Coalition of Services Industries (CSI) Submission:
Comments for the National Trade Estimate Report on Foreign Trade Barriers
Docket Number USTR-2025-0016

Overview

The Coalition of Services Industries (CSI)[1] appreciates the opportunity to submit comments identifying significant barriers to U.S. services exports and investment to the Office of the United States Trade Representative to assist in the preparation of the National Trade Estimate Report on Foreign Trade Barriers (NTE).

Services and digitally-enabled services bolster U.S. technology leadership, including in AI, and promote the competitiveness of U.S. manufacturing, agriculture, and sectors across the economy. The U.S. is a global leader in creating and exporting highly innovative services and digitally-enabled services – boasting $1.0 trillion in cross-border exports in 2023co – with a longstanding services trade surplus. Services and digitally enabled services account for a significant portion of input in manufacturing exports, in U.S. semiconductors, computers, machinery and equipment. In fact, manufacturers are the second largest U.S. exporter of services, after the financial services sector. Think not only of robotics and advanced manufacturing, but also cutting-edge financial services in banking, electronic payments and insurance, as well as logistics.[2] To advance U.S. manufacturing, it is imperative to support U.S. services exports and U.S. services investment abroad.

Rising barriers to services and digital trade continue to threaten the U.S. competitive advantage in services and digital trade, as well as U.S. leadership on key technologies like artificial intelligence. These barriers include limits on cross-border data flows, data localization requirements, and discriminatory regulatory frameworks and standards. It is important to address these nontariff barriers constructively with our trading partners to maintain American competitive advantage in services and digital trade, and to continue to support not only American service providers, but also the brick-and-mortar industries like manufacturing and agriculture that rely on these services to export.

Ongoing negotiations on reciprocal trade, as well as continued and renewed trade and investment framework agreement (TIFA) discussions, are great opportunities and should be used to address services and digital trade and investment barriers, as a part of the overall efforts to maintain U.S. leadership in services, technology, and trade.

Please find below a non-exhaustive list of trade barriers in priority markets that pose the most urgent threats to the growth and competitiveness of the U.S. services and digital sectors. Thank you for the opportunity to provide this submission.

[1] CSI, established in 1982, is the leading U.S. industry association devoted exclusively to ensuring America's services businesses, which are increasingly digitally enabled, and workers compete in world markets. CSI member companies represent a broad spectrum of the U.S. services sector including distribution services, express delivery, financial services, media and entertainment, telecommunications, information and communication technology services, and professional services.

[2] https://apps.bea.gov/scb/issues/2024/05-may/0524-profile-services-traders.htm

Argentina

Data Transfers: 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.

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.

Barriers on Electric Equipment Import: 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. Consequently, 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.

Australia

Audiovisual:
Broadcast Quota: Under Section 9 of the Australian Broadcasting Authority's Content Standards, and as reaffirmed in the March 2016 Broadcasting Services Standard, 55 percent of all free-to-air television programming broadcast between 6:00 a.m. and midnight must be of Australian origin. In addition, under Section 102 of the Broadcasting Services Amendment Act, pay television channels that include more than 50 percent drama programs in their schedules are required to spend 10 percent of their total drama programming expenditures on new Australian/New Zealand programs. Although the U.S.-Australia Free Trade Agreement (FTA) capped broadcast quotas for analog TV at the existing 55 percent level and capped sub-quotas at existing levels, these limitations still pose a barrier to market entry. Moreover, Australia reserved the right to extend these quotas to digital broadcast TV, though the obligation can apply to no more than three multiplexed channels of any current broadcaster.

OTT/VOD Local Content Obligations: There have been several reviews in recent years regarding the availability of Australian content and asymmetry between local content obligations for free-to-air broadcast and the absence of these obligations on digital platforms, as well as, the idea of introducing local content obligations extending to VOD services. The definition of Australian content is still uncertain but will likely be very difficult to meet. Additionally, the expenditure percentage increases with the number of subscribers. Such obligations would be violative of Australia's FTA commitments to the United States. The government can only impose measures if Australian content is not readily available to Australian consumers, but there is no data to support any assertion of market failure.

News Bargaining Incentive: 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 ($160m) 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 amount to a targeted and highly discriminatory DST. A public consultation is expected this year and we hope that stakeholders views will be heard.

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.

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 2026. 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.[3] 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

Draft Taxation Ruling on Royalties: In January 2024 the Australian Taxation Office (ATO) released a revised draft ruling (TR 2024/D1) ruling concerning the characterization of payments by a distributor for software-related rights as royalties subject to royalty withholding tax.

TR 2024/DI replaces 2021/D4, a ruling that signified a significant departure from global norms regarding the tax characterizations of software payments made by distributors and resellers. Specifically, Australia's long-standing guidance, TR 93/12 – Income Tax: computer software (which was withdrawn on July 1, 2021, with the release of draft TR 2021/D4) makes clear that a payment by a distributor for a license of a simple use of software does not constitute a royalty if it is licensed to end-users, as the distributor is not exploiting a software copyright right. The simple use of software means that a licensee or end-user is using the product as intended (and therefore not using the copyright in the software). This is the approach taken in the OECD Model Tax Convention on Income and on Capital and related commentary, which acknowledges that "distributors are only paying for the acquisition of the software copies, not to exploit any right in the software copyrights," and therefore relevant transactions should not be treated as royalties.

Public Country-by-Country Reporting: On June 5, 2024, the Australian government introduced legislation to the Parliament that proposes to implement public country-by-country (CbC) reporting for multinational enterprises (MNEs) for reporting periods that start on or after 1 July 2024. The The Senate Economics Legislation Committee (SELC) endorsed the bill in August 2024, and it is still under Senate review.

[3] https://ccianet.org/wp-content/uploads/2025/02/CCIA_New-Digital-Competition-Regime-Insights-into-Economic-Risks_report.pdf.

Bangladesh

Data Localization Mandates: 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[4] 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.

[4] https://en.prothomalo.com/bangladesh/ovdfi8qd4b

Bolivia

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.

Brazil

Customs: Brazil's de minimis threshold (Decree No. 1804 of 1980 and Ministry of Finance Ordinance No. 156 of 1999) — for which no duty or tax is charged on imported items – only applies to postal shipments under $50. The current level, along with its limited application, is not commercially significant and serves as a barrier to e-commerce, increasing the time and cost of the customs clearance process for businesses of all sizes. This problem is made more acute by the current import duty rate of a flat 60 percent charge levied on all express shipments—an extremely high rate when compared to other countries. In their current form, Brazil's policies increase transactional costs for U.S. exporters and Brazilian businesses and restricts consumer choice and competition in the market. We encourage the improvement of this barrier to trade by extending the de minimis threshold to both B2C and B2B transactions, both to Post and express delivery shipments, and increasing the threshold to a commercially meaningful level. Additionally, consistent with its separate efforts to reduce certain tariff rates, Brazil should reconsider the 60 percent levy on express shipments.

Brazil has already moved forward in its trade facilitation policy, by implementing the new Single Window project for imports and exports. The goal with this project is to reduce the average time of customs procedures, by implementing one integrated system, cutting bureaucracy and paper requirements. The creation of the Product Catalog is part of this proposal to reduce the import time. It is a database of products and foreign operators, and its main objective is to increase the quality of the product description, with information organized in attributes, attaching documents, images and photos that help the administrative treatment, inspection and risk analysis. The e-commerce particularities should be considered within this process to guarantee a simplified process for products bought online. It is crucial that the government considers the e-commerce contributions to the public consultation opened to review the list of attributes and ensures that businesses have proportional time to adapt to these new requirements.

Audiovisual: The current regulatory framework includes long and complex decision-making processes that negatively impact telecom operators by increasing technical, marketing, sales, and IT costs. The government should be challenged to enhance the Brazilian economy through the promotion of a digital single market that better harmonizes federal, state, and municipal policies and practices to foster Brazilian competitiveness at a global level. For example, under Brazil's current legal framework and its implementing regulations, companies that have telecoms licenses and their affiliates are subject to certain restrictions on their ability to engage in the following activities (under Brazil's SeAC law):

- Controlling or holding more than 30% of Brazilian broadcasters, programmers or producers;
- Hiring national artistic talent or works of Brazilian authors, with the purpose of producing content for distribution by pay tv or broadcasting providers; and
- Acquiring rights to "events of national interest", also with the purpose of producing content for distribution by pay tv or broadcasting providers.

Such prohibitions can not only entail restrictions on FDI, but also harm competition and consumers' welfare. CSI urges USTR to request the Brazilian government to modernize the SeAC law by means either of a legislative process or the issuance of an Executive measure that eliminates Articles 5 and 6 of the Law.

Pay-TV Content Quotas: Effective September 2011, Law 12.485/2011 imposes local content quotas for Pay-TV, requiring every qualified channel (those airing films, series, and documentaries) to air at least 3.5 hours per week of Brazilian programming during primetime. It also requires that half of the content originate from independent local producers and that one-third of all qualified channels included in any Pay-TV package must be Brazilian. Implementing regulations limit eligibility for these quotas to works in which local producers are the majority IP rights owners, even where such works are co-productions, and regardless of the amount invested by non-Brazilian parties. These quotas were recently renewed until 2043.

Screen Quotas: Theatrical quotas were recently renewed until 2033. The obligations include exhibiting a minimum percentage of Brazilian works, proportional to the number of screens of the complex, and a minimum amount of different works simultaneously, also proportional to the number of screens. Moreover, theater complexes with between three and five screens cannot exhibit the same work in over 66% of the screenings of a day, while those with six or more screens cannot exhibit the same work in over 50% of the screenings of a day, preventing large theatrical releases from playing continually. Local content quotas limit consumer choice and can push consumers toward illegitimate content sources.

Video on Demand (VOD) Tax and Regulatory Framework: 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 pending in the Brazilian Congress that would extend the Condecine tax to VOD services and impose other obligations on VOD providers, such as catalogue quotas, prominence for local works, and transparency obligations. These bills – most notably #8889/2017 and #2331/2022 – could undermine the viability of providers, chill investment, and reduce consumer choice.

Video on Demand (VOD) Tax and Regulatory Framework: 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 *VOD services* and providers, 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. The bills also impose other obligations on video platforms, such as catalogue quotas, prominence for local works, prominent placement of Brazilian broadcasters on connected TV interfaces, and transparency obligations. These bills could undermine the viability of providers, chill investment, and reduce consumer choice.

Telecommunications:
In-country testing: As mentioned above, Brazil has put in place requirements that effectively require in-country testing for almost all information technology and telecommunications equipment sold into the market. These policies layer on additional costs and significantly delay time-to-market for U.S. providers. It also forces US providers to utilize contracting services to complete the complex device application process with ANATEL; further disrupting mutual business opportunities for Brazilian and US companies alike. A mutual recognition agreement (MRA) for telecom equipment would help solve this problem by allowing labs in each country to conduct testing according to the other country's regulations, precluding the need for localized testing. Brazil also maintains a number of local content requirements related to telecom equipment, including

preferential tax exemptions for locally made products, government procurement preferences for local technology, and requirements that participants in spectrum auctions use telecom equipment with specified portions of local content. The Brazilian government should dismantle such industrial policies, which unfairly hamper the competitiveness of U.S. companies in the Brazilian market.

Permanent Roaming: The Brazilian National Telecommunications Agency (ANATEL) employs a policy restricting the use of permanent roaming limiting it to 90 days by international machine-to-machine or Internet of Things service providers, with the result that U.S. providers must either invest in local service infrastructure or stay out of the market. This policy puts Brazil out of alignment with other major regulatory regimes that have opted to allow for M2M permanent roaming, with the goal of enabling globally harmonized service provision and avoiding fragmentation of the fast-developing M2M and IoT markets. Furthermore, the use of permanent roaming utilizes local telecom operator's resources for the service – thus increasing the economic potential for the telecom operators and for Brazil. Despite industry objections, after a public consultation process, ANATEL decided in 2018 that it would continue to prohibit permanent roaming.

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.

Network Usage Fee: There is an active debate in Brazil over network usage fees with the Brazilian Telecom Agency (ANATEL), telecom companies, and the Ministry of Communications pushing for their implementation. In 2023, ANATEL launched a public consultation that included a discussion on network usage fees to fund telecom infrastructure, with a follow-up consultation in June 2024. Since the consultation, ANATEL has reportedly drafted a proposal that would subject online service providers (OSPs) to telecom regulations. These OSPs are characterized as "large network users" and would include streaming, cloud, or tech companies, most of which are U.S.-based. The imposition of telecom regulations on these companies would come in contradiction with Brazilian law and practices. The proposal would result in a increase in disputes against OSPs that deliver much of the internet content to Brazilian consumers. By increasing disputes against U.S. service providers, large Brazilian telecom companies will be able to retrofit network fees into the existing online framework.

Currently in the legislature, Bill#469/2024 would prohibit network usage fees. We believe the adoption of such fees would severely impair competition in the Brazilian market (especially considering that ISPs frequently also offer audiovisual content), harm consumers, and negatively impact net neutrality

AI Bill: 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. 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. The ANPD plans to issue secondary rules on AI and data protection in late 2025. If the AI Bill passes, its regulatory scope will broaden to include general AI regulation. These broad obligations could disproportionately affect U.S. AI firms in Brazil, given the global nature of U.S. AI systems.

Ex-Ante Competition Legislation: In September 2025, the Brazilian government sent a proposal to Congress (Bill 4675) that would grant Brazil's competition authority (CADE) expanded powers to regulate online companies above a certain size. Inspired by European frameworks including the UK's Digital Markets, Competition and Consumers Act (DMCCA) and EU's Digital Markets Act (DMA), the bill gives CADE authority to designate companies as "systemically relevant" based on criteria including a revenue threshold of at least R$50 billion globally or R$5 billion in Brazil, operation of a multi-sided platform, and level of access to significant amounts of personal and business user data. The Finance Ministry has consistently said there will be no more than 5 to 10 designated companies but they will certainly include the DMA's "gatekeeper" companies, which are largely U.S.-based.

Designated companies may be subject to requirements such as mandatory notification of all mergers, a ban on self-preferencing, data transfers and interoperability, and a requirement to let users easily switch to competing services or install third-party apps. CADE is not required to show that such 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." The objectives of the legislation are broad and undefined, leaving CADE substantial discretion to potentially intervene in corporate operations. Designations will last for 10 years and apply to the entire company. Special obligations may be limited to specific services or products. Failure to comply with the obligations will result in penalties ranging from high fines to the potential break-up of a company.

Additional Ex Ante Competition Bills: Two other similar bills are also under consideration: Bill 2768, inspired by the DMA, which 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 it is hard to determine the specific obligations that would apply to U.S. companies, the bill would at minimum increase compliance costs and may require the restructuring of business operations.

Last, 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 on designated digital platforms.

Data Localization and Transfer Restrictions: 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.[3] 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.[4]

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.

More recently, Bill of Law No 4097, DE 2023, which would introduce new "digital sovereignty" measures into the General Data Protection Law, received first introduction in the Brazilian Congress. It appears to require IT companies providing services in Brazil to have a substantial percentage of Brazilian ownership and control (e.g., 25% of the voting share capital held by Brazilian nationals, be incorporated under Brazilian law or headquartered in Brazil).

Cloud services are required to have some types of government data localized under recent revisions to the Institutional Security Group. The Presidency of the Institutional Security Group (GSI), led by a military, published a Normative Instruction which establishes new rules for the contracting of cloud services by the Federal Public Administration. It established requirements for data and metadata residency exclusively in national territory in a few situations that are red flags for US digital services providers. These requirements disadvantage firms that provide services to the Brazil public sector but do not have the capacity to store data locally, and these guidelines set concerning precedents.

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.

Brazil also maintains a variety of data localization barriers in response to the weak competitiveness of its domestic tech industry. It provides tax incentives for locally sourced information and communication technology (ICT) goods and equipment (Basic Production Process (PPB) – Law 8387/91, Law 8248/91, and Ordinance 87/2013); it offers government procurement preferences for local ICT hardware and software (2014 Decrees 8184, 8185, 8186, 8194, and 2013 Decree 7903); and, it does not recognize the results of conformity assessment procedures performed outside of Brazil for equipment connected to telecommunications networks (ANATEL's Resolution 323).The GSI (Institutional Security Office) revised its cloud guidelines and determined that Government

data should have some types of data localized. While this is only applicable to government data and these are just guidelines this precedent raises serious concerns.[5]

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

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.

Electronic Payment Services (EPS): 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.

Insurance: A new insurance law was passed into December 2024 with implementing measures being drafted in Q1-Q2 2025. U.S. reinsurers are monitoring the drafting and will advocate for full cross border access. Local re-insurers receive preference in cession offers.

[5] Executive Office of the President, Office of the U.S. Trade Representative, "2016 National Trade Estimate," March 2016, https://ustr.gov/sites/default/files/2016-NTE-Report-FINAL.pdf, 69.

CIDE: The so-called Contribution for Intervention in the Economic Domain (CIDE) on remittances abroad is a tax mechanism established by Law 10.168/2000, primarily aimed at financing Brazilian technological development. This contribution applies to amounts paid, credited, delivered, used, or remitted to individuals or entities domiciled abroad as royalties and compensation for technical services. The legal provision seeks to foster national technological innovation through the taxation of transactions involving capital transfers abroad. The amendment introduced by Law 10.332/2001 significantly expanded the contribution's scope, covering a broader range of international transactions. This expansion has significantly raised transaction costs for U.S. companies operating in Brazil.

