telecommunications Surveillance Ordinances (VÜPF), aiming to clarify cooperation duties for telecommunications and communications service providers, and to adapt regulations to

technological developments. The revision seeks to introduce a three-tier obligation system for "derived communications service providers" (including cloud providers) based on user volume (starting at 5,000 users) and revenue thresholds (CHF 100M+ for full obligations), and requires expanded data retention, user identification capabilities, and technical surveillance interfaces that undermine encryption protections**.** The proposal has faced overwhelming rejection in public consultation from all major political parties and industry associations, with prominent Swiss startups threatening to exit due to privacy concerns and disproportionate compliance burdens. For U.S. cloud providers, the proposed revision could significantly impact Swiss operations, potentially requiring substantial compliance infrastructure, expanded data retention capabilities and weakened encryption.

Qatar

Import Policies

VAT: The planned introduction of a 5% VAT may increase operational costs for U.S. exporters. Additionally, logistical challenges still affect supply chain efficiency.

Intellectual Property Protection

Patent Term Extensions & Data Exclusivity Protections: While Qatar has made good progress in IP protection, There is no provision for patent term extensions, and data exclusivity protections are limited. Enforcement mechanisms are underdeveloped, and judicial processes can be slow and opaque.

Services Barriers

Electronic Payment Services: The Qatar Central Bank (QCB) is expanding its domestic payment scheme, Himyan, and has approached U.S. payment networks to explore co-badging options. We urge USTR to encourage a level playing field for U.S. companies.

Russia

Government Procurement

Localization Barriers & Procurement Restrictions: In late 2024, the government introduced new rules requiring localized production of API in order to be eligible for government tenders and pricing advantages. For example, local manufacturers offering to supply medicines from Essential Drug List (EDL) containing locally produced substances would receive a 15% price advantage in state procurement auctions. Additionally, these new rules do not create regulatory standards for "defining" locally produced API creating significant space for unscrupulous actors to disadvantage American firms. The effective date of the SDL rule has been postponed, as further details are still under development; the definition of 'locally produced API' remains one of the most critical elements

Intellectual Property Protection

Inadequate IP Protection: Manufacturers of original, patent-protected pharmaceuticals are increasingly facing challenges due to the inability to effectively prevent IP violation, as unscrupulous market participants are introducing generics and biosimilars prior to patent expiry. Technically, there are no regulatory barriers preventing the launch of generic versions of patented products. The responsibility rests solely with the seller or producer, while government oversight remains minimal. This enables the registration of such products, approval of pricing, and participation in state procurement programs. As a result, the number of legal disputes is rising. However, courts frequently deny preliminary injunctions, forcing patent holders into protracted litigation, often lasting several years. During this time, infringing

parties continue to profit from unauthorized commercialization, causing substantial financial losses to the rightful patent owners.

Saudi Arabia

Services Barriers

Data Localization: Saudi Arabia has implemented several data localization requirements through its key regulatory bodies.

- The Saudi National Cybersecurity Authority (NCA) has implemented data localization requirements under the 2018 Essential Cybersecurity Controls and 2020 Cloud Cybersecurity Controls. These requirements apply to government- and state-owned enterprises, as well as Critical National Infrastructure (CNI) and a broad range of other organizations, from financial services and aviation to oil and gas, and require these organizations' data hosting and storage to take place within Saudi Arabia.
- There are also additional localization requirements in the Cloud Cybersecurity Controls issued by the NCA in 2020. These Controls require CSPs to provide certain services from within Saudi Arabia, including systems used for storage processing, disaster recovery centers, and systems used for monitoring and support.
- The Communications, Space, and Technology Commission (CST) issued the Cloud Computing Regulatory Framework, which could restrict market access for foreign services by imposing data localization, increasing ISP liability, and mandating compliance with local cybersecurity and law enforcement access rules, including the installation of government filtering software.
- Saudi Arabia's Data Protection Law (DPL), which came into effect in 2023, introduced onerous registration and recording requirements, in addition to tight restrictions on cross-border data transfer outside of Saudi Arabia, and punishments for certain violations rising to SAR5,000,000 (US$1.33 million). The Saudi Authority for Data and Artificial Intelligence (SDAIA) and the NCA are working to issue a data localization and processing mandate that would include financial services. These proposals by the SDAIA for a national register of all data controllers and a new Data Sovereignty Public Policy, which has raised industry concerns about potential protectionism and stricter data localization. SDAIA has also drafted rules for the secondary use of public interest data and controls for data protection service providers. However, there are significant gaps and ambiguities in these proposals, such as unclear rules for commercial innovation, intellectual property, and vague definitions that could create additional compliance burdens for businesses operating in the country.

Artificial Intelligence: Saudi Arabia has thus far adopted a generally "light-touch" AI regulatory approach, favoring guidelines over specific laws. A key exception is the draft Global AI Hub Law, which aims to create sovereign data zones to promote international data flow, but the effectiveness of which is limited by a lack of clarity on security standards, legal conflict resolution, and government intervention rules – resulting industry uncertainty in the ability to enhance cross-border management and R&D capabilities. Industry seeks clearer safeguards, predictable data transfer pathways, and alignment with international frameworks.

Digital Platform Regulation: In July 2022, the Communications, Space, and Technology Commission (CST) (formerly the Communications and Information Technology Council of Saudi Arabia (CITC)), published its draft Competition Regulations for Digital Content Platforms with the goal of regulating large online digital services platforms. The draft regulations include concerning provisions like: arbitrary thresholds for designating platforms; vague definitions of prohibited conduct, such as "inappropriately and anti-competitively" favoring their own services; and attempts to bring untested regulatory proposals

from elsewhere in the world to the Saudi market without proof that such regulations work or that such regulations are even needed in the Saudi market. The draft regulations have not yet been adopted, but given their potential to hinder the ability of U.S. firms to operate and innovate in markets such as Saudi Arabia, industry urges USTR to monitor developments in the country closely.

Content Moderation: The regulatory environment is becoming increasingly stringent for content creators and platforms alike, and point to a heightened level of content moderation oversight and responsibility placed on digital platforms and users within Saudi Arabia:

- The SDAIA issued Deepfake Guidelines in September 2024, requiring platforms to disable and prevent the spread of misleading deepfake content, even if user-generated, with potential penalties for non-compliance and an emphasis on proactive detection.
- An amendment to the Telecommunications and Information Technology Act, proposed by the Ministry of Communications and Information Technology (MCIT) in July 2024, could force social media companies to implement internet filtering and prohibit circumvention, with severe penalties including significant fines of up to SAR25 million (US$6.6 million), service suspension, and license revocation for non-compliance.
- In September 2023, the General Authority of Media Regulation (GMedia) proposed a new Media Law. It would impose obligations on media outlets, defined to include social media platforms and individual users, to obtain licenses prior to engaging in "media activity," while reserving the authority to determine if content requires prior approval before publication.The proposed comprehensive Media Law was intended to be a landmark piece of legislation, replacing the existing Audiovisual Media Law and the Law of Printed Materials and Publication. The goal was to create a unified and modern legal framework to govern all forms of media, including traditional press, publications, radio, television, and digital media. The public consultation for this proposed law, concluded on December 5, 2023, after gathering feedback from stakeholders. However, the definitive status of the proposed law has yet to be officially announced, and developments in 2024 and 2025 have seen the GMedia shift its focus towards issuing more targeted regulatory updates, suggesting a potential strategic shift from a single, all-encompassing law to a more agile and incremental approach to media regulation. These include GMedia guidelines for creators issued in September 2025 detailing the types of language and visual content that is prohibited on social media platforms, with individuals and businesses facing direct responsibility for their posts.

Government Procurement

Forced Localization Policy (EPP): Foreign companies are required to provide offsets in order to sell to the government. In November 2022, the LCGPA released, without public consultation or private sector input, the Economic Participation Policy (EPP) mandating that foreign companies locally invest 35 percent of the value (based on certain multipliers) of any government tender filled with more than 100 million Saudi Riyal of imported products. In addition, in February 2021, the Ministry of Investment announced that multinational companies must establish their Regional Headquarters in Saudi Arabia to be eligible to participate in government tenders. This requirement was endorsed by a royal decree in December 2022. As a result, U.S. pharmaceutical companies do not receive reciprocal access to the Saudi market.

Other Procurement Challenges: Frequent renegotiation of tenders, combined with the lack of clear timelines, have resulted in an unpredictable government procurement system. The creation of the Local Content and Government Procurement Authority (LCGPA) to identify lists of products that must be procured from local manufacturers, combined with up to 30 percent price preferences for medicines made

with locally manufactured active pharmaceutical ingredients (API), serve to discriminate against foreign manufacturers and increase uncertainty in the Saudi market.

Intellectual Property Protection

IP Challenges: The Kingdom does not have a notification system for innovator companies and the current system of reliance on third-party agents does not have sufficient oversight and does not prevent patent violations. Additionally, the SFDA and SAIP introduced the "Approach of Dealing with Patents when registering generic drugs" in January 2023 – which includes a major verification loophole as a free-to-operate (FTO) document is enough to register generics. The Kingdom should add an additional step to this approach that guarantees verification of FTO, while also implementing a more robust IP mechanism (similar to FDA's Orange Book) that includes a notification system, quality control measures, elimination of conflict of interest, and a reliable dispute resolution system.

Taiwan

Services Barriers

Restrictive Use of Public Cloud for Generative AI: Taiwan's National Science and Technology Council (NSTC) has issued an administrative ruling restricting government agencies from using public cloud-based generative AI services. While intended to protect sensitive information, the ruling creates significant market access barriers for global cloud service providers (CSPs) and their AI offerings.

The ruling's core requirement mandates on-premises deployment for the use of generative AI by government agencies, explicitly prohibiting public cloud-based AI services for government data processing. This creates a de facto data localization requirement and restricts the use of public cloud through technical specifications. Such requirements contradict global best practices where hybrid and public cloud solutions often provide superior offering of generative AI and security measures.

While the ruling aims to ensure data sovereignty and control, it imposes restrictive requirements including mandatory on-premises deployment, physical system isolation, and local data control. These create substantial barriers through increased infrastructure costs, reduced access to advanced AI technologies, and limited scalability. The requirements effectively prevent government agencies from leveraging global AI innovations and cloud-based solutions that could enhance public services.

These restrictions raise concerns regarding Taiwan's international trade commitments and digital transformation objectives. They potentially violate WTO Technical Barriers to Trade (TBT) Agreement principles and create inconsistencies with Taiwan's open government procurement commitments. **NFTC encourages USTR to recommend revising the ruling to align with international best practices while maintaining secure use of generative AI.**

Intermediary Liability: Taiwan's approach to intermediary liability is creating a significant trade barrier by systematically eroding safe harbor protections, a practice that deviates from established democratic norms. Rather than implementing a clear and predictable legal framework, the government is pursuing a sectoral approach that imposes "strict liability" on platforms for user-generated content. This trend forces digital services to pre-screen and censor content, creating an untenable operating environment and undermining free expression. The enforcement of the Tobacco Hazard Prevention Act is a stark example of this flawed liability model. While the government aims to regulate illicit sponsored user content, the Act's critical flaw is its failure to assign liability to the content creator—the party actually engaged in advertising. Instead, it improperly holds the intermediary platform legally responsible, defining sponsored posts as commercial "advertisements" and mandating that platforms pre-screen all user content against an

ever-expanding list of keywords. This results in severe, repeated fines for platforms over content they did not create.

This pattern of governance ignores the fundamental distinction between paid advertising and user-generated content, compelling platforms to build extensive, preventative censorship systems. This not only constitutes a significant non-tariff barrier to trade but also normalizes speech-filtering mechanisms inconsistent with a free and open internet, undermines the free flow of information online which, in some instances, is essential to U.S. business interests (including for training AI models), and hinders the development of a vibrant digital public sphere. We urge the U.S. government to press Taiwan to adopt a coherent intermediary liability framework with clear safe harbor provisions that correctly assign liability to the originator of illegal content, not the intermediary.

Data Localization: A recent initiative by Taiwan's Personal Data Protection Committee Preparatory Office to develop a unique, domestic set of Standard Contractual Clauses (SCCs) for cross-border data transfers represents a significant concern for U.S. and other foreign investors. This plan risks creating a bespoke data transfer mechanism that is incompatible with established international standards, thereby generating pervasive legal uncertainty and substantial compliance burdens. A fragmented Taiwanese SCC framework will not facilitate secure data flows; instead, it would fragment the digital economy, compelling multinational companies that rely on globally integrated systems to adopt costly and duplicative contractual arrangements. ITI urges the U.S. government to encourage Taiwan to adopt flexible cross-border data transfer mechanisms. Prescriptive SCCs or templates should not be a pre-requisite for cross-border transfers so long as the parties have contractual arrangements or overarching policies in place that contractually obligate the transferee to adhere to a standard of protection comparable to the transferor's home country's standard. Adopting a flexible, risk-based approach will allow data controllers to operate in a safe, efficient, and internationally interoperable manner across jurisdictions, supporting U.S. investment and sustainable digital trade.