Taxation of Digital Products and Services: Brazil has been considering new taxes on digital products and services. On October 3, 2024, Brazil's Ministry of Finance issued Provisional Measure No. 1,262/24, a 15% minimum tax on multinationals operating in Brazil, described as a Social Contribution on Net Profit, ostensibly in line with the OECD's Pillar II scheme. While that the government has reportedly abandoned such plans[6], Brazil's actions on this matter should be monitored, as any future taxation could disproportionately impact U.S. digital products and services.[7]

[6] https://www.reuters.com/technology/brazil-holds-off-big-tech-tax-amid-trump-tariff-talks-say-sources-2025-03-26/
[7] *Brazil's Government Considers Taxing Big Techs if Revenue Falls Short*, Reuters (Sept. 2, 2024), https://www.reuters.com/world/americas/brazils-government-considers-taxing-big-techs-if-revenue-falls-short-2024-09-02/.

Cambodia

Local Testing Requirements: 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.

Content Moderation: Cambodia continues to face censorship, internet filtering, and blocking, with independent outlets often targeted during sensitive political events like the 2023 elections.[8] The government also been reported to silence critics through legal threats and forced public apologies.[9] A February 2021 sub-decree established the National Internet Gateway, creating a single point of entry for internet traffic.[10] A 2024 notification requires companies to use a national domain name[11], raising concerns about potential abuse for content blocking and restricting foreign digital services, similar to China's "Great Firewall".[12] Additionally, a draft Cybercrime bill from Cambodia's Interior Ministry could hold intermediaries liable for third-party content and mandate data localization.[13] 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" [14], with penalties including fines and

[8] *Freedom on the Net 2023: Cambodia*, Freedom House (2023), https://freedomhouse.org/country/cambodia/freedom-net/2023.
[9] https://freedomhouse.org/country/cambodia/freedom-net/2024.
[10] *Cambodia's New China-Style Internet Gateway Decried As Repression Tool*, REUTERS (Feb. 18, 2021), https://www.reuters.com/article/us-cambodia-internet/cambodias-new-china-style-internet-gateway-decried-as-repression-tool-idUSKBN2AI140.
[11] U.S. Department of State, *2024 Investment Climate Statements: Cambodia* (2024), https://www.state.gov/reports/2024-investment-climate-statements/cambodia/.
[12] *Cambodia: Internet Censorship, Control Expanded*, HUMAN RIGHTS WATCH (Feb. 18, 2021), https://www.hrw.org/news/2021/02/18/cambodia-internet-censorship-control-expanded; Internet Society, *Internet Impact Brief: Cambodia National Internet Gateway* (Feb. 18, 2022), https://www.internetsociety.org/resources/2022/internet-impact-brief-cambodia-national-internet-gateway/.
[13] Activists: Cambodia's Draft Cybercrime Law, VOA (Oct. 11, 2020) https://www.voanews.com/a/east-asia-pacific_activists-cambodias-draft-cybercrime-law-imperils-free-expression-privacy/6196959.html.
[14] Fiona Kelliher, *Leaked Law Proposal Would Give Cambodia Expanded Powers to Censor Critics*, Rest of World (Mar. 10, 2023), https://restofworld.org/2023/cybersecurity-law-draft-cambodia-elections/.

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 and Transfer Restrictions: 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.

Further, Cambodia released a draft Law on Personal Data Protection (LPDP)[15] 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.

[15] Available at: https://data.opendevelopmentcambodia.net/laws_record/draft-law-on-personal-data-protection.

Canada

While pleased with the modernizations in USMCA, CSI members are concerned with several services trade impediments listed below: These include:

Investment: USMCA eliminated the investor-state-dispute settlement provision for Canada and curtailed it with Mexico, so that most U.S. services suppliers can only access the ISDS mechanism through claims limited to breaches of a narrow set of obligations, direct expropriation and discriminatory treatment. Claimants must also pursue claims first through domestic courts for an extensive period of time. CSI is concerned with the roll-back of this important, de-politicized and effective dispute settlement remedy for investors, especially in light of the mandatory requirements of certain services sectors to invest abroad to reach clients and customers.

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 block 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.
The USMCA limits the ability of U.S. services providers to participate in government procurement opportunities in both Canada and Mexico, especially in financial and ICT services.

C-11 - Online Streaming Act: As part of the implementation of C11, (the *Online Streaming Act*)[16], which was enacted on April 27, 2023, the Canadian Radio-television and Telecommunications Commission (CRTC) requires that foreign, largely U.S.-based, streaming service providers with revenues over C$25M contribute 5% of their gross in-country revenue to a set of Canadian cultural funds to benefit Canadian content and creators. In its June 2024 policy document[17], the CRTC exempted Canadian-affiliated streaming players tied to domestic broadcasters, but imposed obligations on all other providers, video and audio alike; and while revenues from user-generated content, audiobooks, podcasts, and video game services were excluded, the policy document included subscription, advertising, and transactional video-on-demand revenues.

Despite U.S. streamers making substantial investments in producing content in Canada, this financial levy is scoped to target these U.S. companies and includes discriminatory qualifying factors that largely prevent them from accessing the funds to which the levy flows. Over the next two years, the CRTC will carry out a series of consultations, including to redefine Canadian content and settle on final contribution requirements that may go beyond the already onerous 5% revenue requirement and may include local content production and discoverability requirements. The *Online Streaming Act* is inconsistent with USMCA and the Government of Canada should ensure that the CRTC's implementation of the *Online Streaming Act* does not impose undue burdens or obligations on non-Canadian digital services, including by repealing the requirement for non-Canadian digital media services to pay 5% of Canadian gross broadcasting revenues to certain

[16] C-11, An Act to amend the Broadcasting Act and to make related and consequential amendments to other Acts, https://www.parl.ca/legisinfo/en/bill/44-1/c-11
[17] CRTC, CRTC 2024-121 (June 4, 2024), https://crtc.gc.ca/eng/archive/2024/2024-121.htm

funds. In total, the Online Streaming Act could cost the U.S. industry $7 billion by 2030.[18]

Quebec Bill 109: On May 21, 2025, Québec's Minister of Culture et des Communications (the 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.

Privacy: Bill C-27, which includes comprehensive federal privacy legislation, is currently being studied by the House of Commons Industry Committee. The bill aims to update Canada's current privacy law for the private sector, bringing it in closer alignment with European data protection and privacy standards, and introduces new privacy protections for minors. While the government has stated a desire to prioritize interoperability with new regulations, there is still work to be done at the committee level to ensure consistency and predictability for businesses operating across Canada. This includes introducing a consistent definition of a minor (which currently varies across provinces), adding clarity on consent exceptions, including the addition of advertising and marketing as a legitimate business activity, and confirming a 2-3-year implementation process. Once approved by the House of Commons Committee, the bill will be studied in the Senate.

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.[29] 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[19] on its discussion paper on AI and competition[20] will need to be monitored. The paper is part of the Bureau's broader inquiry on how

[18] https://ccianet.org/wp-content/uploads/2025/09/Cost-of-Canadas-Online-Streaming-Act.pdf
[19] Government of Canada, Feedback Form – Artificial Intelligence and Competition: Discussion Paper (2024), https://competition-bureau.canada.ca/feedback-form-artificial-intelligence-and-competition-discussion-paper.
[20] Government of Canada, *Artificial Intelligence and Competition Discussion Paper – March 2024* (Mar. 20, 2024), https://competition-bureau.canada.ca/how-we-foster-competition/education-and-outreach/artificial-intelligence-and-competition.

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.

Data Localization: The Province of Quebec adopted privacy legislation, known as Bill 64, in September 2021 that would make data transfers extremely difficult. . 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.[21]

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.[22] There are a number of concerns with this approach. 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.[23] 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.

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.

C-2 – Stronger Borders Act: The Canadian government is proposing new legislation for border security. If enacted, C-2 includes the following provisions: 1) Law enforcement and intelligence agencies will be authorized to make warrantless "information demands" to compel non-content information from service providers; 2) Productions orders for subscriber information; 3) Cross-border data sharing provisions which authorize enforcement of foreign decisions to compel

[21] U.S. International Trade Commission, *The Year in Trade 2021 – Operation of the Trade Agreements Program*, https://www.usitc.gov/publications/332/pub5349.pdf at 184.
[22] *Federal privacy reform: Where we left off and what's next*, Gowling WLG (September 26, 2025), https://gowlingwlg.com/en/insights-resources/articles/2025/federal-privacy-reform.
[23] Government of Canada, *Request for Information – Sovereign Public Cloud Capability*, https://canadabuys.canada.ca/en/tender-opportunities/tender-notice/cb-416-17296820

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.

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.[24] 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.[25] 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.[26]

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.[27] While the consultation is officially complete, this process is advancing in concert with pending federal legislation, specifically Bill S-209[28], 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.

---

[24] Government of Canada, *The Government's Proposed Approach to Address Harmful Content Online,* https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html.

[25] Government of Canada, *Proposed Bill to Address Online Harms*, https://www.canada.ca/en/canadian-heritage/services/online-harms.html; and House of Commons of Canada, Bill C-63, https://www.parl.ca/DocumentViewer/en/44-1/bill/C-63/first-reading.

[26] https://www.cbc.ca/news/politics/liberals-taking-fresh-look-at-online-harms-bill-says-justice-minister-sean-fraser-1.7573791

[27] Office of the Privacy Commissioner of Canada, *Consultation on age assurance*, https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-age/

[28] Senate of Canada Bill S-209, *An Act to restrict young persons' online access to pornographic material,* https://www.parl.ca/legisinfo/en/bill/45-1/s-209#:~:text=S%2D209%2045th%20Parliament%2C%201st,June%2012%2C%202025%20(Senate)

Digital Taxes: Canada announced on June 29, 2025 the planned repeal of its Digital Services Tax (DST) before its first collection. The DST, adopted Jun 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.

Additionally, Canada's Bill C-18 (the Online News Act) enacted in June 2023[29], empowers t he 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[30] and the Parliamentary Budget Offices 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.[31] 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[32], while the other U.S. company ceased news linking in Canada. The law harms the user access to the open Internet and threatens security and safety[33]. 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.[34] 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.[35]

[29] C-18, *An Act respecting online communications platforms that make news content available to persons in Canada*, https://www.parl.ca/LegisInfo/en/bill/44-1/C-18.
[30] House of Commons Debates, May 13, 2022, https://www.ourcommons.ca/DocumentViewer/en/44-1/house/sitting-71/hansard#11685803
[31] Office of the Parliamentary Budget Officer, *Cost Estimate for Bill C-18: Online News* Act, https://www.pbo-dpb.ca/en/publications/RP-2223-017-M--cost-estimate-bill-c-18-online-news-act--estimation-couts-lies-projet-loi-c-18-loi-nouvelles-ligne
[32] https://www.canada.ca/en/radio-television-telecommunications/news/2024/10/crtc-approves-googles-application-and-paves-way-for-annual-100-million-contribution-to-canadian-news-organizations.html
[33] Internet Society, *Case Study: Canada's Online News Act Hurt Journalism, Competition, and the Internet* (Sept. 24, 2024), https://www.internetsociety.org/resources/doc/2024/case-study-canadas-online-news-act-hurt-journalism-competition-and-the-internet/.
[34] CCIA White Paper on Canada's Bill C-18, the "Online News Act" (Sept. 2022), https://www.ccianet.org/wp-content/uploads/2022/09/CCIA-White-Paper-on-Canadas-Bill-C-18-the-Online-News-Act.pdf.
[35] https://nationalpost.com/news/politics/carney-suggests-hes-considering-rescinding-online-news-act.

Chile

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.

Additionally, Chile approved a new Personal Data Protection Law[36] 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.

Digital Regulatory Landscape: 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,*

[36] *Ley que Regula La Protección y el Tratamiento de Los Datos Personales y Crea La Agencia de Protección de Datos Personales* (Law no. 21719; https://www.bcn.cl/leychile/navegar?idNorma=1209272), amending the earlier *Ley sobre Protección de La Vida Privada* (Law no. 19628; https://www.bcn.cl/leychile/navegar?idNorma=141599).

through, if possible, electronic means".[37] However, the current customs systems cannot process all the data from different carriers, causing delays at the border. 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.

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.

Potential Barriers in New Cybersecurity Framework Law: Chile recently approved a new Cybersecurity Framework Law (in effect as of March 1, 2025)[38], 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.

[37] Article 5.7. express shipments.
[38] *Ley Marco de Ciberseguridad* (Law no. 21663; https://www.bcn.cl/leychile/navegar?idNorma=1202434).

China

America First Trade Policy investigations

President Trump's "America First Trade Policy" memo calls for investigating PRC practices that are unreasonable, discriminatory and burdensome, as well as assessing China's compliance with commitments made in the bilateral Phase One Agreement signed in the first Trump administration.

US services exports face a complex network of trade barriers in China, some of which may be addressed through remedies based on these investigations and others through enforcement of China's unfulfilled commitments under Phase One. We are agnostic as to forum and encourage USTR to pursue enforcement through whatever mechanism it considers most appropriate.

As the US engages in bilateral trade discussions with China, we strongly urge the administration to include services trade on the negotiating table. Such talks could include enforcement of any outstanding services commitments under Phase One as a prerequisite for further negotiations.

The United States currently enjoys a significant trade surplus in services with China of $33.1 billion, up 24 percent from the prior year[39]—helping offset the substantial goods deficit. But we believe the surplus could be considerably larger if US services suppliers enjoyed fair market access in China.

It's important to acknowledge that as the bilateral relationship has grown more strained, China has increasingly resorted to coercive and at times threatening tactics against individual US companies operating in its market. We hope the administration will squarely address these issues, as well as ongoing sectoral concerns, all of which we have described below.

Macro trade concerns

As bilateral tensions have grown, Beijing has applied selective pressure to US companies through targeted regulatory enforcement and anti-monopoly investigations. Such actions are arbitrary and deliberately intimidating to American business. Another favored means of economic coercion is China's abuse of export controls on critical minerals. This includes a number of minerals for which China is the dominant supplier, leaving US companies with extremely limited alternatives for purchase.

China also continues to exert tight control over data, including data used for routine commercial purposes. Although the government has made some moves to ease up on data restrictions, cross-border data transfers for business remain needlessly burdensome, especially given the lack of a clear national security justification.

In addition, Beijing has continued to promote the use of local standards developed without opportunity for foreign stakeholder input, which deter purchases of US products built around international standards.

---

[39] Bureau of Economic Analysis, Commerce Department. Table 2.2. U.S. Trade in Services, by Type of Service and by Country or Affiliation, July 2025,
https://apps.bea.gov/iTable/?reqid=62&step=9&isuri=1&product=4#eyJhcHBpZCI6NjIsInN0ZXBzIjpbMSw5LDEwLDQsOF0sImRhdGEiOltbInByb2R1Y3QiLCI0Il0sWyJUYWJsZUxpc3QiLCIzMDU2OCJdLFsiVGFibGVMaXN0U2Vjb25kYXJ5IiwiMzA1NjgiXSxbIkZpbHRlcl8jMSIsWyIxIl1dLFsiRmlsdGVyXyMyIixbIjAiLCIxIiwiMiIsIjMiXV0sWyJGaWx0ZXJfIzMiLFsiMSJdXSxbIkZpbHRlcl8jNCIsWyI3MyJdXSxbIkZpbHRlcl8jNSIsWyIwIl1dXX0=

To restore a measure of fairness to bilateral trade, China should be required to cease singling out and intimidating US companies through selective regulatory enforcement; punitively cutting off supplies of vital critical minerals; bottlenecking commercial data; and stacking the deck against international standards.

Phase One Agreement

In the Phase One Agreement Beijing agreed to expand purchases of U.S. goods and services; further open markets in areas including financial services and electronic payment services; ban forced technology transfer; and improve IP protections, among other commitments. While China has met a number of its commitments related to financial services, it has not yet met its commitment to advance pending applications from all U.S. electronic payment services (EPS) suppliers for a bank card clearing institution (BCCI) license. China should promptly complete the approvals required for all pending applicants to obtain a BCCI license.

And Beijing has fallen short on delivering in other commitments of the agreement, notably on services purchases. The agreement called for China to purchase at least $12.8 billion additional services in the first year of implementation and $25.1 billion after that[40]. In practice, however, US services exports to China declined sharply immediately after the agreement was signed, reaching only an estimated 54 percent of the mandated level[41]. To be sure, travel restrictions related to COVID sharply impacted Chinese purchases in areas such as tourism and business travel as well as educational services. Beyond those categories, though, we believe protectionist Chinese policies constrained the sale of other US services. In that sense, some of the market distortions facing US service suppliers could be addressed within the context of Phase One Agreement consultations and enforcement.

***

Additional Trade Concerns

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 since 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

[40] The Phase One Agreement committed China to purchase US services exports in the categories of charges for use of IP; business travel and tourism; financial services and insurance; other services; and cloud and related services.
[41] "China bought none of the extra $200 billion of US exports in Trump's trade deal," Peterson Institute of International Economics, Chad Bown, July 19, 2022, https://www.piie.com/blogs/realtime-economics/2022/china-bought-none-extra-200-billion-us-exports-trumps-trade-deal

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 for 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, to 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.

Electronic Payment Services: China has not acted in accordance with its U.S.-China Economic and Trade Agreement Article 4.4 obligations to ensure that its regulatory authorities operate an improved and timely licensing process for U.S. suppliers of electronic payment services so as to facilitate their access to China's market. As of March 2025, only two U.S. EPS suppliers had secured the license to operate in the domestic market. China should promptly complete the approvals required for all pending applicants to obtain a Bank Card Clearing Institution (BCCI) license.

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" ICT 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 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.

Protectionist Procurement: US ICT companies report that State-Owned Enterprises have sharply reduced their purchase of American ICT hardware, software and services. The goal is to accelerate the indigenization of the Chinese technology stack by reducing or prohibiting purchases of U.S. technology. To that end, in 2022, The Chinese Communist Party issued "Document 79" directing SOEs to reduce purchases of foreign hardware and software (particularly from U.S. companies) in favor of domestic suppliers. The Document was reportedly so secret that only high-ranking officials were sh own it. Consequently, procurement practices have become more aggressive in the effort to "Delete A," industry shorthand for "Delete America." This in turn has led to the broad decline in sales in China for major U.S. technology companies for hardware, software and services.

Cryptography Law China's *Cryptography Law,* enacted on October 26, 2019, and effective starting January 1, 2020, classifies encryption into three categories: "core," "common," and "commercial" encryption. "Core" and "common" encryption categories are used to protect information considered to be "state secrets," while commercial encryption is used to protect information that is not a state secret.

In April 2023, *Commercial Cryptography Administrative Regulations* was amended. The amended regulations a) fail to support the interoperability of inter-national standards and use of internationally standardized encryption algorithms; b) suggest an extensive import license/export control scheme; c) include ambiguous clauses that potentially enforce a de facto mandatory certification instead of a voluntary one; and d) impose requirements applicable only to CII and Party and government organs to networks above 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. This concept could be interpreted broadly to cover massive networks including Multi-Level Protection Scheme ("MLPS") level three, as we have already seen in some local governments. If the above issues are not

clarified, the regulations will impose high compliance cost and create entry barrier for MNCs who heavily rely on encryption algorithms that comport with international standards.

Cloud Services: China's accession to the WTO permitted it to maintain foreign equity limits on value-added and basic telecommunications services that restricted market access for foreign suppliers. Although there was expectation that China would eventually open up the sector to greater foreign participation, that has yet to occur, and, in fact, China has classified a number of new services as telecommunications services and limited foreign participation in emerging digital services.

China's publication of a Telecom Services Catalog in December 2015 expanded regulation and market access barriers to a host of new services not typically regulated, including cloud computing, content delivery networks, and online platforms (under a broadly written provision for Information Services). China currently imposes a 50 percent equity cap on foreign investment in value-added telecommunications services. Although the Ministry of Industry and Information Technology announced the expansion of the opening-up of the VAS sector on a pilot basis in April 2024, the opening-up is only limited to four designated areas, posing difficulties for cloud service providers with interconnected data centers both inside and outside those areas.

It is critical that MIIT interpret the definition of VAS in a manner that is consistent with China's explicit WTO commitment and widely accepted international standards. Replacing these conservatively applied vertical service classifications with more objective and transparent guidelines for Type I (facilities-based) and Type II (non-facilities based) services would allow more foreign carriers to invest in China, which eventually would stimulate economic growth in the Chinese market.

China also 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. 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).

Telecommunications: Under the Basic Service license regime, China limits foreign equity stakes to 49 percent in basic telecommunications services. It also mandates that foreign companies select a state-owned and licensed telecom company as a joint venture partner. These requirements serve as a significant market access barrier from an operational and economic perspective. Service providers are unable to establish operational control, protect their brand, and deliver services in China that are seamlessly integrated into global network offerings.

Foreign entities established as joint ventures become a horizontal competitor of their joint venture local operator, eroding the value of the investment. USTR should encourage China to remove this provision and allow foreign companies to partner with any legally operating telecom entity they find suitable.

The Chinese government also imposes strict limitations on non-Chinese companies that wish to offer Voice over Internet Protocol (VoIP) services in China. No non-Chinese company may offer any kind of VoIP service in China, since VoIP requires a VAS license that foreign companies may obtain only through a joint venture with a Chinese company. Connection to the public switched telephone

network (PSTN) requires a basic service license. Only a few small pilot VoIP projects -- involving the dominant Chinese telecom operators -- are allowed to offer PSTN-interconnected VoIP services to Chinese consumers. USTR should urge the Chinese government to remove restrictions in the efficient use of IP technologies, including voice applications.

We urge USTR to encourage China to take the following steps to remove the bottlenecks to development of value- added services in China:

- Approve the use of ICT software used by financial services and other service providers
- Adopt approaches that enable cross border data flows and enable the use of global standards in a manner that supports an international, interoperable policy framework;
- Take an open approach to value added services, streamlining licensing requirements. Expand the list of value-added services in the Catalogue to include such services as managed International IP VPN, in conformity with international standards for categorizing basic and value-added services while eliminating cloud computing, content delivery networks, and information services from the catalog and the licensing requirements;
- Lift the prohibition on resale, enabling all carriers to acquire capacity at wholesale rates and interconnect their networks to deliver services to a broader reach of the country;
- Remove remaining caps to Foreign Direct Investment (as noted above), and
- Allow full market access for resale of mobile services.

Financial Services: China made extensive commitments to open its financial services market in the Phase One Agreement, in which Beijing set out timelines to make e-payment licensing decisions, remove equity caps in securities, fund management and futures, and allow wholly owned foreign enterprises in sectors including life and health insurance. China has made some progress in market opening, although substantial further reforms are needed.

Insurance: In the phase-one deal China made important commitments to open its insurance market, including the removal of equity caps for life and health insurance, but more work remains to clarify and fully effectuate those reforms. Foreign insurers have less than an eight percent cumulative market share in the third largest market in the world. Furthermore, with the exception of aviation, aerospace, nuclear, oil and credit reinsurance contracts, the amount of proportional business ceded to any one reinsurer in respect of any one risk may not exceed 80% of the sum insured or liability limit of the direct insurance policy. The amount of each facultative cession to an affiliated company of the cedant may not exceed 20% percent of the sum insured or limit of liability of the direct insurance policy.

Express Delivery: China has blocked foreign companies' full access to China's domestic letter and document market, also applying overly burdensome regulatory approaches in China's domestic express delivery market. One such example is the requirement for 100 percent open box inspection, x-ray inspection and shipper ID check for all express shipments. A related risk is that Chinese authorities may inspect shipments and seize legitimate goods when they are merely being routed through China, even if it is not the final destination. Also, express operators are required to have registrations with Post authorities at the local city level. It is very burdensome for operators to obtain and maintain the registrations, given the number of cities in the express network.

Audiovisual: Import Quotas/Revenue Share – China continues to maintain an official quota of 34 foreign revenue-sharing films per year. It has not complied with the commitment it made in 2017 to meaningfully increase compensation for filmmakers, and the current 25 percent share of revenue earmarked for US suppliers is far below comparable markets and the international norm. (In practice, because distributors deduct ticket distribution fees before calculating the U.S. studio share, the allocation amounts to even less than 25 percent of revenue.)

Government Film Importation and Distribution Monopoly – The China Film Administration (CFA) still permits only one film importer and two distributors of foreign films, both of which are state-owned companies. While China affirmed in the 2012 Film MOU that any properly licensed Chinese enterprise may distribute imported films, CFA has yet to approve any new private distributors. China Film Group also determines the release dates and length of theatrical runs of foreign films, often restricting the ability of U.S. producers to obtain the full commercial value of the film.

Blackout Periods During Peak Seasons – In order to prevent competition against domestic films released during peak movie-going periods, the Chinese government has historically implemented a "blackout" during which no new foreign imported films may be released. Such blackouts typically occur either during national, school, and summer holidays, or coincide with political events. Restricting the release of new foreign imported titles during peak season and day-and-date releases not only drives down theatrical revenues but also contributes to increased unauthorized consumption, as piracy websites and services meet consumer demand for foreign blockbuster titles.

Online Video Restrictions –Chinese websites are required to cap distribution of foreign content to a maximum of 30 percent of the total. Of total foreign content – which is further limited by country and genre -- U.S. content is restricted to less than 10 percent in real market terms. The content review process allows only two windows each year for online distributors to submit content for registration and censorship review and requires foreign TV series to be submitted as complete seasons, versus the global market practice of per episode submissions. These rules have substantially reduced the number of U.S. TV programs licensed in China.

Censorship: Beijing actively censors cross-border internet traffic, blocking some 3000 sites and services, including that of many American online services.

Colombia

Digital Services Tax: In December 2022, Colombia enacted tax reforms under Law 2277 of 2022, introducing a significant economic presence (SEP) concept for imposing income tax for the sale of tangible goods and certain digital services, such as cloud service. For both goods and services, an entity will be in-scope if it has a deliberate and systematic interaction with the Colombian market, defined as interacting with 300,000 or more users or customers located in Colombia. Further, an entity will be in scope if it earns a gross income of roughly $300,000 or more from consumers within Colombia. The tax reforms impose a new 10% withholding tax on gross income from overseas providers of goods and digital services.[42] A non-resident can, if it registers in Colombia, avail itself of an alternative, a 3% declarative tax on the gross income from sales of goods and/or digital services. However, this optional declarative gross-basis tax for non-residents is not transferrable to customers (like a value-added or consumption-based tax). The SEP rule entered into force on January 1, 2024, and is currently being applied to US technology companies operating within the country, making it the first country into the Latin American region to impose a DST.

Further compounding the uncertainty, the tax reform bill submitted to Congress by the Government on September 1, 2025, includes a provision (Article 12) that would increase the optional, declarative gross-basis tax for non-residents opting for this mechanism, from the current 3% rate to 5% on the gross income from sales of goods and/or digital services. Moreover, the latest tax reform bill also includes a provision that eliminates the VAT exclusion that a prior 2018 reform had established for cloud computing services, a measure which reflects a governmental inclination to discourage cloud services in favor of on-premise solutions.

Colombia's implementation and proposed expansion of its DST represents a significant trade barrier that disproportionately affects U.S. companies. 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. The measure would also impede U.S. sales of goods and services, likely causing double taxation due to the lack of a U.S.-Colombia tax treaty. It is also likely to violate Colombia's WTO and U.S.-Colombia Trade Promotion Agreement obligations by discriminating against U.S. suppliers.

Electronic Payment Services: While the new tax regulation establishes income, VAT and other municipal withholding taxes applicable to credential payments, it 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 in the process of being implemented, 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

[42] KPMG, *Colombia – Law 2277 of 2022 Tax Reform* (2022), https://assets.kpmg.com/content/dam/kpmg/us/pdf/2022/12/tnf-colombia-dec19-2022.pdf.

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 payments methods (cash, QR, transfers) and prevents the fully successful deployment of US credential companies in the country's payment ecosystem.

Banking: In implementing the Large Exposures framework and in accordance with the provisions issued by the Financial Superintendency, financial institutions have identified an issue in the calculation of bank balances that has had significant adverse effects across the financial sector and materially impacts the foreign exchange (FX) market. Decree 2555 establishes that the calculation of the large exposure limit must include all assets used in the calculation of assets by credit risk level for solvency purposes. For these purposes, it has been established that, although bank balances are weighted at 0% for solvency margin purposes, they must be computed for the purposes of the large exposure limit based on the gross value of the balance.

Requiring these transactions to be fully computed within the individual exposure limit forces entities to underutilize solid counterparties solely for regulatory reasons, generating significant operational risk and jeopardizing the scalability of operations, the normal functioning of payment systems, and transaction clearing, among others.In Colombia, banks are forced to maintain accounts abroad to execute their proprietary transactions, such as foreign exchange purchase and sale transactions with their clients, since the Central Bank of the Republic does not offer foreign currency account services.

Bank balances should be excluded from the Large Exposure limit. The Regulator could establish requirements or conditions for the account or entity holding the balance, whether local or foreign, to consider them ineligible for Large Exposures, as has been done in Mexico and Brazil, or delegate the definition of such conditions to the Financial Superintendency.

Trade Facilitation: Under the USCTPA, Colombia committed to modernize their customs procedures through automation and the use of electronic systems. For example: Article 5.3 states that each party shall "provide for electronic submission and processing of information and data before arrival of the shipment to allow for the release of goods on arrival" and "employ electronic or automated systems for risk analysis and targeting." Colombia also committed to adopt expedited customs procedures for express shipments, including the full incorporation of express shipments into Colombia's Single Window (Articles 5.2, 5.3, and 5.7). This includes providing for the submission and processing of information necessary for the release of an express shipment before the express shipment arrives, as well as allowing for a single manifest through electronic means, if possible. However, the Colombian government have yet to implement these commitments and still require physical documents at the border.

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.

Cloud Procurement Uncertainty: Colombia's public cloud procurement framework is becoming increasingly erratic, harming U.S. cloud providers. The Public Cloud Framework Agreement (AMP V) is indefinitely delayed, and its predecessor (AMP IV) expired without extension, causing "digital paralysis" for new services. Adding to the confusion, CCE's original plan for AMP V introduced a mixed system aiming to make "Nube Pública Hiperescala" (Segment 1, for global CSPs like Google, Microsoft, Oracle and AWS) and "Nube Pública Abierta" (Segment 2, for smaller, local/hybrid cloud providers) compete under unclear terms. This segmentation itself presented challenges by creating artificial divisions. More recently, however, CCE has signaled an intent to temporarily eliminate the local or open cloud segment (Segment 2), ostensibly to move forward with the bid for public cloud services (Segment 1), with an intention to introduce new offerors in the private and hybrid cloud market later in time. This constant shifting of terms and the lack of a clear, stable framework fundamentally undermine planning and fair competition.

Simultaneously, Presidential Directive No. 06 (August 13, 2025) instructs public entities to leverage Internexa S.A., a state-controlled company, for technology procurements. This move is seen as favoring Chinese Huawei cloud products, bypassing competitive bidding and contradicting existing laws promoting transparency and free competition. This Directive unilaterally establishes a preference without a competitive process, severely distorting the market. To further entrench these practices, CCE has published a draft bill ("*Proyecto de Ley No. - Por el cual se dictan disposiciones para la Compra Pública para la Innovación*") that would fundamentally alter the public procurement legal framework. This bill seeks to justify circumventing mandatory public cloud framework agreements by creating new pathways for "Public Procurement for Innovation" that could be used to directly contract with specific providers like Internexa. This legislative proposal would undermine the legal obligation to use framework agreements, further eroding transparency and competitive principles, to the detriment of established U.S. cloud service providers.

These actions, procedural irregularities, and legislative attempts to bypass established rules demonstrate a profound erosion of transparency and the rule of law, making the market opaque, unpredictable, and highly discriminatory against U.S. service providers. This environment creates risks of compromised cybersecurity standards and makes long-term investment difficult due to constant uncertainty.

Costa Rica

Electronic Payments: U.S. EPS firms face two major barriers in the Costa Rican market. First, 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.

We respectfully urge USTR to ask 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.

Secondly, tax withholdings on card payments continue to create an uneven playing field for U.S. EPS providers. And 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 the 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

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 USD20.000, 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.

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, 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 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.

Banking: Ecuador’s financial regulatory framework presents several challenges for U.S. and other foreign financial institutions. Settlement rules in Ecuador do not provide exceptions for derivatives transactions—either for committed flows or for margin and collateral—and the limited development of derivatives regulation, including the absence of netting provisions for derivatives positions, constrains financial institutions’ ability to manage risk and operate efficiently in the market. The government should adopt a more mature and comprehensive regulatory framework for derivatives, including clear netting provisions and settlement flexibility aligned with international best practices.

In addition, foreign bank branches are subject to differential regulatory treatment compared to local banks. Current regulations do not permit operations above 20 percent of capital, even when such operations are fully guaranteed by solvent foreign institutions. Moreover, no framework exists for branches to reduce capital—a measure available to subsidiaries and previously exercised within the system. This asymmetry creates an uneven playing field and limits operational flexibility for foreign institutions. The government should ensure equitable treatment of foreign bank branches and subsidiaries by allowing capital reductions and operations above 20 percent when backed by guarantees from solvent foreign entities, subject to regulatory approval.

Egypt

Electronic Payment Services: The Central Bank of Egypt's (CBE) co-badge mandate for payment cards has created challenges in aligning its policy objectives with the market-led principles required for a sustainable partnership, leading to a pause in negotiations. A collaborative approach to developing mutually beneficial commercial terms is essential for a successful outcome.

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).[43]Additionally, in May 2020, Decree No. 26 of 2020 [44]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 [45]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[46] 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.

Data Localization and Transfer Restrictions: The Personal Data Protection Law, which aims to regulate data collection, processing, and storage, is awaiting the release of its Executive Regulations (ERs)[47]. These ERs, initially anticipated in early 2025, will provide businesses with specific compliance guidelines and introduce a one-year transition period after issuance. The

[43] *Law on the Organisation of Press, Media, and the Supreme Council of Media,* https://www.article19.org/wp-content/uploads/2019/03/Egypt-Law-analysis-Final-Nov-2018.pdf
[44] *Egypt's new press and media regulation era*, Soliman, Hashish & Partners (June 6, 2020), https://www.shandpartners.com/egypts-new-press-and-media-regulation-era/
[45] R*egulating Websites and Platforms in Egypt: Compliance Requirements*, Al Tamimi & Co (Jun 24, 2024), https://www.tamimi.com/news/regulating-websites-and-platforms-in-egypt-compliance-requirements/
[46] https://issuu.com/decree_no_92_of_2020/docs/_
[47] *Data Protection Laws and Regulations Egypt 2025*, International Comparative Legal Guides, https://iclg.com/practice-areas/data-protection-laws-and-regulations/egypt

delay in their release, reportedly due to recent political and crisis management priorities, has left businesses in a state of uncertainty.