News Media-Related Digital Services Taxes: Legislators in Taiwan have introduced proposals to the Legislative Yuan to initiate a mandatory news bargaining code, with the legislative process advancing without industry or public consultation. The opposition parties have designated the bill as a priority, creating a significant risk of enactment of a law imposing mandatory revenue transfers from digital services providers to local news businesses. This legislative push ignores substantial, proactive digital investments and voluntary support from platforms to help foster a sustainable news ecosystem in Taiwan, including multi-year co-prosperity funds and ongoing digital skills training designed to support the transformation of local news organizations. Industry remains concerned that the proposed law would constitute a discriminatory trade barrier and urges the U.S. government to continue to oppose its enactment.

Services Barriers - Telecommunications

National Communications Commission: Since 2021, Taiwan's National Communications Commission ("NCC") has mandated firewalls, switches, and routers deployed in critical telecommunications infrastructure to undergo re-certification at two designated laboratories located in Taiwan, regardless of any existing certifications from foreign laboratories (*e.g.*, U.S.-based laboratories that are already recognized by the Taiwan government). The local testing in the two designated testing facilities – one of which is affiliated with the Ministry of Digital Affairs ("MODA") and the other a private laboratory named "Onward Security" – are mandatory under MODA regulations. Furthermore, each firmware update requires additional re-certification in both Taiwanese laboratories.

Taiwan's Bureau of Standards, Metrology and Inspection (BSMI) regulates safety, health, and

environmental standards for imported products. Under its recent draft regulation on "Relevant Inspection Regulations for Information Products, Audiovisual Equipment, and Ten Other Categories of Goods Subject to Mandatory Inspection", BSMI has proposed new requirements that would require U.S. companies to re-certify products and rely on local laboratories for cybersecurity testing. These duplicative rules would significantly increase compliance costs, delay time-to-market, and create unnecessary barriers for U.S. exporters.

Such dual certification requirements, coupled with the mandatory re-testing of firmware updates, creates significant trade barriers by requiring redundant and unnecessary testing. U.S. companies already invest heavily to meet internationally recognized standards, and BSMI should accept certifications from accredited global testing laboratories instead of mandating re-testing in Taiwan. Unless addressed, these measures risk discouraging investment and limiting the competitiveness of U.S. technology products in Taiwan's market.

Thailand

Technical Barriers to Trade

Pricing: National Drug Committee sets price ceilings for essential drugs, limiting pricing flexibility. Price negotiation required for public reimbursement listing, especially via the National List of Essential Medicines (NLEM). Private pricing remains largely unregulated, but under public scrutiny and consumer protection lens (e.g., Consumer Protection Board).

Government Procurement

Maximum Procurement Price: Thailand's Ministry of Public Health and the National Drug System Development Committee oversee the Maximum Procurement Price (MPP) system for pharmaceuticals. While intended to control public spending, the MPP process lacks transparency and predictability, especially when combined with preferential treatment for domestic suppliers. This has created barriers for foreign companies and delayed patient access to innovative medicines: only 21% of new global medicines since 2014 have launched in Thailand, with an average delay of 36 months.

The 2017 Public Procurement Act introduced a Reference Price Subcommittee to standardize pricing, but its implementation remains slow. **NFTC urges expedited formation and inclusion of private sector stakeholders to improve transparency and collaboration.**

The Oncology Prior-authorization System under the Civil Servants Medical Benefit Scheme (CSMBS) was designed to reduce out-of-pocket costs for high-cost cancer drugs. However, recent tiered revisions have made reimbursement inconsistent and unclear, with some newly approved drugs deemed non-reimbursable. Patients may face financial barriers or limited treatment options due to opaque criteria and budget constraints. To ensure equitable access, stakeholders recommend transparent OCPA procedures, outcome-based evaluations, and flexible financial models to balance innovation, affordability, and public health needs.

Services Barriers

Data Localization: In 2025, Thailand's Digital Government Development Agency (DGA) introduced draft guidelines – the Government Cloud Usage Guidelines and the Cloud Data Classification Guidelines – to support the national "Go Cloud First" policy. Despite the policy's aim for greater cloud adoption, the guidelines impose significant data localization requirements, mandating that most government and regulated data be stored in Thailand. Cross-border transfers are subject to narrow exceptions requiring

DGA approval and a local data center being built in Thailand. Furthermore, the policy stipulates that the most sensitive government data (in the “Secret” and “Top Secret” categories) can only be handled by a state-owned enterprise. Furthermore, there are requirements that providers comply with domestic procurement rules, achieve government-mandated certifications, and demonstrate conformity with Thai security standards, which will raise compliance costs and exclude providers that rely on global or regional data management models. These data localization and sovereignty requirements effectively limit participation by U.S. and other foreign cloud services providers from participating in public sector projects. These measures not only restrict competition but also risk fragmenting the digital ecosystem by forcing data silos and limiting the scalability of international services, creating significant market access barriers for U.S. cloud services providers.

Postal Parity: Current Thai law restricts any other carriers for transporting documents other than Thai Post. Express Carriers are regularly fined by Thai Post for transporting documents to recipients in Thailand.

Logistics Regulation: ETDA is proposing a logistics regulation that will require all e-commerce marketplaces to provide both customers and sellers with at least three logistics carrier options for deliveries. ETDA is aiming to implement the Logistics Regulation by December 2025. The draft, however, has not been shared publicly, and we understand that a call for public comments can be expected soon. Five local logistics carriers had been consulted behind closed doors by ETDA.

Ecommerce Guidelines: The Trade Competition Commission of Thailand (TCCT) is considering “Draft Guidelines on the Consideration of Unfair Trade Practices and Conduct Constituting Monopoly, Reducing Competition, or Restricting Competition in Multi-Sided Platform Businesses in the Category of Digital Platforms for the Sale of Goods or Services (E-commerce)”. The TCCT’s proposed guidelines are duplicative of the current competition law and enforcement framework in Thailand and will mandate significant compliance burdens on online retailers, while sparing local brick and mortar competitors. The guidelines propose a blanket restriction on certain conduct, without any need to show that the conduct is harmful. They include many vague and undefined terms without clear definitions or foundations in competition enforcement principles.

Platform Economy Act (Cloud Services): Thailand is drafting legislation to regulate digital services, adopting concepts from the EU's Digital Services Act (DSA) and Digital Markets Act (DMA). Under this proposed law, cloud services could be classified as 'intermediaries' and may become subject to 'gatekeeper' obligations. During the previous administration, development of the law was paused due to concerns about potential impacts on digital innovation and possible creation of trade barriers. However, with the recent change in government, the initiative has been revived. The new administration announced its intention to pursue this legislation in its policy statement in late September 2025, renewing industry concerns about potential regulations that could distort digital competition or disadvantage U.S. firms.