Additional E-Commerce Barriers: Egypt's import regime is marked by inconsistent application and a lack of transparency in its customs processes, creating significant barriers for businesses, particularly smaller e-commerce firms and those engaging in cross-border trade. For instance, customs valuation practices often deviate[48] from WTO-compliant methodologies, with declared values on commercial invoices— even those sealed by the Chamber of Commerce in the country of origin—frequently disregarded. Discrepancies in Harmonized System (HS) codes can lead to goods being reclassified under higher tariff categories, and specific practices, such as a 50% value uplift on spare parts under service contracts, further inflate costs. Such inconsistencies, coupled with fines equal to the levied tariffs and the additional costs associated with protesting valuations, undermine predictability and efficiency in the import process.

In addition, businesses wishing to import goods into Egypt face [49]stringent registration requirements, including the need to establish a permanent establishment (PE) in the country. The Simplified Vendor Registration System obligates non-resident firms to register with the Egyptian Tax Authority, while PE rules define a PE as any fixed place of business or service operation lasting over 90 days in a 12-month period. These requirements, which also include navigating complex tax obligations and avoiding inadvertent PE triggers, place a significant administrative and financial burden on smaller e-commerce businesses. For many, the lack of resources and expertise to comply with these regulations restricts their ability to enter and compete in the Egyptian market. Together, these challenges create an unpredictable trade environment and limit opportunities for smaller businesses to benefit from Egypt's growing digital and regional shipping potential.

[48] *Inconsistent customs valuation of imports in different ports*, European Commission Access2Markets (updated Apr 29, 2025), https://trade.ec.europa.eu/access-to-markets/nl/barriers/details?isSps=false&barrier_id=14222
[49] *Doing Business in Egypt 2024, A Tax and Legal Guide*, PwC (2024), https://www.pwc.com/m1/en/tax/documents/doing-business-guides/dbie.pdf

Ethiopia

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.

European Union (EU)

The US-EU joint statement on a framework for reciprocal trade issued in August 2025 includes a joint commitment to address unjustified digital trade barriers commitment. Unfortunately, we understand the EU has interpreted this reference in narrow terms, contending that it relates only to two specific commitments that directly follow in the text of the joint statement (i.e., that the EU will not impose network usage fees and that it will support a multilateral moratorium on duties on e-commerce). As we detail below, there are a number of significant digital trade barriers that US companies face in the EU, and we hope the framework will provide a means for USTR to address these obstacles.

We are concerned by the growing number of EU digital policies that appear intended to favor domestic firms at the expense of U.S. companies amid a renewed push for digital (or data, or technological) sovereignty. In practice, policies premised on promoting sovereignty often have a protectionist impact and diminish U.S. market access.

The Data Privacy Framework that allows for the transfer of EU personal data has been vital in facilitating cross-Atlantic data transfers, and protecting the framework and its underlying mechanisms will be key to sustaining American export competitiveness. We urge the administration to provide continued support for the mechanisms that underlie the framework, including through the appointment of new board members to ensure a fully functioning Privacy and Civil Liberties Oversight Board.

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.

Digital Markets Act (DMA): Adopted on Sep 14, 2022 and applicable since May 2, 2023, the DMA[50] requires "core platform services" to notify the European Commission if they meet certain thresholds. These thresholds disproportionately affect U.S. tech companies, while excluding European rivals, thus shielding major European firms in media, communications, retailing and advertising from the DMA's highly prescriptive and burdensome obligations. Although the original intent was to designate up to 25 companies as so-called "gatekeepers" under the DMA (a number that would have likely swept in European operators)[51], the European Commission ultimately only designated six companies, and 22 of their services, as subject to the new rules – with five out of

[50] Official Journal of the European Union (Oct. 12, 2022), https://eur-lex.europa.eu/eli/reg/2022/1925.
[51] See "Opinion of the Board," p. 10 at https://digital-strategy.ec.europa.eu/en/library/impact-assessment-digital-markets-act.

those six companies (the sixth is Chinese) and 21 of the 22 services being American.[52] That list remains unchanged.

Under the DMA, European Commission has carved out a role in which its regulators are permitted to override corporate strategy and mandate product redesigns on an ongoing basis. With the ostensible goal to end what it calls "self-preferencing," the DMA has prohibited "gatekeepers" 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, US 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. Even so, EU regulators have kept moving the goalposts for compliance, continuing to push for continual changes that incur ever-increasing costs for US firms.

Companies may be fined up to 10 percent of total global (not just European) revenue and 20 percent for what are deemed to be repeat violations. 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).[53]

In an approach antithetical to the spirit of competition, the EC has also openly solicited input from EU competitors as part of public workshops on how "gatekeepers" should alter their products. The result is that US companies have had to revise business models in ways that advantage their rivals. Under the law, US firms have also been forced to share data with rivals, a requirement that has created substantial new privacy and security risks for digital consumers in the EU. Moreover, so far the only companies to be subjected to EC investigations under the DMA are American (Alphabet, Apple and Meta).

Because of confusion and uncertainty stemming from the subjective nature of DMA enforcement, US service providers have for now opted to block or delay the integration of new AI-powered services into their products in the EU. The risk appears too high that such services may be viewed as a form of self-preferencing or other behavior subject to penalty under the DMA. We are also concerned that an official EU review of the DMA could expand its scope to more explicitly cover services including AI and cloud.

In short, the implementation of the DMA has proven needlessly complex and extremely costly. We hope it may be possible to find ways to ease the compliance burden on innovative companies.

Digital Services Tax: The Tax Foundation notes that "currently, about half of all European OECD countries have either announced, proposed, or implemented a DST." As the OECD BEPS Pillar 1 negotiations have reached an impasse, many EU Member states that do not currently have a DST are seeking to reinstate discussion of a Directive on the common system of a digital services tax on

[52] European Commission, *Gatekeepers* (last updated Oct. 14, 2024), https://digital-markets-act-cases.ec.europa.eu/gatekeepers.
[53] See https://ccianet.org/wp-content/uploads/2025/03/CCIA_EU-Digital-Regulation-Factsheet_reportfinal.pdf

revenues resulting from the provision of certain digital services and possibly on a corporate tax of a "significant digital presence." Both measures have been blocked during the Pillar 1 negotiations.[54]

The imposition of DSTs and the potential adoption or expansion of measures at the EU level or by individual Member States continue to pose challenges for U.S. service providers. We encourage the USTR to continue using Section 301 investigations and the 2026 NTE to address the significant trade-related concerns posed by all unilateral digital services taxation measures and similar measures, including those adopted or under consideration to date in the following jurisdictions:

Austria: Effective January 1, 2020, the Austria DST imposes a 5% tax on revenue generated by digital advertising services supplied in Austria; in-scope companies have global revenue exceeding €750 million and revenue from supplying digital advertising services in Austria exceeding EUR 25 million. The Austrian government directs some of the resulting revenue to subsidize Austrian media companies by way of a digitalization fund.

Belgium: In 2025, the new 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: 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: The Czechian government proposed in 2019 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.

France: At the end of October 2025, the French National Assembly voted to double the French DST from its current 3% to a new rate of 6%. Though the rate hike still needs to be approved by the Senate, such a move would set an alarming precedent that would be likely to influence other governments around the world. French politicians have made clear that the proposed higher tax rate is targeted at a small number of American companies. The latest development marks a further escalation, reflecting a political push to substantially increase what is already an unreasonable baseline tax.

Since 2019, France has imposed a 3% DST on gross revenues generated from digital platform services and the sale of advertising space and digital data. The threshold is for companies with

[54] https://taxfoundation.org/data/all/eu/digital-services-taxes-europe

worldwide revenue of €750 million and local revenue of €25 million. France has also imposed since 2017 a tax on video content ("TVC"), on streaming services and video-sharing websites that distribute content in France but are not established there. The tax revenues are collected primarily from U.S. companies and the funds are used by the French National Film Fund (CNC) to subsidize the production of original French content and programming. The tax was originally dubbed the "YouTube tax"; USTR considered the naming of the French DST the "GAFA tax" as evidence of discrimination in its 2019 Section 301 findings. The TVC is collected in addition to corporate income tax and the DST, leading to double and possibly triple taxation. A new tax on streaming music services is being currently discussed in France with a similar goal of using revenue from foreign companies to subsidize original French content. USTR should discourage discriminatory treatment of streaming and video-sharing platforms via taxation the same way it condemns service barriers imposed on the sector.

Germany: German Cultural Minister Wolfram Weimer (independent, CDU/CSU appointee) has proposed 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 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.

Hungary: Adopted several years ago, the rate for the Hungary tax on digital advertising services has been set to 0% from July 1, 2019 until December 31, 2025, at which point it transitions to 7.5%.

Italy: Since 2020, Italy has imposed a 3% DST on revenue from (a) supplying targeted advertising on a digital interface to Italian users; (b) making available to Italian users a multisided digital interface that facilitates the provision of goods and services among users; and (c) transmitting data about Italian users derived from their activities on digital interfaces. The threshold is for companies with worldwide revenue of €750 million and local revenue of €5.5 million. U.S. companies are also facing targeted tax investigations in Italy.

Poland: On August 13, 2025, Deputy Prime Minister Krzysztof Gawkowski publicized[55] the Ministry of Digital Affairs' intent to develop draft legislation for a DST that would impose a 3% tax on digital interface services, targeted digital advertising, and data transfer services. In October 2025, Deputy Prime Minister Gawkowski affirmed his intent to produce legislation by the end of 2025. Poland also imposes a tax on audiovisual services.

Portugal: Portugal imposes a tax on streaming services and a tax on audiovisual services.

Slovakia: State Secretary of Slovakia's Ministry of Investments, Regional Development and Informatization (MIRRI) Radomír Šalitroš announced[56] in August 2025 a plan to establish a tax on multinational technology platforms operating in Slovakia. Šalitroš stated his interest in scoping the proposal to cover social networks, streaming services, and cloud services provided by large foreign technology companies, and estimated the tax would bring in EUR 30-100 million per year depending on scoping and rate. Slovakia also imposes a digital platform permanent establishment.

[55] https://www.gov.pl/web/cyfryzacja/rownosciowy-podatek-od-uslug-cyfrowych--spotkanie-z-organizacjami-pozarzadowymi

[56] https://www.teraz.sk/ekonomika/r-salitros-predlozi-navrh-na-zaved/900456-clanok.html

Spain: Since 2021, Spain has imposed 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.

Preferences for Carrying European Media: 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.[57] 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[58] creates problems with respect to online services providers needing to pay news organizations for hosting news content, including links.[59] 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*"[60], 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[61]; 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

[57] *Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act)*, Official Journal of the European Union (April 17, 2024), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401083.

[58] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019L0790.

[59] See Glyn Moody, *The Copyright Directive's Link Tax Has Been A Failure; Will Anyone Learn From This?,* TECHDIRT (Sept. 30, 2024, 11:04 AM), https://www.techdirt.com/2024/09/30/the-copyright-directives-link-tax-has-been-a-failure-will-anyone-learn-from-this/

[60] Ula Furgal, *The journalists' share,* KLUWER COPYRIGHT BLOG (July 12, 2024), https://copyrightblog.kluweriplaw.com/2024/07/12/the-journalists-share/.

[61] *France Rules Google Must Pay News Firms for Content*, Reuters (Apr. 9, 2020), https://www.reuters.com/article/us-google-france/france-rules-google-must-pay-news-firms-for-content-idUSKCN21R14X

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.[62]

Government Procurement/Services Barriers - EU Cloud Security Scheme (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.

Please see the section on trade barriers in France below for related information on SecNumCloud, the French cloud cyber certification that inspired EUCS and has already taken effect.

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

[62] *Rémunération des droits voisins : l'Autorité sanctionne Google à hauteur de 500 millions d'euros pour le non-respect de plusieurs injunction* (July 13, 2021), https://www.autoritedelaconcurrence.fr/fr/article/remuneration-des-droits-voisins-lautorite-sanctionne-google-hauteur-de-500-millions-deuros.

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.

Plans for European Preference in EU Public Procurement and Funding Instruments: The European Commission and the European Parliament recently announced in September 2025 a comprehensive public procurement reform to introduce European preference in public procurement for "strategic sectors" and technologies. 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. It remains unclear whether preferences will apply to EU-headquartered companies only, or to companies with a physical location or infrastructure in the EU.

In addition to cloud (mentioned in a separate item above), the strategic sectors could include 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 would directly exclude American companies from being eligible for certain public procurement opportunities, 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.

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.

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.[63]

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. The proportionate and flexible implementation of the AI Act's requirements, as well as alignment with emerging international best practices and consensus, international technical standards, will be key to providing providers and deployers of AI sufficient legal certainty to market AI systems and products in the EU.

Digital Networks Act/Network Usage Fees: 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.

[63] See CCIA, CCIA Position Paper with EU Trilogue Recommendations on the Artificial Intelligence Act (July 2023), https://ccianet.org/wp-content/uploads/2023/07/CCIA-Europe-Position-Paper-with-EU-trilogue-recommendations-on-the-AI-Act.pdf

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, which 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.

In addition, 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.

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).

Digital Operational Resilience Act (DORA): U.S. information communications and technology service (ICTS) providers are unfairly harmed and burdened by the extraterritorial reach and unduly intrusive and burdensome requirements of the Digital Operational Resilience Act (DORA), which also overlaps and is inconsistent with the EU's Network and Information Security (NIS2) Directive framework.

As an initial matter, to the extent that financial entities contract with ICTS providers and include DORA compliance requirements in the service agreements, those providers' NIS2 compliance should be considered sufficient for conducting risk-based audits of ICTS providers and to harmonize oversight

Additionally, in the key contractual provisions, audit rights should be moderated by allowing mutual agreement on alternative assurance levels. Audit rights also should be limited to what is necessary and proportionate, ensuring they do not exceed EU authority. Instead of its intrusive audits and testing that reach shared infrastructure – indeed, potentially infrastructure located outside the EU – that actually reduce security and resilience, the EU should allow ICT providers, including US providers, to comply with DORA for their worldwide network infrastructure by relying upon requirements that parallel the contractual assurances concerning the reliability and security the ICT providers use today with large financial customers and other institutions, such as certifications with ISO and other standards organizations. Finally, registration and supply chain obligations should be limited to direct ICT suppliers to align with the scope of NIS2.

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.

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.

EU Health Data Space: The European Health Data Space (EHDS) regulations came into effect in 2025, and contain a range of cross-border data transfer restrictions and localization requirements. We urge a reasonable approach to implementation that does not harm the health of the citizens of the EU and its partner nations. The cross-border exchange of non-personal health data is important to developing and maintaining products and services for medical and non-medical patients in the EU and beyond.

There is also concern over a European Financial Data Space platform as an overarching effort by the EU to mandate data sharing among financial services providers. This has yet to be proposed in regulation.

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:

- Constellation size classification: The EUSA establishes three categories of operators, which are subject to different requirements. The category subject to stricter requirements, 'giga-constellations' (≥1,000 satellites), targets two U.S. constellations
- 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.
- 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.
- 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).
- 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.

Data Act/Data Governance Act: The Data Act[64] regulates access to and transfer of data generated by connected products and related services in the EU. It builds on other digital market regulations such as the Digital Markets Act and Digital Services Act to establish restrictions on how companies can use personal, commercial, and industrial data generated within the EU as well as additional obligations for large firms operating in local data markets.

The Data Act 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 provider 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.

Additionally, EU's Data Governance Act,[65] 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 Data Act and Data Governance Act risk 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: 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

[64] *Regulation (EU) 2023/2854 on Harmonised Rules on Fair Access to and Use of Data* (Data Act), https://eur-lex.europa.eu/eli/reg/2023/2854.
[65] REGULATION (EU) 2022/868 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), https://eur-lex.europa.eu/eli/reg/2022/868.

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.[66] 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.[67] We see ongoing politicized use of the VLOP designation in unrelated legislation as a further way to target the designated companies.

In March 2024, new regulation was adopted on the "transparency and targeting of political advertising", mandating clear labeling and stricter controls on political targeting, going further than the restrictions on personalized targeted advertising already foreseen in the DSA.[68] Non-compliance can lead to fines up to 4% of global annual turnover, resulting in some U.S. companies withdrawing political ad services from the EU.

Standards: In a development with the potential to affect the course of both data and AI regulations, the EC has launched an initiative to localize standards-setting within the Union for key sectors of the economy. The EC has explained this is to avoid "undue influence of actors from outside the EU and EEA" for standards in key areas. Indeed, the effort could undermine the ability of U.S. firms to provide input into standards that will be key to new regulations. Both the Data Act and AI Act authorize the Commission to establish specifications for forthcoming rules.

VAT: The cost of compliance with VAT requirements when selling into the EU Single Market is higher for non-EU businesses than for EU businesses and constitutes a significant non-tariff barrier. The current EU VAT registration system is generally found to be fragmented, complex and particularly costly for SMEs. This in effect restricts access to EU trade.

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

[66] Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising, Official Journal of the European Union (May 13, 2024), https://eur-lex.europa.eu/eli/reg/2024/900.
[67] Mathilde Adjutor, *The Digital Services Act's Moment of Truth: Implementation*, Disruptive Competition Project (October 20, 2022), https://www.project-disco.org/european-union/102022-the-digital-services-acts-moment-of-truth-implementation/.
[68] European Comm'n, *Supervision of the Designated Very Large Online Platforms and Search Engines Under DSA* (last updated Oct. 11, 2024), https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses

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.[69] 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.

[69] https://competition-policy.ec.europa.eu/public-consultations/guidelines-foreign-subsidies_en.

- 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.

Express Delivery & E-Commerce: The EU recently implemented the Import One Stop Shop (IOSS) to enable the import of e-commerce goods up to €150 by charging VAT to the customer at the point of sale. At the same time, it also introduced a super reduced data set to customs clear all low value goods and eliminated the €22 VAT exemption for small parcels. While some of these initiatives have brought some limited benefit, the reduced ambition and ineffective rollout of the July 2021 VAT e-commerce package have added costs to businesses and consumers and resulted in additional administrative red tape, while its facilitative aspects are not always applicable to a majority of express shipments. To enhance its utility, the EU should look to make the use of IOSS mandatory (as is the case with a similar scheme rolled out in Australia), and significantly increase the IOSS threshold from 150 euros to cover more goods, expanding this threshold in line with a similar increase which should be made to the EU's duty de minimis for all shipments.

Audiovisual: The EU has extended content quotas and levies from traditional broadcasters to VOD providers. In November 2018, the EU agreed on a new obligation for all video-on-demand (VOD) service providers, falling under the jurisdiction of a European Member State, to reserve at least a 30 percent share in their catalogues for EU works, and ensure adequate prominence of such works on services accessible from the EU. The directive also allows Member States to oblige media service providers (linear and non-linear) targeting their audiences to contribute financially to the production of European works and/or local AV production funding schemes, even if a media service provider falls under the jurisdiction of another Member State.

More than half of EU Member States have completed or are in the process of completing the legislative process to obligate media services providers targeting their territory to either invest in the production of domestic works and/or to contribute a percentage of their turnover to a national film fund. Audiovisual producers are concerned that disproportionate investment obligations, coupled with excessive subquotas for works of original national expression and restrictions on contractual freedom, might fuel the inflationary trend in production costs and work against the objective of supporting and attracting foreign investment and opening the market to new entrants.

EU Local Content Requirements: The European Commission is expected to propose a "Circular Economy Act" at the end of 2026, with the aim of strengthening EU circular economy models and facilitating the free movement of circular products, secondary raw materials, and waste. As part of this initiative, the Commission is reportedly considering making public procurement a central

pillar, using it as a lever to drive demand for circular materials.[70] Such European content requirements in public procurement would likely limit the market share of non-EU companies, creating new barriers to the free flow of goods and services between the EU and its global partners. Such requirements could also be inconsistent with EU obligations under the WTO Government Procurement Agreement.

EU General Product Safety Regulation (GPSR): When applied to second-hand products, the GPSR may be particularly impactful to numerous companies and platforms. First, the EU currently does not distinguish between new and second-hand products when imported into the EU (such as when sold by a U.S. seller). Second-hand products may therefore be expected to comply with rules that would require a change in their design, which by nature cannot be accomplished on a second-hand product, or by anyone else except the original manufacturer (e.g. CE mark, safety labelling, etc.). Additionally, second-hand products come in unique quantities, unlike new products which are generally manufactured by batch and shipped in bulk. Information to be compiled by the trader is therefore only valid for this one specific unit of product (vs. potential thousands in a new product batch). Where information is difficult to retrieve or to otherwise compile, this creates a clear economic disincentive, reducing or even sometimes erasing any potential profit margin from the sale of the product.

Digital Fairness Act: The Mission letter of newly appointed EU Justice and Consumers Commissioner Michael McGrath tasks him to "develop a Digital Fairness Act (DFA)". This is the result of a fitness check to which the European Commission committed in 2020 that is focused on a large list of practices like subscription traps, dark patterns, influencer marketing, addictive designs, personalization, and price comparison tools. There is a high risk that the Act and its enforcement targets U.S. companies.

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[71] while the draft Czech Republic transposition demonstrates divergence in its definition of "important" and "essential" entities[72], potentially leading to discrepancies in which organizations fall under the scope of the regulation. Diverging reporting obligations can be seen in

[70] See 2025 State of the Union Address by President von der Leyen, available at https://ec.europa.eu/commission/presscorner/detail/ov/SPEECH_25_2053, in which President von der Leyen announced that "*we will introduce a "made in Europe" criteria in public procurement*" and that "the future of clean tech will continue to be made in Europe. But for that, we also need to make sure that our industry has the materials here in Europe."

[71] https://njt.hu/jogszabaly/en/2023-23-00-00

[72] https://www.psp.cz/sqw/text/orig2.sqw?idd=244061

the Croatian draft transposition[73] 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.

Carbon Border Adjustment Mechanism (CBAM). The EU's CBAM requires 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.

CBAM has imposed a significant compliance burden. In the first year of the regulation, U.S. suppliers have been 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

[73] https://narodne-novine.nn.hr/clanci/sluzbeni/2024_02_14_254.html

gradually phased out. CBAM essentially discriminates against products from countries like the United States that do not have equivalent carbon emissions taxation schemes in place. The UK is in the process of adopting a similar CBAM mechanism.

Other country-specific policies of concern:

National Cybersecurity Certification Scheme for Cloud Services (SecNumCloud): In March 2022, France's national cybersecurity agency (ANSSI) revised its cybersecurity certification and labeling program SecNumCloud (version 3.2) to disadvantage and effectively preclude foreign cloud service providers (CSPs) from providing services to government agencies and 600+ organizations operating "vital" and "essential" services. Specifically, SecNumCloud and France's 'Trusted Cloud Doctrine' require certified CSPs to be "immune to non-EU laws" ("Immunité au droit extra-communautaire"), and explicitly disqualify from certification any CSP that is more than 24% foreign-owned (i.e., non-European).

As a result, U.S. CSPs must partner with and transfer technology and control to a local providers in order to provide cloud services to covered entities. This provision appears to be a clear violation of Article 3 of the WTO Government Procurement Agreement. The French legislature continues to expand these requirements to additional sectors through various amendments, often without explicitly referencing SecNumCloud, but incorporating its ownership restrictions. This growing trend of amendments across different sectors suggests a pattern of discriminatory regulation under the guise of security requirements, with the ownership criteria being the primary focus rather than actual security measures.

Cloud Technology Usage Barriers: Czech law requires CSPs to register under a Cloud Computing Catalog, which is onerous for U.S. companies. With a new Cybersecurity Law being adopted, users will face further administrative burdens when using U.S. cloud services.

Data Localization/National Cybersecurity Perimeter Law: A decree implementing Italy's National Cyber Perimeter Law (DPR. N. 81 of April 14 2021 - Annex B) requires that strategic data and supporting infrastructure for central and large local public administration and health authorities must be localized and cannot leave the national territory of Italy. When the decree entered into force in December 2023, some companies did not offer data localization and were therefore limited in their ability to provide services to Italian entities.

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.

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.

Polish Cybersecurity Act (NIS 2 Directive Implementation): The draft law will update and expand existing cybersecurity regulations in Poland, and will introduce the possibility for the Minister of Digital Affairs to designate High Risk Vendors (HRV). If an entity is designated as an HRV, it would be required to remove its equipment or software from the systems of essential entities, important entities and telecommunications operators within a designated time period. As the rules are broad, there is a risk of arbitrary designation of non-EU providers as HRVs. The draft has undergone a public consultation and is now awaiting further review, but these controversial provisions are likely to be maintained.

Data Localization: The Czech government, through the National Cyber and Information Security Agency (NÚKIB), is currently implementing the EU NIS 2 Directive with a new draft Cybersecurity Act. The current version of the draft will determine the requirements for servicing public administration information systems and has proposed to categorize data workloads from public administration information systems at security level 4 (critical) on the risk scale, thereby limiting the storage of this data to servers located in the Czech Republic.

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.

U.S. CSPs face significant barriers in Cyprus due to strict data sovereignty rules, particularly when providing services to the public sector or regulated industries such as healthcare and financial services. These rules require sensitive data, such as personal health records or financial transactions, to be stored and processed within Cyprus or the EU. These requirements mean that U.S. CSPs must either establish local data centers or partner with local providers to offer their services to covered entities. Additionally, Cyprus's public procurement framework often specifies data residency requirements for government contracts, making it difficult for U.S. providers to compete.

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.

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.

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.

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.

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 electricity security 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.

Investment: In Bulgaria, non-payment of contractual obligations remains a significant deterrent to investment. Cyprus maintains significant restrictions on the foreign ownership of real property and construction-related businesses.[74]

Legal Services: U.S.-based legal services face greater challenges in Austria, Belgium, Bulgaria, Cyprus, Greece, Hungary, Lithuania, Malta, and Slovakia – countries that require European Union or European Economic Area citizenship for full admission to the bar.

Telecommunications: There has been a growing tendency by telecom operators in EU member states to charge higher rates to end calls initiated outside the EU than for calls originating inside

[74] Executive Office of the President, Office of the U.S. Trade Representative, "2016 National Trade Estimate," European Union, March 2016, https://ustr.gov/sites/default/files/2016-NTE-Report-FINAL.pdf, 167.

the EU. It is not clear that the higher rates are based on an actual higher operating cost associated with terminating calls for the former group. This has raised questions about whether such policies are inconsistent with the EU's obligations under the General Agreement on Trade in Services. Countries with operators that assess higher fees for telecom traffic initiated in the U.S. include: Croatia, Cyprus, the Czech Republic, Estonia, Greece, Hungary, Latvia, Lithuania, Malta, Poland, Portugal, Slovakia, and Slovenia.

German Competition/Ex Ante Rules: The German competition authority (FCO) has specific powers granted under Article 19a of the Act Against Restraints of Competition (ARC), and only five US 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 with the risk to impose further restrictions on those companies to address AI concerns.

German Investment Obligation Proposal: The German Minister of Culture, under 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.

German Extended Producer Responsibility (EPR): EU legislation requires Member States to prevent the generation of waste (Extended Producer Responsibility), but until recently did not specifically address e-commerce, which led to the adoption of various national laws (France, Germany, Spain, Italy) placing obligations on online platforms to verify their sellers' compliance with EPR rules. For e-commerce sellers, these rules consist in sellers registering, reporting and paying fees to a national and category-specific "EPR scheme." The rules remain fragmented and complex for sellers. For example, a U.S. seller wishing to sell smartphones to French and German buyers will have to register with 6 different EPR schemes: one for packaging waste, one for battery waste, and one for electronic waste, multiplied by the number of Member States addressed (two in this example). In turn, the online marketplace will have to collect the 6 corresponding EPR numbers for this seller. There is no *de minimis* applicable to EPR rules so sellers are in scope from the first item sold. Marketplace verification obligations for EPR rules will be extended to all 27 Member States of the EU in August 2025 for batteries, in August 2026 for packaging, and in 2027 for textile waste.

<u>Non-EU Europe</u>

Data localization: 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, telecom and financial services. The national cloud solution can only be developed by Norwegian providers within Norwegian borders.

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.

Telecom 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.

India

U.S. companies in all industries face mounting trade and investment barriers in India. The raft of digital protectionist policies imposed, or under consideration, by the Indian government remains concerning to the U.S. services sectors.

Electronic Payment Services: The United States has continued to raise concerns relating to informal and formal policies with respect to electronic payment 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, some of which give unfair advantage to NPCI, creating a non-level playing field for U.S. 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.

Financial Services Data: 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. In 2019, RBI stated the requirement to store payments data locally also applied to banks operating in India. Additionally, through various regulations, regulators like RBI and Securities and Exchange Board of India (SEBI) endeavor to mandate data localization in certain segments which is a challenge for international banks. The data storage requirement hampers the ability of service suppliers to detect fraud and ensure the security of their global networks.

Insurance: Recent regulatory developments amended the way in which the order of preference is applied to local cedants when placing reinsurance business. While the new approach provides more business opportunities for U.S. reinsurers, it still limits their ability to compete on equal terms with domestic, Indian reinsurers. Specifically, the Reinsurance Regulations came into force on January 1, 2019 with the intention of maximizing retention within the country, subject to adequate diversification of risks. They envisage a two-step procedure for reinsurance placements:

- Step 1: Obtaining the best terms for cessions: Indian and foreign reinsurers can offer their terms to cedants on an equal basis.
- Step 2: An offer of participation taking into account the order of preference: Every cedant must offer the best terms obtained firstly to Indian reinsurers and, subsequently, to foreign ones.

It should be noted that the previous law granted full right of preference to national reinsurers. The two-step approach therefore constitutes a partial reopening of the Indian market to foreign players, since they are now able to compete on the same basis as Indian reinsurers while offering their best terms. However, the approach does not provide for equal treatment of Indian and foreign players as there is still an order of preference that favors local reinsurers.

India's rules on foreign reinsurance branches also create trade barriers. In January 2021, the Insurance Regulatory and Development Authority of India (IRDAI) launched a consultation on draft Registration and Operations of Branch Offices of Foreign Reinsurers Regulations, which contain some concerning provisions.

Specifically, the Regulations, 1) Introduce the right of first preference and cap on intragroup retrocessions; 2) Require branches to localize all core and non-core activities in India; 3) Limit the integration of global infrastructure that the foreign reinsurance branches enjoy due to the global master service agreements/service agreements that their parent companies have with IT companies; 4) Mandate dedicated underwriters for each line of business; and, 5) Require data to be held in centers located and maintained in India.

Equity Cap Limitations: India also maintains a 74% foreign direct investment (FDI) cap on insurance companies with corresponding regulations that place more onerous regulatory requirements on foreign-controlled investors relative to domestic groups. On February 1, 2021, the Finance Minister of India presented the Union Budget for the Financial Year 2021¬22 and proposed an increase in foreign investment limits for Indian insurance companies from 49% to 74%. She also indicated that foreign control may be permitted subject to certain safeguards. This increase was passed by the Indian Parliament in March 2021 and is a significant, positive development.

Unfortunately, subsequently the government released rules implementing the new amendments to the Insurance Law, which are less favorable for foreign insurers than for Indian insurers, including requirements for there to be resident Indian citizens in the corporate governance structure of foreign-controlled insurers and requirements that foreign-controlled insurers hold more capital in some cases. Another safeguard requires foreign invested majority companies to have higher solvency requirements than domestic controlled companies, for no apparent prudential purpose.

On February 1, 2025, the Finance Minister of India proposed increasing foreign investment limits to 100% from the current 74%, alongside a review of the current conditionalities (outlined above) for foreign investors. While the process to amend the laws and rules on foreign investment limits is expected to receive legislative approval, it is unclear how India will review the current conditionalities placed on foreign insurance companies and investors or if the government intends to introduce new regulatory requirements for investors that increase their investment.

Data Localization: India's insurance regulator also imposes stringent data localization requirements, most notably in the IRDAI (Maintenance of Insurance Records) Regulations, 2015 and the IRDAI (Outsourcing of Activities by Indian Insurers) Regulations, 2017. Under the IRDAI's rules, insurers are required to store all customer data and business data on servers in India and obtain express consent from the data subject to transfer data outside India. These regulations apply in addition to the aforementioned draft bill on data protection and should be eliminated.

Banking: India's regulatory environment remains non-transparent and often requires massive investments and operational complexity with aggressive timelines for implementation. A few examples are: SEBI's Merchant Banking Regulation and SEBI's Cyber Security Framework Regulations.

Priority Sector Lending: India also requires priority sector lending with specific targets in certain sectors. In the past, India permitted banks to meet their priority sector lending requirement through export credits. Ending this practice led to a decrease in the availability of financing and consequently an increase in financing costs for several industries like Textiles, Chemicals, Engineering, Small IT / ITeS. It would benefit both banks and India to permit exports credit as PSL for all entitles having exports turnover of less than 100 crs. This approach will help identify and provide incentives to export oriented entities who are in the process of achieving scale in their export business. Access to concessional credit will encourage adoption of advanced technologies and increase productivity, which in turn will also generate employment opportunities. In addition, foreign banks should be permitted to count exports financing to meet priority sector lending requirements.

Lack of Tax Parity: U.S. banks also have not enjoyed tax parity with domestic banks in India. In September 2019, corporate tax rate cuts were announced which allowed domestic companies to apply a lower tax rate of 22% (including applicable surcharge and cess 25.17%) provided such companies did not avail specified tax exemptions/incentives under the Income Tax Act, 1961.

Tax rates for branches of foreign companies remained unchanged at 40% (including surcharge and cess 43.68%). This created significant tax rate disparity between domestic companies and branches of foreign companies. The base tax rate differential became 18% (40% applicable to branches of foreign companies' vs 22% for domestic companies). Including surcharge and cess, the differential came to 18.51%. Considering applicable withholding tax and India-U.S. treaty rate

of 15%, the effective tax rate differential (between Indian companies and foreign companies operating in India as branches) came at ~10.09%.

In the July 2024 budget, Finance Minister announced a base tax rate reduction of 5% (including applicable cess and surcharges ~5.46%) for foreign companies. Currently, the effective tax rate differential between Indian banks and branches of foreign banks is ~4.63%..