Digital Platform Fair Competition Draft Rule. The Trade Competition Commission of Thailand (TCCT) released its draft Guidelines on the Consideration of Unfair Trade Practices and Conduct Constituting Monopoly, Reducing Competition, or Restricting Competition in Multi-Sided Platform Businesses in the Category of Digital Platforms for the Sale of Goods or Services (E-commerce). The draft provides the first detailed framework for how the TCCT will interpret and enforce the substantive provisions under the Trade Competition Act against digital platforms, which have a unique network effect and require complex competition analysis. This development will profoundly impact the operations of e-commerce platforms, sellers, and associated service providers in Thailand. Affected digital platforms have highlighted issues such as proportional algorithmic transparency (aligned with international practice), allowing legitimate operational requirements (e.g., logistics/payment solutions) where justified, and flexibility in designing transparent and non-discriminatory fee structures.

Digital Platform Services (DPS) Decree: The DPS Decree, came into force in 2022, is a regulation that aims to enhance consumer protection in digital transactions. Initially designed to regulate electronic intermediary services that facilitate connections between users for commercial transactions, the decree primarily targeted platforms such as e-commerce marketplaces, ride-hailing services, and food delivery applications. The Electronic Transaction Development Agency (ETDA) is the owner of this regulation.

However, the implementation of this regulatory framework has evolved beyond its original scope, with ETDA extending registration requirements to a broader range of digital service providers. This expansion now encompasses social media platforms, video conferencing services, and cloud service providers - entities that arguably fall outside the decree's intended purview. This broadened interpretation of the regulation's scope has raised questions about the true objectives of the registration scheme and its effectiveness in achieving its stated consumer protection goals.

The registration requirements impose significant obligations on digital service providers, including annual reporting of user statistics and gross revenue disclosure. These extensive reporting requirements, particularly those related to financial data, suggest potential agendas beyond consumer protection, possibly laying the groundwork for future digital taxation initiatives. Moreover, the regulatory burden appears redundant given the existence of multiple consumer protection frameworks already governing digital commerce, raising concerns about regulatory overlap and unnecessary administrative complexity.

High-Impact Marketplaces. Thailand's Electronic Transactions Development Agency (ETDA) designated 19 digital platforms as "High-Impact Marketplaces," imposing additional compliance obligations. On July 9, 2025, the Royal Gazette published this list of digital platforms required to comply with Section 20 of the Royal Decree on the Operation of Digital Platform Service Business, effective July 10. Under Section 20, designated platforms must undertake business risk assessments and implement risk management frameworks. This requirement applies to platforms involved in selling or advertising products governed by regulatory standards and considered critical to economic and financial stability. The list of platforms will be reviewed annually to ensure continued relevance and oversight.

Content Moderation: Thailand has enacted two laws that raise significant industry concerns regarding government overreach and surveillance. Under the Computer Crime Act, the Ministry of Digital Economy and Society established an Anti-Fake News Center to combat what is considered "false and misleading" in violation of the Act, and leveraged this to expand oversight of content and identify millions of posts. Similarly, the controversial Cybersecurity Act grants officials broad authority to search and seize data and equipment in what are vaguely defined as "national emergencies," enabling potential government surveillance.

State-Owned Enterprises / Procurement

Preferential Procurement: Thailand Government Pharmaceutical Organization (GPO), a Thai State-owned enterprise that manufactures pharmaceutical products in Thailand, benefits from preferential procurement privileges. Per Ministerial Regulation B.E.2560 (2017), government hospitals must procure at least 60 percent of their medicines budget from the NLEM. Specific procurement methods are required if the product on the NLEM is manufactured by the GPO or the Thai Red Cross Society. Purchases from other suppliers are permitted only when the GPO or the Thai Red Cross Society is unable to produce and distribute the product. In addition to these procurement preferences, under the Drug Act B.E. 2510 (1967), the GPO is not required to obtain FDA approval prior to launching medicines on the Thai market. There is no such exemption for private sector manufacturers or sellers, all of whom must obtain appropriate market authorization from the Thai FDA prior to selling their products in the Thai market. Further procurement privileges are also being extended to local vaccine producers under National Vaccine

Committee Regulations on “Vaccine Procurement in Government Sector” that went into effect on August 14, 2020.

Türkiye

Import Policies

Market access delays (Pharmaceuticals): Long licensing processes delay product entry into the Turkish market. The Turkish Drug and Medical Device Agency (TITCK) prioritizes Good Manufacturing Practices (GMP) audit procedures and allows marketing authorization applications to advance in parallel with GMP process. However, these procedures have not diminished the delays in MA approvals. While “highly innovative designated products” receive preferential reviews, products without this designation face increased delays in GMP inspections. For the GMP inspections that are carried out by the FDA and/or EMA, the Turkish authority should not carry out GMP inspections for the same imported products with approved and accredited certificates. Instead, it should recognize FDA or EMA approvals and there should not be an additional GMP audit by Turkish authority.

Services Barriers

Data Localization: A 2019 Presidential Decree on Information and Communication Security Measures introduced broad data localization requirements for government workloads deemed “strategic”. In 2020, the Digital Transformation Office published guidelines detailing the applicability of the localization requirements to be inclusive of critical information and data. Strict data localization requirements are also applied to the financial services industry, where the Banking Regulation and supervision agency requires primary and secondary information systems to be hosted in Türkiye. The Central Bank of Türkiye implements similar restrictions for the outsourcing of cloud services, and prohibits the use of cloud for certain workloads. The Capital Markets Board published legislation requiring data localization for the cryptocurrency sector. The Ministry of Industry and Technology's R&D body (TUBITAK) introduced strict data localization requirements for cloud usage.

Competition / Ex Ante Rules: Türkiye proposed an amendment to its competition law that largely mirrors the EU's Digital Markets Act. The draft law imposes significant obligations on large digital platforms, which are disproportionately U.S. companies, including mandatory interoperability, a ban on self-preferencing, and restrictions on using data across different services. The draft law also includes severe penalties, such as fines of up to 20% of annual turnover and potential five-year bans on mergers and acquisitions. While the draft law is currently on hold pending trade negotiations with the U.S., certain obligations included in the draft law were, however, adopted in the Regulation of E-Commerce Law, which took effect January 1, 2024. The law prohibits e-commerce intermediary service providers from selling their own trademarked goods on their platform. It imposes additional obligations on larger providers, with those with an annual net transaction volume greater than ₺10 billion (US$538.3 million) prohibited from using data collected to compete with other providers, and those with an annual net transaction volume greater than ₺60 billion (US$3.3 billion) prohibited from expanding into industries such as payments, transportation, and delivery as separate business models. Moreover, it imposes new taxes on companies based on their revenues, while providing relief for Turkish-headquartered e-commerce companies. These excessive regulatory requirements, *de facto* preference for Turkish companies, and pressures for localization represent clear barriers for U.S. companies.