Derivatives Clearing: U.S. banks have not enjoyed a level playing field when it comes to accessing the ASTROID platform. CCIL (Clearing Corporation of India) has a Rupee Derivative Segment and a ASTROID trading platform for trading interbank OIS. American banking entities like JPM and BoFA and Citi are not members on the platform. CCIL, the local clearing house, is seeking an exemption from registration with CFTC as a Derivatives Clearing Organization (DCO) for offering direct clearing to its US members (Citi, BAML & JPM) for INR IRS. RBI has objected to CFTC's request for direct access to CCIL's books and records as part of providing the exemption citing that the request breaches local privacy law breaches. For many years, there have been ongoing discussions between the CFTC (Commodity Futures and Trading Commission) and the RBI on clearing of INR derivatives. While we understand that there has been progress on the same, the delay in closure of the issues has resulted in the markets being fragmented across cleared (through Clearing Corporation of India) and non-cleared rupee derivatives trades.

Participation in Government Agency Business: Currently, any scheduled commercial bank in India requires approval from the RBI to carry out government businesses in India. To date, no international banks have been granted this approval. We respectfully ask USTR to work with U.S. and Indian regulators to facilitate the ability of U.S. banks to participate in government agency business.

Rupee Interest Rate Derivatives: RBI is proposing a requirement for the reporting of Rupee Interest Rate Derivatives (IRD) transactions undertaken globally. In summary, a market-maker must report the necessary details of its offshore Rupee IRD transactions undertaken by its offshore related parties to the local Trade Repository (TR) of CCIL. The proposed framework has significant extraterritorial implications, requiring Indian market-makers, including US banks, to report—or ensure the reporting of—Rupee IRD transactions undertaken by related entities that are legally independent, regulated outside India, and operating under local laws, which may include data privacy, banking secrecy, or client confidentiality obligations. This type of extraterritorial data collection obligation is highly unusual and potentially unprecedented in global derivatives regulation. It could result in US Banks being in contravention of obligations under local laws/regulations, cause significant operational challenges and incur costs as well as set a troubling precedent for other jurisdictions to impose similar requirements on offshore affiliates, create conflicting compliance obligations across markets and lead to duplicative or inconsistent reporting, contrary to international efforts to streamline global trade data.

The U.S. should discourage India from imposing extraterritorial obligations on US and international banks operating in India. If the RBI wishes for information on IRD transaction outside of India, that they make the request/s directly with the relevant regulators/officials in the jurisdictions that they are seeking that information.

Express Delivery: India has made progress on key TFA commitments in important areas such as a single window interface, expansion of 24/7 customs clearance facilities, increased digitalization of

customs documents and greater interagency coordination both at the policymaker level and in key ports. However, there still remains a consistent lack of predictability in the application of customs regulations and laws across ports of entry, which includes severe and arbitrary restrictions imposed by customs authorities for infringement of regulations, and a slow pace of dispute resolution. To further facilitate trade, India should introduce a de minimis regime that also lifts all duties and taxes for all goods, including low value commercial shipments and business to consumer shipments, in the same manner currently applied to gifts or samples and a more moderate approach towards suspension and revocation of courier licenses to provide business confidence. Along the same lines, India should follow through on the proposal of the Special Secretary for Logistics, Ministry of Commerce, to remove all commodity and value restrictions on couriers. Lastly, the recent customs improvements in India (e.g., single window clearance) should be expanded to all courier clearance ports and India should also improve pre-arrival processing (e.g., by separating release from final clearance) and strive toward clearance off a single, consolidated document such as a manifest with minimal data fields. Among other things, such an outcome will facilitate e-commerce exports and simplify the return process.

Digital and AI Competition Regulation and Enforcement Targeted at American companies: 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.[75] These developments risk delaying AI product launches in India and creating non-tariff barriers for American companies. The Indian government is also considering an ex-ante digital competition law.[76] Similar to the EU Digital Markets Act, this law would primarily impact American companies and restrict their ability to innovate in India under threats of significant fines and penalties. While the Indian government has since withdrawn the draft digital competition law in its current form and announced that it will first commission a comprehensive market study before introducing a fresh version of the legislation, there is a possibility this could be resurfaced.

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.[77]

Legislative changes in 2023, particularly the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (amended in 2023)[78], further challenge U.S. exporters by creating significant digital trade barriers that raise compliance costs and restrict market access for foreign digital service providers. These rules require service providers to prevent the display and sharing of an

[75] https://www.financialexpress.com/business/industry-cci-probing-google-microsoft-for-clubbing-ai-with-office-suite-3979854/lite/.
[76] Draft Digital Competition Bill 2024, available at https://www.medianama.com/wp-content/uploads/2024/03/DRAFT-DIGITAL-COMPETITION-BILL-2024.pdf.
[77] U.S. International Trade Commission, *Foreign Censorship Part 2: Trade and Economic Effects on U.S. Business* (July 2022), Table 3.2 at page 75, https://www.usitc.gov/publications/332/pub5334.pdf#page=75.
[78] https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf

extensive and vaguely defined range of information. 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.

India's use of harassment and intimidation tactics, including issue-specific interventions like the November 2023 advisory on "deepfakes"[79], further complicates the market for digital service providers. 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.[80] 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[81], 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.

---

[79] *Union Government issues advisory to social media intermediaries to identify misinformation and deepfakes*, https://pib.gov.in/PressReleasePage.aspx?PRID=1975445.

[80] *Trai releases Consultation Paper on Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services*, TRAI.GOV (July 7, 2023), https://www.trai.gov.in/sites/default/files/PR_No.59of2023.pdf. See also *Consultation Paper on Regulatory Mechanism for Over-The-Top (OTT) Communication Services, and Selective Banning of OTT Services*, TRAI.GOV (July 7, 2023), https://www.trai.gov.in/sites/default/files/CP_07072023_0.pdf (full text of the consultation paper).

[81] *Public Notice on Website of Ministry of Information & Broadcasting*, PRS (Nov. 10, 2023), https://prsindia.org/files/parliamentry-announcement/2023-12-09/Draft_Broadcasting_Services_(Regulation)_Bill,_2023.pdf.

Potential data localization under Data Protection Rules: The Digital Personal Data Protection Act (DPDP Act) entered into law on August 11, 2023[82], 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 under the DPDP Act (DPDP Rules)[83], 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 a lack of certainty 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.

Telecommunications: The Government of India removed the 49 percent foreign equity cap in the telecommunications sector, and allowed for FDI up to 100 percent. While this was a welcome development, the licensing fee charged to foreign telecommunications providers disproportionately affects smaller operators and serves as a market entry barrier.

The telecom sector, particularly the provision of new IP-based productivity and communications tools, including those that connect Internet-delivered VoIP applications and services with traditional PSTN voice services, is subject to outdated regulatory provisions that are impeding competition, the introduction of new and innovative communications capabilities, and the fuller participation of a wider variety of providers in the Indian market.

We continue to draw USTR's attention to the fact that certain elements of the May 31, 2011, amendment to the telecommunications service provider licenses deviate from global practice, while others require clarification to understand how they will be implemented to ensure that these elements do not become barriers or have unintended consequences. While the most egregious provisions of the May amendments were rescinded by the Indian government, there remain problematic legacy provisions that could undermine the ability of U.S. ICT companies to compete fairly in India's telecommunications sector.

Mandatory telecom certification framework: Most concerning is the mandatory requirement for Indian Telecom licensees to connect their networks only with telecom equipment that has been tested and certified under the Mandatory Testing and Certification Framework (MTCTE). Many of the testing requirements are redundant as U.S. technology products are already tested and accredited in international labs before introduction into the Indian market. Moreover, labs accredited by the government lack infrastructure to carry out testing and issue required certification, significantly delaying the deployment of American technology in the market. The

[82] The Digital Personal Data Protection Act 2023 (No. 22 of 2023), available at https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf.
[83] https://cdn.digitalindiacorporation.in/wp-content/uploads/2025/01/Draft-Digital-Personal-Data-Protection-Rules2025.pdf#page=28.

stringent testing regime of government in the form of MTCTE creates market assess barriers and should be rationalized by accepting testing reports or certification issued by globally recognized labs.

The scope of this requirement was recently increased to include cloud software (Hypervisors), which goes beyond telecom products. This expansion introduces localization and testing requirements for software that is not manufactured or deployed solely in India. Hypervisors and other virtualization 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 localized. 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 are not more trade-restrictive than necessary. Cloud services providers already adhere to existing international certifications and cybersecurity frameworks (such as ISO/IEC 27001, SOC 2, or FedRAMP). 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.

On March 21, 2024, the Telecom Regulatory Authority of India (TRAI) issued a recommendation to the Department of Telecommunications (DoT) that all M2M devices with eSIMs be converted to domestic operators within six (6) months. We have grave concerns with the proposal and respectfully urge USTR to encourage DoT to reject TRAI's recommendation in this regard.

The scope and number of global M2M applications are growing rapidly as businesses leverage the efficiency gains that IoT devices provide. India in particular benefits from these solutions because of its dynamic capacity to deliver high-tech services across borders.

International mobile carriers have been using roaming agreements with domestic carriers in line with GSMA standards for M2M.[ii] Although TRAI's proposed localization mechanisms are technically compliant with published GSMA specifications, in practice CSI members have found them complex, cumbersome, costly and time-consuming to implement, resulting in a poorer customer experience. Customers are left with a complex model in which it is costly to build and maintain platforms that adhere to individual provider requirements across multiple countries, with separate contracts, and the possible need to create new legal entities and manage devices in each destination country differently. Ultimately, this leads to lower IoT adoption rates, stifling innovation and higher prices for consumers.

USTR should express its opposition to TRAI's recommendation for several reasons. From a procedural standpoint, DoT's standing practice is to review TRAI recommendations without engaging in meaningful discussion with stakeholders. While there is no requirement for DoT to provide for comments on such recommendations, failure to do so and approving TRAI's recommendation without broader consultation could have significant unintended consequences, particularly for companies that operate globally using U.S. based MNO'' roaming services for IoT,

across industries such as the automotive, agriculture, manufacturing, and other sectors. These could include:

- International Roaming not only makes global M2M services accessible in India, but also allows Indian M2M services to be accessible worldwide. [84] Any restrictive timeline on permanent roaming for M2M devices would likely result in a diminished investment in connected devices in India by foreign mobile operators, as the costs and complexity of re-credentialing to local SIM would outweigh the benefits.

- Mandating the migration of M2M eSIMs to Indian MNOs may result in existing M2M service offerings becoming unavailable as the cost of migrating eSIMs to a domestic carrier is both cost prohibitive and technically challenging.[85]

- Regulation should not mandate a particular approach to eSIM. The cost of connectivity is typically rolled into the overall price of an M2M product, which must be standardized and sold in significant volumes worldwide to be economically viable. Moreover, some customers may choose not -to deploy eSIM for various technical, security or business reasons. The market is best served by a regulatory approach that allows flexibility in choosing how connectivity solutions are implemented.

  The proposed restrictions are inconsistent with prevailing international regulatory policies, norms, and best practices. In recognition of the value M2M services provide, regulatory authorities in a number of countries including the EU,[86] Australia,[87] and Singapore[88] have opted to leave decisions about eSIMs implementation to consumers and industry rather than imposing strict regulatory mandates. In fact, only about 2% of countries explicitly prohibit permanent roaming.[89]

Telecom Source Code Disclosure Requirements (ITSAR / COMSEC Scheme): India's Department of Telecommunications continues to impose market access barriers under its Communication Security ("COMSEC") scheme, implemented through the India Telecom Security Assurance Requirements (ITSAR). Originally, these rules required foreign telecom equipment and software suppliers to submit their source code to the Indian government as a condition for certification. Following engagement by the U.S. government, the requirement was revised in June

[84] DoT recognized this point in its M2M Roadmap (May 2015): "The ability to offer services globally is critical for supporting many vertical sectors including automotive and consumer electronics. Regulatory prohibition of roaming will fundamentally influence how connectivity is provided." Quoted at: https://www.trai.gov.in/sites/default/files/ACTO_20092022.pdf

[85] For one experience in China, the cost exceeded $2 million with a domestic operator willing to negotiate such an arrangement—something that may not be immediately available in India.

[86] The recently finalized European Electronic Communications Code states that Member States should promote, but not mandate, the availability of this technology. Recital 224: http://europa.eu/rapid/press-release_IP-18-4070_en.htm

[87] The Australian Communications and Media Authority has recognized the importance of device interoperability and data portability to the development of the IoT environment, though it has not intervened to mandate switching of eSIM: https://www.acma.gov.au/theACMA/internet-of-things-and-the-acmas-area-of-focus

[88] Singapore's Infocomm Media Development Authority held a consultation process on eSIM technology for M2M/IOT in 2018. Most stakeholders opposed any regulatory mandate and IMDA has yet to render a decision.

[89] Machina Research: The Impact of Regulation on the Internet of Things (January 2015): https://www.gsma.com/solutions-and-impact/technologies/internet-of-things/wp-content/uploads/2016/09/Machina-Webinar.pdf

2025. Under the updated framework, Original Equipment Manufacturers (OEMs) are no longer required to submit their source code up front but must provide internal test reports summarizing vulnerabilities and a "Self-Declaration of Conformity" affirming that the code is free from certain risks and committing to disclose the source code if a cyberattack or security incident occurs.

Despite this reform, the measure continues to pose serious challenges. The obligation to provide source code in the event of an "attack" remains undefined, leaving broad discretion to Indian authorities. Source code often contains algorithms and encryption protocols that are export-controlled under U.S. law, meaning compliance could require an export license from the Department of Commerce's Bureau of Industry and Security. Moreover, India's required test format produces numerous false positives and imposes unrealistic expectations that software be entirely free of vulnerabilities. The requirement to disclose internal testing reports and algorithms also exposes U.S. firms to intellectual property and data security risks.

CSI urges the U.S. government to continue pressing India to align its telecom security certification regime with international standards such as ISO/IEC 27001, 62443, and Common Criteria; to replace source code disclosure with accredited third-party penetration testing and vulnerability assessments; and to adopt secure-by-design development practices. India's current ITSAR framework remains inconsistent with global best practices, creates legal and commercial uncertainty, and functions as an ongoing barrier to U.S. participation in the Indian telecom market.

Remote Access: The current Remote Access (RA) Guidelines dated January 31, 2013, are highly prescriptive and require simplification. Global enterprise operators rely on RA for network operations, maintenance, and disaster management, leveraging international expertise while ensuring robust security. Currently, operators must seek approvals not only for initial RA setup but also for every subsequent addition of sites in both India and abroad, leading to process duplication and operational delays. We recommend that, once the RA server/system is approved by DoT/LEA, any further addition of sites within India should require only an intimation to DoT, not a fresh approval. Details of new IPs and locations can be shared in mutually agreed format. Similarly, approvals for foreign sites should be time-bound and should not require repeat demonstrations of the RA process already approved by DoT. This approach will streamline operations, maintain security standards, and enhance efficiency without compromising regulatory oversight.

Audiovisual: The Indian government regulates the uplink and downlink of satellite signals beaming into India. Foreign broadcasters are required to set up offices in India licensed by the government and must pay prescribed fees per channel beaming into India. More generally, India's Telecom Regulatory Authority (TRAI) imposes an onerous set of regulations on the broadcast sector, stifling innovation and hindering competition. For example, TRAI has issued tariff orders that establish the amounts, by genre, which broadcasters can charge satellite and cable platforms for content. (these orders were upheld by India's Supreme Court in 2018) and continues to create regulatory uncertainty around pricing of pay-TV channels. The government's attempt at price controls reduces the incentive for foreign investment in the sector, despite the lifting of many foreign direct investment restrictions in 2015.

Geospatial Data: Guidelines relating to geospatial data and associated services introduced in 2021 were ostensibly aimed at opening up India's mapping policy and improving the ease of doing business through deregulation, however they also contain elements that are discriminatory to foreign service providers. These guidelines on geospatial data and services limit cross-border data

transfers and are obstructing foreign firms, including U.S. companies, from forming partnerships and pursuing technology development in India.

Direct Tax Permanent Establishment Issue for Cloud Service Providers (CSPs): India's income tax laws[90] 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 enter into arrangements with data hosting service providers—often affiliated entities—that own and operate data centers globally, including in India. These data centers support customers from multiple regions and are not limited to serving users in the host country. Recently, during tax audits and assessments, Indian tax authorities have taken the position that CSPs may have a PE in India. Authorities have cited CSPs' technological control over servers and software deployed in Indian data centers as a basis for this position. This interpretation has introduced uncertainty regarding the applicable tax treatment for U.S. and other foreign CSPs operating in India, with potential implications for companies that have made substantial investments in the Indian market and seek clarity on business and taxation frameworks.

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. The Ministry of Electronics and IT deliberates on the applications before 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. 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, tables, 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.

[90] Including the *Income Tax Act, 1961* and *Income Tax Rules, 1962*.

Customs Duties on IT Products: 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%. While a step in the right direction, the lower duty rate is still not zero.

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 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.

Government Procurement: 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, including for the telecom sector and for foreign software and cloud service providers (CSPs). 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. In the case of CSPs, the requirement to demonstrate local value presents a separate unique problem as the Government of India 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 labs, 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%.

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.

Indonesia

Duties on Electronic Transmissions: CSI applauds the digital trade commitments made in the Framework for United States-Indonesia Agreement on Reciprocal Trade ("the Framework") in July of this year, and look forward to seeing the Indonesian government implement its commitments to support a permanent e-commerce moratorium "immediately and without conditions," eliminate existing HTS tariff lines on "intangible products" and suspend related requirements on import declarations under Ministry of Finance Regulation No. 190/PMK.04/2022.

GR 71: CSI also greatly appreciates the commitment Indonesia made in the Framework to provide certainty regarding the ability to move personal data out of Indonesia to the US, recognizing the US as a providing adequate data protection under Indonesia's law. We look forward to the implementation of this commitment, in particular as it relates to Government Regulation No. 71/2019 (GR71) and the Personal Data Protection Law.

Indonesia is currently planning amendments to 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.

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.

Personal Data Protection Law: 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.

Cybersecurity Bill: Indonesia's proposed Cybersecurity Bill raises significant concerns 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 - 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, particularly during security incidents where multiple agencies may issue conflicting directives.

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. The bill's current structure appears to deviate from international best practices for cybersecurity governance and could create unnecessary market access barriers.

Financial Services:
Data localization: The Bank of Indonesia still requires core/important financial transactions to be processed domestically. The Financial Services Authority (OJK) has incrementally allowed some electronic processing systems to be based offshore for banking services, insurance services, multi-financing services, and lending-based technology, but for the most part, the policy remains highly restrictive and burdensome for global companies trying to operate within Indonesia.

Insurance: The acquired ownership rights of foreign insurers who have received regulatory approval to own more than 80 percent equity has been in question. It is also important to ensure that the Indonesian government does not waiver on its decision to lift the 100% mandatory cession to domestic reinsurers.

Audiovisual:
Film Law: The Indonesian government has expressed its intention to amend the 2009 Film Law, which contains a 60 percent local screen quota and prohibits imported films from being dubbed into local language. Ministerial Regulation (MR34/2019) Concerning the Procedure for the Distribution, Exhibition, Export, and Import of Film added further limitations on screen time by a single distributor, importer, or producer to 50 percent.

Censorship Restrictions: KPI suggested that non-compliance in pre-censorship and classification requirements may violate the Broadcasting Ethics and Broadcast Program Standard, thus subjecting operators to fines and imprisonment. There has been growing pressure for Komdigi, the KPI, and the Indonesian Censorship Board to broaden their mandates by applying similar strict censorship and classification requirements on VOD/OTT services, including proposed June 2024 amendments to the Broadcasting Law which would expand the remit of the KPI to include VOD/OTT. Additionally, Komdigi's consideration to revise GR71 could expand the Government's access to private data for the purposes of enforcing content moderation, increasing compliance costs for streaming platforms operating in Indonesia.

Digital Platform Media 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.[91] This regulation, while seemingly neutral, primarily targets U.S. companies – stating that digital services companies have a "responsibility" to support news organizations.[92] 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[93] and the Child Protection/PP Tunas regulation[94] impose significant 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.

Electronic Payment Services: Bank Indonesia's (BI) regulatory framework for electronic payment services (EPS) mandates that the initiation, authorization, clearing, and settlement of payment card transactions must occur locally, and there are 80% domestic ownership requirements for all local card processors. It also mandates all domestic card transactions to be processed using the National Standard Indonesia Chip Card Specification (NSICCS). While 100% foreign ownership of US EPS companies is grandfathered, recent BI regulations (23/6/2021, 23/7/2021, PADG 24/7/2022) reaffirm BI's authority to extend the onshore/domestic processing mandate to domestic credit and e-commerce transactions. Further extension and implementation of domestic processing requirements for all domestic transactions (including domestic credit and e-commerce transactions) would require international networks to cease processing domestic transactions or establish joint ventures ceding 80% of their stake in a local subsidiary. BI also limits foreign switches to working with only two local switches on the provision of value-added services, restricting market access and operational flexibility.

Government of Indonesia should continue to provide a level playing field, including by ensuring that:

1. 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

[91] *Government Issues Regulation on Publisher Rights*, https://setkab.go.id/en/govt-issues-regulation-on-publisher-rights/.
[92] Putra Muskita, *Indonesia to require Google, Meta to compensate new publishers*, TECH IN ASIA (Feb. 20, 2024), https://www.techinasia.com/indonesia-require-google-meta-compensate-news-publishers.
[93] *Minister of Communications and Informatics Regulation No. 5 of 2020 on Private Electronic System Operators*, https://jdih.komdigi.go.id/produk_hukum/view/id/759/t/peraturan+menteri+komunikasi+dan+informatika+nomor+5+tahun+2020
[94] *Government Regulation No. 17 of 2025 on the Governance of Electronic System Implementation in Child Protection,* https://jdih.komdigi.go.id/produk_hukum/view/id/965/t/peraturan+pemerintah+nomor+17+tahun+2025

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.

2. 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). Current regulations (PBI 23/11/2021 and PADG 24/7/2022) require use of the domestic NSICCS chip standard, which is not interoperable with the global EMVCo standard, preventing banks from enabling tap-to-pay features. Allowing EMVCo interoperability would facilitate participation of all networks and align with BI's approach to the QR Indonesia Standard (QRIS), which is based on EMVCo standards. Using national standards that are not interoperable with global standards contradicts BI's goal of creating a secure, innovative payments ecosystem.

ESO Registration and Blocking: The Ministry of Communication and Digital Affairs (Komdigi) has notified 36 global companies (including US-based companies) to register as electronic system operators (ESOs). 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.

E-commerce:
Ministry of Trade Reg 31/2023 (amending No.50/2020) 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.

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.

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.

PMK 37/2025: Ministry of Finance Regulation 37 went into effect in July 2025, requiring online marketplace platforms to withhold Article 22 Income Tax on income earned by domestic sellers through electronic transactions. The Finance Ministry had announced that a 0.5% income tax on e-commerce transactions would take effect in February 2026, though implementation of this policy will be postponed until the economic growth achieves certain levels.

Express Delivery: The postal law of 2009 restricts courier services to JVs with a maximum of 49 percent foreign ownership and further prevents foreign express delivery firms from conducting the last-mile delivery unless they outsource to a third party.

Discriminatory Local Standards: Through various regulations, the government has been requiring service providers to possess Indonesian National Standard (SNI) certificates as part of public procurement process, while not acknowledging the international equivalence (ISO). Most recently, 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 local entity and local presence, as well as local content, presenting 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.

Local Content Requirements: CSI appreciates Indonesia's commitment made in the Framework to exempt US companies and originating goods from local content requirements, to apply to US ICT products, data centers and medical devices. Local content requirements create uncertainty and limit the ability of internationals service providers to serve local customers. However, the below policies are still impacting U.S. companies.

The Ministry of Industry (MoI) issued Regulation 35/2025 (Reg 35), less than two months after the Framework was announced. The regulation, replacing 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.

In addition, 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 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, 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.

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 Impor/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.

WTO Information Technology Agreement (ITA) 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.

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

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.

Product Compliance Certification and Testing Requirements for Imports: Under Komdigi 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.

Prohibition on Import of Refurbished Products: Issue: 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.

Japan

Digital platforms: In 2019, Japan established the Digital Market Competition Headquarters (DMCH) to coordinate digital market competition policy. In May 2020, the Diet passed the DMCH-developed "Improving Transparency and Fairness of Specified Digital Platforms" law. This law 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.

Telecommunications Business Act: US and foreign services operators in Japan, including those offering only streaming and cloud-based services, became subject to regulation under Japan's Telecommunications Business Act (TBA) in April 2021. Businesses that undertake intermediate communications with users in Japan, including providers of cross-border services, must register as telecommunications providers with the Ministry of Internal Affairs and Communications (MIC), appoint a representative or agent physically domiciled in Japan, and comply with regulations imposed on domestic operators under the TBA, including disclosure and reporting obligations, confidentiality rules, and services disruption notifications. Of particular concern is compliance with the TBA's "secrecy of communications" (SoC) provision, which, when extended to digital OTT services, requires user consent to access or transmit communication content and metadata in any electronic commerce, streaming, search, email, messenger, cloud, or payment service deemed by MIC to intermediate two-party communications.

Economic Security Promotion Act: 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.

Subsidies for the provision of Cloud services/GPUs under the Economic Security Promotion Act has 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.

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 technological neutral approach to security clearance would be a fair alternative.

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. 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). 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.

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 area. Such requirements favor on-prem solutions and limit use of cloud services, hindering interoperability with allies including US 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 systems without amending the security guidelines.

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 arrangement favors on-premise solutions and exclude cloud service providers from supporting the project. Massive GPUs purchase by local entities could entail the risk of transshipment of computing resources to third countries including adversaries.

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.

Insurance: Japan's cooperative-run insurance entities, called ("kyosai"), are not regulated by Japan's financial services regulator, the Financial Services Agency, resulting in an uneven playing field and lack of transparency of the regulatory environment.

Jordan

Electronic Payment Services: CBJ's 2019 Circular No. 3/10/6474 aims to empower banks 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.

Kenya

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, and 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; and
- the Computer Misuse and Cybercrimes Act of 2018, and the Critical Information Infrastructure Regulations of 2024, which mandate localization for information classified as Critical Information Infrastructure (CII), and require operators in the CII space to seek regulatory approval 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[95]

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.

The Data Protection Regulations of 2020 mandates 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. The Regulations require that at least a copy of the data falling under these categories to be stored in a data center located in-country.

In addition, 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/Taxation: 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% DST on income from services derived from or accruing in Kenya through a digital marketplace. In December 2024, Kenya passed legislative amendments replacing the 1.5% DST with a Significant Economic Presence Tax (SEPT) levied at 3% of gross turnover on non-resident entities operating through digital platforms.[96] In addition, the amendments 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.

[95] *Regulating Websites and Platforms in Egypt: Compliance Requirements*, Al Tamimi & Co (Jun 24, 2024), https://www.tamimi.com/news/regulating-websites-and-platforms-in-egypt-compliance-requirements

[96] Via the Tax Laws (Amendment) Act, 2024 (Act), and the Tax Procedures (Amendment) (No. 2) Act, 2024.

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. The Kenya Revenue Authority (KRA) published draft SEP tax regulations on 22nd Sept 2025 which are the subject of public consultation. The SEP tax may increase the tax burden for consumers and slow down card penetration where exemption clause is not applicable. While the replacement of the DST is a welcome development, we urge 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.
Financial services: Though regulatory approval can be sought, Kenya generally prohibits cross-border Difference-in-Conditions and Difference-in-Limits (DIC/DIL) insurance trade, which is an important type of insurance for facilitating U.S. exports by multinational enterprises by covering their unique risks.

The Kenyan government also employs problematic nationality requirements in the insurance sector, mandating that a minimum of one-third of the equity of an insurer be held by Kenyans or citizens of East African Community countries. In addition, one-third of the Board of Directors must be Kenyan citizens and 60 percent of brokerage companies must be owned by Kenyan citizens.

With respect to cross-border reinsurance, Kenya requires that reinsurance brokers be licensed and accredited by the Kenyan regulator, which limits access to international markets through offshore brokers. Kenya also maintains measures that accord advantages to both state-owned insurance entities and regional insurance entities. Specifically, local insurers in Kenya are legally bound to offer state- owned Kenya Re, and regional reinsurers Zep Re and Africa Re, 20 percent, 10 percent and 5 percent, respectively, of all their outward reinsurance treaties, both life and non-life. Beginning in 2021, the mandatory reinsurers have also been issuing guidelines that set minimum premium rates for some lines of business. These guidelines distort the competitive market and conflict with Kenya's Risk Capital Requirements Regulations that direct insurers to set premium rates based on their individual risk profile.

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.[97] 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 and the government's interest in using cybercrime legislation to target of political opponents[98], 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.

[97] Mwendwa Kivuva, Urgent *Concerns Regarding Internet Shutdown in Kenya during the #RejectFinanceBill2024 demonstrations*, KICTANET (June 26, 2024), https://www.kictanet.or.ke/urgent-concerns-regarding-internet-shutdown-in-kenya-during-the-rejectfinancebill2024-demonstrations/.
[98] Wycliffe Muia, *Uproar as Kenyan activist in court over cyber-crime*, BBC (Oct. 1, 2024), https://www.bbc.com/news/articles/c1wngd0d0n2o.

Republic of Korea

While the U.S.-Korea Free Trade Agreement (or, KORUS) has on the whole improved the business environment for U.S. services companies operating in Korea[99], there remain considerable obstacles to access and ease of doing business. These include the following areas:

Digital Platform Regulation: Korea has been pursuing various proposals on ex-ante digital platform regulations that disproportionately disadvantage U.S. firms. Industry estimates that these proposed bills would impact at least US$109 billion in total market revenues for U.S. companies. Overall, these rules, along with broader structural discriminatory enforcement by the Korea Fair Trade Commission (KFTC), could cost the U.S. and Korea nearly $1 Trillion in lost economic growth over 10 years ($525B in the U.S. alone), according to a study by the Competere Foundation. These include the following:

- "Online Platform Monopoly Regulation" bills, comprising ex-ante style competition rules designed to target designated U.S. companies by imposing substantial restrictions on their conduct, including forced disclosure of sensitive intellectual property. An example of this is the December 19, 2023 proposal by the Korea Fair Trade Commission ("KFTC") to enact the "Platform Competition Promotion Act" ("PCPA") for ex-ante regulation of platforms by designating "dominant platform operators". Following significant stakeholder pushback, the KFTC in September announced a pivot away from ex-ante regulation and instead issued an ex-post regulatory proposal with amendments to Korea's main antitrust legislation, the "Monopoly Regulation and Fair Trade Act." Concerningly, the new proposal still retains problematic elements from the ex-ante proposal such as disproportionately targeting U.S. companies and narrowly focusing on online services that U.S. firms provide in Korea.
- In addition, the National Assembly and the Korean Fair Trade Commission have prioritized passage of the "Online Platform Fairness Regulation," which would grant the Korean Fair Trade Commission (KFTC) expanded powers to impose restrictions on the commercial relationships between designated platforms and businesses, including the arbitrary capping of service fees, introducing unreasonable collective bargaining tactics, and the extreme shortening of payment cycles. This bill encompasses a broader set of intermediaries based on quantitative thresholds combined with a subjective "superior bargaining position" test. Not only does this risk Korea creating barriers to entry that stifle the growth of smaller digital firms, but the qualitative criteria of the superior bargaining test appear to grant the KFTC wide discretion for targeted enforcement. Like the OPMA, the "Fairness Act" would apply only to specific sectors and sets arbitrary revenue and user-base thresholds similarly designed to target U.S. firms while exempting most Korean conglomerates and large Chinese firms operating in the Korean market.

These proposals appear to be modelled on EU rules like the EU's Digital Markets act, which a recent DMA-focused report[100] has found to have imposed costs on European businesses amounting to an estimated €114 billion. The proposals' heavy-handed approach, which in some ways goes beyond the DMA, counters market principles, and is an unnecessary irritant to the longstanding bilateral relationship and a potential KORUS violation. They would only serve to

[99] Bureau of Economic Analysis, "Table 2.3. U.S. Trade in Services, by Country or Affiliation and by Type of Service," Republic of Korea, October 19, 2018, https://www.bea.gov/itable/.
[100] Copenhagen Business School – Digital Markets Competition Forum, *Economic Impact of the Digital Markets Act on European Businesses and the European Economy*, 2025, https://www.dmcforum.net/publications/economic-impact-of-the-digital-markets-act-on-european-businesses-and-the-european-economy/.

impose unwarranted non-tariff barriers on mainly U.S.-based platforms and prevent them from competing on a level playing field, benefitting only a limited number of companies, particularly other non-U.S. players experiencing rapid growth in Korea. CSI respectfully asks USTR to urge the Korean government to withdraw proposals that would significantly disadvantage U.S. firms at the expense of a broad swath of Korean and Chinese companies which are among the fastest growing firms in Korea.

Targeted enforcement by the Korea Fair Trade Commission (KFTC): 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 Reciprocal Trade Memo. These practices lead to significant compliance costs and in practice constitute major de facto barriers for U.S. companies seeking to compete in the Korean market. The U.S. should closely monitor KFTC enforcement actions and identify any discriminatory or politically motivated patterns to ensure that Korea's competition policy does not become an instrument of economic nationalism.

Data: Data localization barriers continue to exist in Korea, such as geospatial data restrictions preventing internet service suppliers from offering online maps, navigation tools, and related applications, as well as in health care and financial services, including cross-border reinsurance.

Korea's restrictions on the export of location-based data have led to a competitive disadvantage for international suppliers seeking to incorporate such data into services offered from outside of Korea. For example, foreign-based suppliers of interactive services incorporating location-based functions, such as traffic updates and navigation directions, cannot fully compete against their Korean rivals because locally based competitors typically are not dependent on foreign data processing centers and do not need to export location-based data. Korea is the only significant market in the world that maintains such restrictions on the export of location-based data. While there is no general legal prohibition on exporting location-based data, exporting such data requires a license. To date, Korea has never approved a license to export cartographic or other location-based data, despite numerous applications by foreign suppliers. U.S. stakeholders have reported that Korean officials, citing security concerns, are linking such approval to a separate issue: a requirement to blur certain integrated satellite imagery of Korea, which is readily viewable on other global mapping sites based outside of Korea. Korean officials have expressed an interest in limiting the global availability of high-resolution commercial satellite imagery of Korea but have no ready means of enforcing such a policy since most imagery is produced and distributed from outside of Korea. It is unclear how limiting such availability through specific services (e.g., online mapping) of a particular supplier addresses the general concern, since high-resolution imagery, including for Korea, is widely available as a stand-alone commercial product (and is often available free of charge), and offered by over a dozen different suppliers.

With respect to financial services data, Korea's Financial Supervisory Service (FSS) regulations, overseen by the Financial Services Commission (FSC), mandate financial institutions to establish domestic data centers for processing sensitive financial data, ensuring data sovereignty, security, and compliance. It occurs operational challenges, increasing costs, cybersecurity inefficiencies, and competitive disadvantages for global financial institutions in Korea.