Digital Services Tax: Türkiye continues to administer its DST that USTR has previously determined to be discriminatory in a Section 301 investigation initiated in 2020. USTR has previously found that the Turkish DST “is discriminatory against U.S. companies, “contravenes prevailing international tax principles”, and “burdens or restricts U.S. commerce” in its 2021 report on this barrier. The tax

undermines U.S. exports, threatens American jobs, and raids the U.S. tax base. Türkiye's 7.5% DST went into effect on March 1, 2020. The global revenue threshold for this tax is ₺750 million, with a local threshold of ₺20 million. The tax applies to revenue generated from the following services, all of which are sectors where American companies are world leaders: (1) digital advertising, (2) online streaming and sales of audio and audiovisual content, and (3) social networking services. The tax disproportionately impacts U.S. companies. By maintaining this discriminatory tax, Türkiye is promoting unfair treatment of US companies in the market, to the detriment of American exports, tech leadership, and for consumers and businesses in the Turkish market that partner effectively with US tech companies. **NFTC encourages USTR to continue working with Türkiye to address the discrimination against U.S. companies under Türkiye's DST.**

Additionally, in 2024, Türkiye amended Law No. 6563, which would impose burdensome withholding tax requirements for non-resident companies that operate e-commerce platforms, depending on how the law is implemented. There is significant uncertainty in the scope and base of the tax, and industry urges vigilance to ensure companies can operate with fair access in the market. The new requirements took effect January 1, 2025.

Content Moderation: Türkiye has established a highly restrictive and punitive environment for internet services, actively using censorship and legislation that economically harms U.S. companies. A key step was the July 2020 passage of Law No. 7253 (amending the Law on the Regulation of Publications on the Internet and Suppression of Crimes Committed by Means of such Publications), which grants the government sweeping powers over social media. This law compels platforms with over one million daily users to appoint a local representative, respond to takedown requests within hours, and store the data of Turkish users domestically. Authorities moved quickly to enforce these rules, imposing fines, advertising bans, and bandwidth restrictions on non-compliant firms.

The government further intensified its control with Law No. 7418 (Amendment of Press Law, and Certain Laws) in October 2022, which criminalizes the spread of "disinformation" with prison sentences of up to three years. This law requires platforms to disclose algorithms and user data to the government upon request and threatens penalties including fines of up to 3% of global revenue and bandwidth throttling up to 90%. The law also extended the authority of the Information Technologies and Communications Authority (ICTA) over messaging (OTT) services, empowering it to demand detailed user activity data. Failure to comply could result in fines rising to ₺30 million (US$1.6 million), throttled service up to a 95% restriction on the usual bandwidth capacity, or outright service blockage. Subsequent regulations in April 2023 solidified these obligations, holding platforms responsible for user-generated content and imposing a comprehensive set of duties on all social network providers, regardless of size. These measures negatively impact U.S. companies by imposing steep financial penalties, significant operational burdens like mandatory data localization, and severe legal risks, including liability for user content and the forced disclosure of proprietary algorithms and user data.

OTT Regulation: In March 2025, Türkiye's Information and Communication Technologies Authority (ICTA) proposed sweeping regulations that would subject over-the-top (OTT) communication providers to the same burdensome regime as legacy telecommunications firms. The draft rules mandate that OTTs with over one million monthly users must incorporate locally as a Turkish company, obtain authorization under telecom law, and contribute to a universal service fund for infrastructure they do not use. Additionally, providers would face vague "national security" obligations that could lead to surveillance, and the government reserves broad power to impose severe penalties, including fines, service throttling, or outright blocking. These requirements, particularly the forced local incorporation, create significant market access barriers for U.S. and foreign companies, undermining the cross-border model of the internet, stifling innovation, and tilting the market in favor of domestic incumbents.

Additional E-Commerce Regulations: A new set of e-commerce regulations in the Law on Amending the Law on Regulation of Electronic Commerce took effect in 2023. Firms that facilitate sales equaling or topping ten billion Turkish lira net ($538.3 million) annually and over one hundred thousand executed transactions will be required to obtain a license to operate in the country and renew that license when the Ministry of Commerce dictates. Further, the law requires a restriction on e-commerce providers selling goods of their own brand or brands with which they have economic associations. E-commerce providers will also be subject to obligations to take down illegal content and ads, ensuring information is correct, obtaining consent before using brands for promotions, and refraining from anticompetitive practices. For firms with a net transaction of over 60 billion liras ($3.3 billion), there are a host of other restrictions regarding banking, transportation, and delivery.

Electronic Payment Services level-playing field: Türkiye continues to contemplate extraterritorial authority over U.S. electronic payment services companies and their clients domiciled outside of Türkiye. Specifically, Türkiye is considering regulation of inbound cross-border payments originating from the EU, and such regulation would be more burdensome and restrictive on U.S. EPS providers and their clients, than it is on domestic companies. In order to promote local payment facilitators, the Finance Ministry and Central Bank continue to scrutinize Visa rules prohibiting Turkish acquirers from providing acquiring services to a merchant located in a jurisdiction where it does not have a license to operate, and misrepresenting the location of the foreign merchant as if it was based in Türkiye.

Intellectual Property Protection

Inadequate Regulatory Data Protection and patent enforcement (Pharmaceuticals): According to Türkiye's Industrial Property Law, which was passed by the Turkish Parliament in 2016, the RDP term begins with first marketing authorization of the original product in any of the EU-Türkiye Customs Union Area Member States. As a result, the effective RDP term is reduced significantly to 6 years in Türkiye – and considering the marketing authorization process timeline of approximately 2-3 years, the life without generics is approximately 3 years for originator/innovator products.

Ukraine

Services Barriers

Cloud Law, Public Procurement Law, Public Electronic Registers Law, Information Protection Law, Law on Protection of Personal Data, National Bank of Ukraine Regulations: Ukraine's Martial Law (a special legal regime introduced in February 2022 after Russia's invasion) temporarily suspended restrictions on the use of commercial cloud services by the public sector and certain private sector entities (e.g., banks). This allowed the Ukrainian Government to safeguard its data with support from U.S. CSPs. However, Ukraine's cloud adoption may be hampered once the Martial Law is withdrawn, as its outdated legislation poses challenges for both U.S. CSPs and their Ukrainian customers. Key concerns regarding the legislation include: (i) a lack of recognition of international cybersecurity standards (e.g. ISO) obtained by CSPs, and a preference for local technical requirements; (ii) the exclusive application of Ukrainian law to govern cloud service agreements, which is incompatible with the cross-border nature of cloud services; (iii) restrictions on the ability of non-Ukrainian CSPs to provide services to public institutions involving the processing of personal data; (iv) requirements to re-migrate certain categories of data to Ukraine (temporarily allowed by the Martial Law to be stored abroad); and (v) a lack of clear data classification regulations.

United Arab Emirates

Services Barriers

Data Localization and Sovereignty Requirements: The UAE Cyber Security Council mandates cloud services providers that serve the public sector and certain regulated industries to be solely subject to UAE law; not be subject to foreign jurisdiction and foreign laws; and physically localize data centers as well as engineering, security, maintenance, and support operations and respective personnel in the UAE. Similar localization requirements are now imposed on data processing for financial services and the healthcare sector: the UAE Central Bank's outsourcing guidelines ban financial services institutions—not including subsidiaries of foreign banks—from storing and processing personal data outside the country; and the UAE 2019 Health Law also obligates processors to conduct activities for health data within the UAE. Further, the Abu Dhabi Healthcare Information and Cyber Security Standard disallows hosting information sharing systems on cloud services. The UAE Government's approach to data sovereignty for CSPs serving public sector and regulated industries has evolved with the publication of the National Cloud Security Policy by the UAE Cyber Security Council (CSC) in September 2025. The new policy allows foreign CSPs with infrastructure in the UAE to serve most government and regulated workloads, except for Secret and Top Secret classified data which must be hosted in fully sovereign infrastructure (e.g. Gov Cloud) with more stringent controls, including exclusive UAE jurisdiction, UAE-based Hardware Security Modules (HSMs), and denial by default of all foreign access requests. While this framework provides clearer pathways for foreign CSPs to serve government customers, informal preferences remain for local technology champions like G42, and ongoing data and infrastructure localization requirements continue to undermine U.S. providers from serving the private sector and regulated customers and serve as a barrier to market entry.

The United Kingdom

Import Policies

UK CBAM: The United Kingdom is developing its own Carbon Border Adjustment Mechanism (CBAM), closely modeled on the European Union's system but with differences in pricing and scope. Announced in December 2023, the UK CBAM will apply to imports of carbon-intensive goods with implementation set for 2027. The measure aims to prevent carbon leakage by aligning the carbon costs of imported goods with those produced domestically under the UK Emissions Trading Scheme (ETS). However, variations in calculation methods and reporting requirements compared to the EU's CBAM will greatly increase compliance complexity for U.S. exporters operating in both markets.

Technical Barriers to Trade

Excessive revenue clawbacks (Medicines): Revenue clawbacks on brand medicines have increased dramatically over the past several years, further reducing spending on already devalued medicines. The UK government should with the industry to review the terms of the VPAG scheme and agree a solution that returns VPAG to a situation where the clawback declines towards a single digit percentage of revenue by the end of the scheme (2024-2028) as a step towards elimination.

Biased health technology assessment: The United Kingdom uses low and outdated monetary thresholds per life year gained from clinically proven treatments, which have not been updated for inflation since 1999 (depreciating a life year by more than 47% over the past 25 years). The National Health Service (NHS) requires excessive price discounts (£3.4B in 2025, among the highest in the world) based on these biased valuations before agreeing to fund new treatments. These same valuations are also used as a reason to restrict access to only a small subset of the population for which the regulator deems the product to be

safe and effective and to deny access completely for many treatments. The UK government should urgently review and increase the cost-effectiveness threshold in line with levels that at least reflect inflation and healthcare budget growth since its introduction.

Services Barriers

Digital Markets, Competition, and Consumers Act: The Digital Markets, Competition and Consumers Act (DMCCA) is a new competition framework that came into force in January 2025. It is designed to regulate digital markets by designating firms with 'Strategic Market Status' (SMS) and imposing behavioral requirements and 'pro-competition interventions'. The regime empowers the UK Competition and Markets Authority (CMA) to address alleged competition issues in digital markets, particularly focusing on companies with 'substantial and entrenched market power', 'strategic significance', and turnover thresholds of over £25 billion globally or £1 billion in the UK. This framework represents a shift from traditional ex post market investigations to permanent regulatory oversight, enabling the CMA to impose forward-looking conduct requirements on a small set of firms, overwhelmingly U.S. headquartered. These can include regulation of prices and other commercial terms allowing CMA to create transfers to domestic vested interests (including a final offer mechanism similar to the Australian news media bargaining code, but not limited by sector); requiring interoperability and data sharing; which services will be offered to consumers and how and when (e.g. choice screens) and restrictions in other areas such as how complaints are handled and how data is used. The CMA has also published "roadmaps" with potential conduct requirements. These would include many of the potential measures described above including speculative interventions regarding the integration of AI services. The breadth and potential impact of these measures has created considerable uncertainty for the services affected. . While the CMA has not yet designated a firm with SMS, it has provisionally decided to designate Apple and Google with SMS in specific areas. A final decision is expected by 22 October 2025. Additionally, the CMA has launched three SMS investigations so far, all of which have concerned services provided by American companies (Google Search and the Apple and Google mobile ecosystems). USTR should encourage the UK to make sensible changes to the regulatory regime, including: making compliance simplifications, undertaking a formal economic assessment and only intervening when it finds clear evidence of economic or competitive harm, base fines and fees on UK turnover (not global).

Online Safety Act: The Online Safety Act (OSA) passed into law in 2024, under the previous (Conservative) Government. It creates new rules for internet services, designed to protect users from harmful content. Under the Act's Section 122, the Office of Communications (OFCOM) can provide notice to companies to scan their data, including user messages, to proactively identify and prevent illegal content. Such requirements are incompatible with end-to-end encryption security measures deployed by digital platforms, and would require companies to install client-side scanning software that would undermine encryption, increasing risks to privacy and security. The intention of the Act was that the most onerous rules would apply to a small number of 'Category 1' firms – the largest, most harmful social media services. However, there is now discussion on whether to include unrelated, low-risk services like marketplaces. The Government recognizes that low-risk services like marketplaces were not the intended target of the Act, and should not be subject to Category 1 obligations, but the final decision rests with the regulator, Ofcom. It is critical that Ofcom not designate marketplaces as in scope.

Digital services tax: The UK has a 2% DST. The threshold is for companies with worldwide revenue of £500 million and local revenue of £25 million. The tax applies to revenues of "digital services activity" which includes "social media platforms," "internet search engines," or "online marketplaces." The UK government has acknowledged that 90% of the tax is paid by 5 digital services companies, which are likely all American, as USTR has previously identified in its Section 301 report.

Intellectual Property Protection

SPC Term Calculation: Following the UK's exit from the EU, one of industry's key IP incentives, the term of the supplementary protection certificate (SPC), has been linked to the date at which a medicine is granted marketing authorization (MA) in the UK or EEA/EU, whichever is first. This means that the term of some UK SPCs will be determined by decisions taken by the European medicines regulator, rather than the post-Brexit UK regulator (MHRA). This is inconsistent with other updates to post-Brexit pharmaceutical legislation in the UK which puts decision making solely in the power of UK organizations. It also means that if a company is granted MA in the EU prior to the UK, the term of protection in the UK begins to run before the company can sell the medicine in the UK market, reducing the effective duration of IP protection in the UK below that in European countries. The UK regulation on SPCs should be minimally amended to remove the reference to EU marketing authorization, so that only the UK MA is used in the calculation of the SPC term in the UK.

Vietnam

Import Policies

Import / Export License Requirements for Encrypted ICT Products: Vietnam's Government Cipher Committee ("GCC") requires that the import and export of any product containing cryptographic functionality obtain specific permits and licenses. Suppliers importing and exporting IT products with regulated data encryption capabilities (civil cryptography products or "CCP") must obtain a Cryptography Trading License ("CTL") and a Cryptography Import License ("CIL"). These requirements are unfair because it takes several months to obtain CTLs and CILs, which is an inordinate amount of time. Detailed information needs to be submitted alongside the application, including detailed product information, defined technical plans, information regarding the equipment's cryptographic functions, information regarding local personnel, and other material. In seeking to meet these requirements, companies often experience delays and inconsistent/non-transparent approvals or rejections by the GCC. These burdensome requirements, and the routine follow ups that the GCC requires, limit the ability of companies that invest in Vietnam to import critical hardware. A new regulation for cryptographic certification equipment, the Circular 23/2022/TT-BQP of the Ministry of Defense, has introduced further uncertainty.

In addition to the license required for CCP, since April 2024, Vietnam introduced an additional cyber information security licensing requirement for products designed with functions to maintain cyber information security. As such, products previously determined to be exempted from the CCP licensing now require a separate license from the Ministry of Information and Communication. The application process and required documentation are unclear, and initial applications for cyber information security trading license still remain pending approval. The dissolution of the Ministry of Information and Communication in February 2025 further adds to the confusion, as it is unclear if the license authority would be transferred to the Ministry of Public Safety or to the Ministry of Science and Technology. The vacuum of regulatory authority also creates uncertainty about how to obtain the necessary licenses to continue importing to Vietnam.

Prohibition on the Import of Refurbished Products: Vietnam maintains import prohibitions on certain used information technology ("IT") products. While Decision 18/2016/QD-TTg eases import prohibitions on some used IT products, lenient treatment only applies provided that they meet various mandatory technical regulations and standards.

Prohibiting the import of refurbished products violates Vietnam's international trade commitments. Products and components are essential in order to continue supporting customers with products that are under warranty, especially when such products have reached end-of-sale and components are no longer

available as new products. In particular, critical infrastructure customers are unable to obtain replacement parts to service and maintain critical elements of their infrastructure without access to refurbished products.

Authorised Economic Operator: Vietnamese Customs is reported to be requesting that companies applying for the Authorised Economic Operator (AEO) compliance program are being asked to accommodate onsite visits from a third party as a necessary precondition to be approved for the application. The program fee is reported to be US$100K. U.S. tech companies have encountered this and engaged USTR to intervene, and were subsequently able to bypass the third party. Membership in a trusted trade program should not be preconditioned on the payment of a significant fee to a third party.

Services Barriers

Draft Cybersecurity Law: Vietnam's 2018 Cybersecurity Law introduced problematic data and server localization requirements, imposed severe penalties, and required companies to closely monitor and report information to the Vietnamese government. Among other things, it included provisions on content regulation, requiring online services to monitor user-generated content and remove "prohibited" content within 24 hours upon notification from the government. It also established procedures for service providers to both terminate access for a user posting "prohibited" content and share information regarding the user (information service suppliers may not have, if data is encrypted). "Prohibited" content is vaguely defined as any content that, *inter alia,* is critical or disparaging of the Vietnamese government. Companies have already been fined under this provision. Decree 53/2022/ND-CP, implementing the Cybersecurity Law, expanded data localization requirements with vague and inconsistent data localization rules. While it appears that only domestic companies were required to immediately localize data and foreign companies only needed to do so under certain conditions, uncertainty around applicability and the scope of localization has resulted in local companies discriminating against foreign service providers – effectively favoring local service providers.

The 2018 Cybersecurity Law is currently undergoing revision. However, the draft revisions, based on the latest September 2025 version, imports the 2018 Cybersecurity Law's broad and vague data localization requirement. The draft revisions would also require service providers on telecom networks, on the Internet, and value-added services on cyberspace in Vietnam to store user data domestically and establish representative offices in Vietnam. Additionally, the draft revisions contain concerning provisions, including overly broad and vague surveillance mandates, insufficient takedown timelines and procedures, insufficient time for compliance, and inadequate due process for information requests.

Overall, such measures serve as a significant market entry barrier for U.S. cloud and software providers and disrupt the cross-border provision of cloud services and business software service suppliers.

Draft New E-commerce Law. Vietnam has unveiled a draft e-commerce law that would mandate online platforms to verify domestic sellers via VNeID and foreign sellers through legal documents, extending oversight to livestream sales, affiliate marketing, and social media commerce. The draft law is nearing completion and is expected to be submitted for National Assembly approval during the Oct. 20 -- Dec. 12, 2025 session, being effective starting in 2026. Foreign platforms would be required to establish a local entity or representative, deposit funds at a Vietnamese bank, and comply with transparency and consumer compensation rules. The draft also assigns responsibilities to logistics, payments, and infrastructure providers, obliging them to work only with compliant platforms.

Domestic Processing Mandate (SBV Circular 18/2024/TT-NHNN): This circular, which replaces previous regulations, codifies and reinforces a discriminatory domestic processing mandate. It requires

that all domestic card-present transactions conducted on the networks of U.S. electronic payments companies must be routed through the National Payment Corporation of Vietnam (NAPAS). This mandate limits competition, preventing U.S. companies from using their own global processing infrastructure for domestic transactions, and favors a state-owned entity, undermining the principles of national treatment.

Data Localization Requirements: There continue to be policy developments that mark a trend toward data localization in Vietnam. Any changes mandating that foreign companies store data physically within Vietnam poses a significant threat to the country's economic competitiveness, risks derailing the government's digital transformation agenda, and could significantly diminish the country's position as a regional leader in the digital landscape. Examples include the Cybersecurity Law and (discussed above), and the following:

- **Data Law and its implementing decrees - Decree 165 and Decree 169:** In November 2024, the National Assembly passed the Law on Data (No. 60/2024/QH15) (Data Law). The Law went into force together with its implementing Decrees 165 and 169 on 1 July 2025. The Law and its implementing decrees have duplications with the PDP Law on regulations on personal data governance. The Prime Minister Decision No. 20/2025 dated 1 July 2025 supporting the execution of the Data Law and its Decree introduces new categories of "important data" and "core data" similar to China's Data Security Law that can have chilling effects on foreign investors in Vietnam. The Data Law and Decree 165 impose onerous obligations on individuals and organizations for authenticating and ensuring the accuracy of created data as well as approvals for cross border transfers of core data. They also grant the government sweeping powers to requisition private data under vaguely defined "national interest" or "public interest" grounds, without clear due process safeguards. The Data Law and Decree 169 mandate licensing and regulating data products and services such as data intermediary, data analysis and aggregation products and services, and data exchange services. An implication of such requirements is that offshore enterprises not incorporated or registered in Vietnam would not be allowed to offer any of the above services to Vietnamese customers.

- **Personal Data Protection Law**: In June 2025, the National Assembly passed the Personal Data Protection Law - PDPL and released the draft implementing decree (draft PDPD) for public comments. The PDPL and draft PDPD regulate personal data processing in specific contexts (e.g., marketing, behavioral and targeted advertising, big data processing, AI, cloud computing, recruitment and employment monitoring, banking and finance, social networks and media services) as well as specific categories of personal data (e.g., health and insurance data, location data, biometric data, credit data, children's data). The PDPL and the draft PDPD expanded their scopes beyond Decree 13/2023/ND-CP to include personal data of individuals residing in Vietnam, regardless of their nationality. The PDPL and draft PDPD impose onerous obligations on the processing of personal data as well as the transferring of personal data across borders. The PDPL also establishes stringent penalties for non-compliance, including administrative fines of up to 10 times the revenue generated from the unlawful sale of personal data, penalties of up to 5% of annual revenue for unauthorized cross-border data transfers, and fines up to VND3 billion (US$115,000) for other infractions. These obligations would impede the ability of companies that need to process cross-border data from continuing to offer services to customers in Vietnam.

Digital Transformation Law (DTL): Vietnam is considering implementing a comprehensive digital regulation law that closely mirrors the EU's Digital Markets Act and Digital Services Act, but includes additional government-led compliance and data sovereignty elements that will likely disproportionately impact U.S. companies. The draft Digital Transformation Law (DTL)_incorporates a wide range of distinct legal frameworks including consumer protection, data privacy, and algorithmic transparency obligations, new digital specific ex ante obligations, and new online safety obligations.

National Digital Transformation Strategy – Domestic Preferences: Under its 2020 National Digital Transformation Strategy, Vietnam is implementing policies to control cross-border platforms and promote domestic industry. The government has issued cloud standards that offer preferential treatment to local providers for public sector projects, a move that is inconsistent with Vietnam's government procurement obligations under the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). Although technically voluntary, these standards are expected to be widely adopted, creating a significant advantage for Vietnamese firms in cloud computing and digital infrastructure.

Content Moderation: On November 9, 2024, the Vietnamese government issued Decree No. 147/2024/ND-CP on the Management, Provision, and Use of Internet Services and Online Information (Decree 147) replacing Decree No. 72/2013/ND-CP ("Decree No. 72") and imposing stringent requirements on foreign "Regulated Cross-Border Services" (over 100,000 monthly Vietnamese visits or local data center use). . Decree 147 requires these entities/services to: appoint a local contact; store user data; remove flagged content within 24 hours; temporarily block content within 48 hours of complaints; and form "cooperation agreements" with Vietnamese press. Additional obligations include content scanning, child protection, and regular reporting. Social networks must verify accounts and restrict features, while app stores must comply with payment laws and remove government-requested apps. Decree 147 also prohibits cross-border online games, requiring foreign publishers to establish local entities and introduces a 16+ age rating. These rules create market entry barriers, expand state surveillance, increase compliance costs, and conflict with data minimization. ITI supports USTR's acknowledgment of these risks in its 2025 NTE report and urges continued U.S. engagement to counter measures undermining digital trade, user rights, and market access.

Artificial Intelligence: In July 2024, the Vietnam government proposed provisions relating to artificial intelligence (AI) in its draft Digital Technology Industry Law (DTI Law). The government has since reframed the AI provisions into a separate piece of legislation – the draft Law on Artificial Intelligence. Planned for approval in December 2025, the draft Law establishes a comprehensive regulatory framework using a prescriptive, risk-based approach that classifies AI systems into risk tiers – "unacceptable" (prohibited), "high", "medium", and "low". High-risk systems face stringent pre-market requirements, including mandatory conformity assessments, rigorous logging, and human oversight. However, this "regulate-first" model is considered ill-suited for the dynamic nature of AI, as its extensive documentation requirements and resource-intensive obligations create excessive compliance burdens that stifle innovation, disproportionately harm smaller innovators, and create significant barriers to entry, ultimately deterring investment.

Digital Services Taxes: The Tax Administration Law, effective July 1, 2020, taxes cross-border e-commerce and other digital services. The Ministry of Finance issued Circular 80 providing guidance on the Law and its Decree 126 in September 2021.The Circular added a requirement for foreign digital service and e-commerce suppliers without a permanent establishment in Vietnam to directly register and pay taxes. If the foreign service providers do not register, service buyers (or commercial banks in case of individual buyers) will withhold tax from their payment to foreign suppliers at deemed tax rates. While the Law allows for certain exemptions under applicable tax treaties, digital suppliers who have sought such exemptions have faced onerous processes coupled with undue administration processing delays. The additional tax burden created by the deemed tax rates (Corporate Income Tax and Value Added Tax) will result in further complications and costs for cross-border service providers and conflict with international taxation rules.

Telecommunications Services: Vietnam permits foreign participation in the telecommunications sector, with varying equity limitations depending on the sub-sector. According to the Law on Telecommunications (Telecom Law) 41/2009/QH12, for domestic companies that provide basic telecommunication services with infrastructure, foreign ownership is generally capped at 49 percent; for

companies that supply telecommunications services without infrastructure, foreign ownership is capped at 65 percent. Vietnam allows foreign ownership of up to 70 percent for virtual private network (VPN) services suppliers. Facilities-based operators are required to be state-controlled firms, meaning that the state, through the relevant line ministry, must hold 51 percent or more of equity.

The revised Telecom Law was passed by Vietnam's National Assembly on November 24, 2023 with a "light touch" regime for OTT, data center and cloud services. The Ministry of Information and Telecommunications (MIC) has drafted the Decree implementing the Telecom Law and sought industry's inputs. The final draft is under final review by the Government Office.