The FSS regulations prohibit Cloud Service Providers (CSPs) from processing personal (credit) information on platforms or infrastructure located outside Korea in accordance with the Personal Information Protection Act (PIPA). The PIPA have been amended to clarify the legal basis for cross-border transfers, but still cross-border data transfers are not freely allowed.

On the insurance front, Korea continues to require U.S. reinsurers to localize all operational data on shore. This has created concentration risk for U.S. companies and contravenes global best practices on risk diversification and operational resiliency. Such restrictions continue to be the basis of U.S. state regulators for insurance denying Korea's request to receive reciprocal treatment from the United States for insurance regulation.

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), effectively precluding U.S. companies from selling 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.

Personal Information Protection Act (PIPA): The Personal Information Protection Commission of South Korea (PIPC) published explanatory guidelines in July 2025 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.

Network Usage Fee: Since 2016, South Korea's "Sender-Party-Network-Pays" (SPNP) system has required foreign content providers to pay excessive network usage fees to Korean Internet service

providers (ISPs). This regulatory framework diverges from the global standard of settlement-free peering and creates a significant market access barrier. Because some Korean ISPs are also content providers, fees paid by U.S. providers directly benefit their competitors. The system has strengthened Korea's ISP oligopoly, with three major providers charging network fees up to 100 times higher than other advanced economies. 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. We urge 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

Network Segregation: FSC announced 'Financial Sector Network Segregation Improvement Roadmap' on Aug 13, 2024, to relax network segregation regulations via a regulatory sandbox, enabling financial institutions to adopt Generative AI (Gen AI) tools, even processing pseudonymized personal credit data. This framework aims to support AI innovation while ensuring enforceable regulatory oversight and auditability.

While the adoption of Gen AI provides significant opportunities for operational transformation, it also occurs significant regulatory and security risks. Regulators emphasize the necessities of self-regulation, reiterating that the key to successful adoption is not speed, but compliance, security robustness, and building strong internal governance.

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.[101] The Korea Communications Commission (KCC) approved implementing rules on March 8, 2022[102], 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.[103] 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.[104] 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.

---

[101] Reason for Proposal and Main Contents, New regulations on prohibited acts of app market operators, etc. (Agenda No. 2102524) (June 30, 2020), *available at* https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_B2C0H0N7Z3O0I1Y5X3Q0Z3Y1D1U2L3.

[102] https://www.kcc.go.kr/user.do?mode=view&page=E04010000&dc=E04010000&boardId=1058&cp=4&boardSeq=52916.

[103] *KCC Begins Fact-Finding Investigation of Three App Market Operators*, (Aug. 16, 2022), https://www.kcc.go.kr/user.do?mode=view&page=E04010000&dc=E04010000&boardId=1058&cp=1&boardSeq=53609.

[104] The Korea Times, *Assembly to grill Apple, Google execs over in-app purchase fees*, (Oct. 4, 2024), https://www.koreatimes.co.kr/www/tech/2024/10/129_383576.html.

Amendments to the E-Commerce Act: Korea's Fair Trade Commission proposed amendments to Korea's E-commerce Act, which require e-commerce firms to appoint local agents, and maintain personnel and facilities in Korea as a condition of doing business. More specifically, the amendments require that in cases where a non-Korean company already has a local affiliate, that affiliate must also register as the local agent of the foreign company and must carry out consumer dispute resolution activities. We believe this requirement is overly rigid in terms of dictating how a company can operate in the Korean market, and it appears inconsistent with Korea's commitment to not mandate local presence requirements as a condition for market access under KORUS.

Information Technology Equipment: Cybersecurity Testing Requirements: Network equipment such as routers or switches procured by Korean government entities in Korea are still subject to further in-country testing requirements despite the fact that Korea is a member of the Common Criteria Recognition Arrangement (CCRA).

Audiovisual: In 2006, prior to the KORUS FTA negotiations, the Korean government agreed to reduce its screen quota requiring exhibition of Korean films, to 73 days per year. With the rapid development of its cultural industries and the success of many Korean films and television productions internationally, now is the time for Korea to show leadership in the region, trust the choices of its consumers, and further reduce or eliminate its screen quota. However, several bills have been introduced in the recent past that would further restrict the legitimate market.

Content Moderation: Korea's *Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.* (Network Act)[105] 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

[105] https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=64717&type=sogan&key=41

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 that is inconsistent with the principles of transparency, due process, and non-discriminatory digital regulation.

Artificial Intelligence: South Korea's AI Basic Act[116], 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.

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.

Brokerage Services: U.S. express delivery services companies would like to do stand-alone brokerage, but this is not possible today. Based on current laws, express companies can only clear the shipments that they handle. To clear third-party shipments and provide other ancillary services, a company must obtain a customs services corporation (CSC) license. However, express companies cannot obtain this CSC license according to current laws. CSC licenses are only granted to licensed customs brokers, and 100 percent of the staff customs brokers of the company must be licensed customs brokers. In fact, KORUS accepts this condition. Under KORUS Service

Annex I, Korea opens customs clearance services to foreign investors, but the licensing requirements are subject to domestic laws, which we hope to see change.

Express Delivery Services: Korea only applies the $200 de minimis mentioned above to imports from the United States and has not implemented it globally on a most-favored nation (MFN) basis. This has undermined the main benefit of a higher de minimis level, namely a streamlined process for rapid border clearance of these goods. Conversely, Korea's interpretation has added to the complicated web of regulatory restrictions that inhibit trade facilitation, while requiring the dedication of more automated resources to distinguish shipment values for separate customs procedures according to origin. Korea's position also requires more administrative resources by the Korean Customs Service (KCS) to ensure low value goods are moving through the right channel. The result has been service delays and higher costs for both the private sector and the government.

Financial Services: U.S. financial firms operating in Korea continue to receive administrative guidance from regulators that are not aligned with current regulations. These actions effectively develop two sets of regulatory requirements, one a public set of written and promulgated regulations and the other, a grey area of guidance issued by regulators. The grey area of administrative guidance is unwritten, developed without financial sector input, and often runs counter to current regulations or rights of financial companies. Given the two sets of rules, companies find it difficult to operate and exercise their rights (as per written regulations). It also presents a challenge as the regulatory inconsistency undercuts a sense of the rule of law, uniformity, and predictability.

The development and implementation of regulations through a transparent process is critical to the growth of the financial sector in South Korea. The development of off-the-book rules that are not aligned with written regulations reduces confidence in the regulatory system. To avoid these issues, Korea should adhere to its commitments under KORUS, which underline's Korea's commitment to "expand and enhance transparency" and within such context "shall provide interested parties an opportunity to comment on that guidance."

Malaysia

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.

Universal Service Provision Fund Obligations: CSI appreciates the commitments the Malaysian government made its trade deal with the US earlier this year, specifically the commitment to withdraw the following revenue-sharing requirements. The Malaysian Communications and Multimedia Commission (MCMC) introduced a 6% levy on net revenue effective January 2025 or all application service provider-class licensees, targeting select US and other foreign technology companies. This levy was essentially a digital services tax and represented a significant expansion from traditional USP fund contributors.

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[106], 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

[106] By way of the *Communications and Multimedia (Amendment) Act 2025* (https://www.mcmc.gov.my/skmmgovmy/media/General/pdf2/A1743-BI-COMMUNICATIONS-AND-MULTIMEDIA-AMENDMENT-ACT-2025-1.pdf), which was brought into force (except for sections 92 and 112) on February 11, 2025 by Gazette Notice (https://lom.agc.gov.my/ilims/upload/portal/akta/outputp/2685090/PUB%2061.pdf).

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.

Financial Services: Bank Negara requires all local direct insurers to cede business first to local reinsurers (first tier) and then to Labuan- based reinsurers (second tier). Only after these two options have been exhausted may business be offered to 'offshore' or third tier reinsurers. Furthermore, (a) Malaysian Re must be offered up to 15 percent for both proportional and non-proportional treaty reinsurance (excluding aviation, energy and D&O); (b) for facultative and engineering reinsurance Malaysian Re must be offered up to 15 percent of MYR 5mn on a total sum insured basis, the PML monetary limit being MYR 1.5mn; (c) for retrocession, 20 percent must be offered by Malaysian Re to licensed direct insurers in Malaysia, for treaty and facultative business.

Malaysia also maintains a "national interest test" on the operation of financial institutions writ large, including for investments and licensing in the insurance sector, and uses that test to maintain de facto FDI caps in the insurance sector. Additionally, while Malaysia did allow a higher than 70 percent foreign ownership of insurers (which at times was necessitated by Malaysia's mandatory tender rules for acquisitions), Bank Negara Malaysia announced that it will apply a hard 70 percent FDI equity cap to existing acquisitions, and no longer respect the acquired ownership rights of foreign insurers who have received regulatory approval to own more than 80 percent equity.

Payments: Competition with state owned enterprises who enjoy preferential treatment in digital payments is a concern. Bank Negara is the largest shareholder (33%) in the domestic payment scheme, PayNet. Central banks that regulate and provide payment services should maintain operational separation to prevent conflicts of interest and avoid regulations that favor domestic service providers and unfairly disadvantage foreign/international service providers. Under BNM's Payment Card Framework, interchange fees are capped at 0.10% for domestic scheme debit cards and 0.27% for international scheme debit cards. BNM's proposal to adopt lowest cost routing in a differentiated debit interchange environment where the domestic scheme (0.10%) appears as the more cost-effective option compared to international schemes (0.27%) is an example of regulation that favors domestic service providers and unfairly disadvantages international service providers.

Local Content Requirements: Local content requirements (LCRs) are being proposed by both State and Federal authorities in Malaysia. The state of Selangor has plans 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.

Import certification: 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.

Domestic Preference: Foreign-owned stores are required to reserve at least 30 percent of shelf space for goods and products manufactured by Malaysian-owned businesses.

Customs: Foreign companies are not allowed to conduct customs clearance services unless they meet a range of criteria, including the need to establish regional headquarters in Malaysia.

Intellectual Property: Concerns remain on intellectual property issues, including the availability of pirated copyright and counterfeit trademark products as well as the lack of appropriate U.S.-style safe harbors to ensure efficient removal of infringing or problematic content.

Mexico

While the USMCA has buoyed U.S. services trade with Mexico, concerning impediments remain. These include:

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 entry into force, Mexico has failed to comply with these commitments, maintaining significant barriers to U.S. EPS suppliers that effectively prevent them from fully participating in Mexico's domestic payments market.

Mexico should immediately take all necessary steps to comply with its USMCA obligations pertaining to EPS. In particular, Mexico should promptly finalize regulations that enable U.S. EPS suppliers to process domestic transactions using their own attributes – specifically, the draft regulation on card payment networks ("card payment networks regulation") led by the Comisión Nacional Bancaria y de Valores (CNBV) and the Central Bank (Banxico) and the draft regulation on clearinghouses ("clearinghouses regulation") led by Banxico.

On October 24th, 2025 Mexico published a draft of the card payment networks regulation for public consultation. As published for open consultation, the draft regulation would not resolve the barriers that USTR has sought to address by enabling U.S. EPS suppliers to process domestic transactions using their own attributes and to differentiate their value proposition.

The draft clearinghouses regulation has not been published. Once finalized, Mexico should promptly publish the regulations and solicit public comments in accordance with Mexican law and the USMCA.

Through the consultation process, we urge USTR to engage the Mexican Ministry of Economy closely to ensure that all final regulations facilitate interoperability among networks. Addressing interoperability will allow U.S. EPS suppliers to operate on a level playing field, specifically under their own rules and to offer value-added services.

Subject to the consideration of public comments – including from the United States and U.S. stakeholders – Mexico should then implement the regulations without further delay.

These regulatory changes intend to promote financial inclusion for both individuals and businesses by providing a wider range of payment options. It would also help Mexican financial institutions introduce new payment services and enhanced fraud-prevention tools more quickly, ultimately benefiting their users.

As Mexico is looking to modernize state-owned payments infrastructure, there is an opportunity to ensure that Mexico will maintain a level playing field in the future so that the U.S. EPS suppliers can justify expanding the export of services they offer in Mexico. Mexico's President Claudia Sheinbaum has publicly stated the intention to adopting payment infrastructure models similar to Brazil's Pix or India's UPI.

Ensuring that Mexican policy does not entrench preferential treatment for its government endorsed domestic platform is critical to maintaining secure, interoperable, and competitive payment networks that benefit consumers and businesses alike. We urge the USTR to address these concerns proactively, safeguarding U.S. interests and promoting a balanced framework for electronic payments under the USMCA. Eliminating existing measures that favor domestic players and harm U.S. EPS suppliers will not be impactful if new, similar measures are later introduced in a different form.

Tax Actions Targeting U.S. Firms: A deeply concerning provision within the 2026 Economic Package presented to the Mexican Congress[107] would, if enacted, create a new tax surveillance tool of unprecedented reach. The proposal, identified as Article 30-B of the Federal Tax Code, would obligate digital service providers to grant the Mexican Tax Authority (the Servicio de Administración Tributaria, or "SAT") permanent, "online and real-time access" to their internal systems and operational records. This disproportionate measure, aimed at VAT collection, is explicitly coupled with an expansion of the existing "kill switch" mechanism, allowing SAT to administratively block services that fail to provide this access.[108] This proposal creates 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 press the Government of Mexico to simplify the bureaucratic requirements (e.g., local legal representative and apostilled documentation) for foreign Small and Medium Enterprises (SMEs) seeking an RFC, which currently acts as a market entry barrier, and to seek assurances that the "kill switch" mechanism will not be activated, as its use would raise immediate USMCA compliance concerns.

Beyond new proposals, existing Mexican tax law creates foundational market access barriers, particularly for U.S. small and medium-sized enterprises (SMEs). Legislation mandates that foreign businesses, including e-commerce platforms and digital service providers, must register for a local tax ID (Registro Federal de Contribuyentes, or RFC).[109] The process for a non-resident firm is prohibitively burdensome, requiring the appointment of a local legal representative who is "jointly and severally liable"for the firm's tax obligations, along with a local tax domicile. This, combined with a bureaucratic process of apostilles, translations, and notary legalizations, can take over five months and cost in excess of $5,000. effectively "filtering" U.S. SMEs from the market.

Furthermore, 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, SAT and related agencies have increasingly targeted U.S. multinational companies with unreasonable 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

[107] PwC, *Economic Package 2026 proposal,* https://www.pwc.com/mx/es/archivo/2025/202510-mx-tax-reform.pdf
[108] EY, Mexican tax reform proposals applicable to digital platforms, https://www.ey.com/es_mx/technical/tax/boletines-fiscales/tax-reform-proposals-digital-platforms
[109] KPMG, *Mexico: List of 260 registered foreign providers of digital services (as of April 30, 2025)*, https://kpmg.com/us/en/taxnewsflash/news/2025/06/tnf-mexico-list-of-registered-foreign-providers-of-digital-services.html

2019-2024 period[110], 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[111], a program essential for IMMEX operations. The targeting of U.S. companies represents in discriminatory and arbitrary manner raises the costs of doing business and undermines the stability pledged under the USMCA.

Government Procurement: Mexico must meet its commitments by affirmatively covering the Comisión Federal de Electricidad (CFE) "Telecom y Internet Para Todos" program, which was launched as USMCA entered into force. Mexico's Ministry of Economy has confirmed that this program falls under its current government procurement obligations, but has never provided that confirmation in writing. The agreement should explicitly reflect that "Telecom y Internet Para Todos" is covered under CFE's listing. The U.S. should engage Mexico on CFE's failure to meet its obligations under the agreement, particularly with respect to the notice, supplier qualification, technical specifications, time periods, and compliance obligations. CFE has routinely failed to comply with these provisions, to the benefit of Chinese suppliers. The United States should press Mexico to fully meet its obligations in these areas.

Insurance: On September 8th, 2025, Mexico's Executive Branch presented to the Mexican Congress its proposed economic package for 2026 which includes a set of proposed bills to the Federal Fiscal Code (FFC). One proposal to Article 141 of the FFC is to change the means through which taxpayers may guarantee a tax liability / tax assessment. This change discriminates against U.S. insurers providing surety bonds in Mexico tilting the playing field toward Mexico's state-owned bank, Banco del Bienestar, SNC. US insurers are the world's largest surety providers and play a key role in the Mexican market.

Currently Article 141 of the FFC allows the taxpayer to guarantee tax liability through the authorized means that they deem appropriate for their situation. Taxpayers may choose to guarantee a tax liability in any of the following manners: (a) by making a deposit in cash, with a letter of credit, or with other forms of equivalent financial guarantees; (b) with a pledge or mortgage; (c) by providing a bond issued by an authorized institution; (d) through a joint and several obligation; (e) through an administrative-law attachment; or (f) through securities or the credit portfolio of the taxpayer itself.

The proposed reform to Article 141 seeks to establish a mandatory order of priority of the ways in which taxpayers may choose to guarantee tax liability: 1) a deposit slip from a specific bank (*Note*: The deposit slip, which covers a cash deposit, is issued exclusively by Banco del Bienestar, SNC, Mexico's state-owned bank); 2) letter of credit; 3) pledge or mortgage; 4) surety bond; and, 5) joint obligor.

The change from a choice system to one that requires the taxpayer to justify why it is unable to use each successive option, the primary one being a state-owned bank, means that there will be a reduction in the demand for surety bonds which is an important segment for U.S. surety companies operating in Mexico. Other changes to Article 141 further contribute to discrimination against U.S.

[110] SAT, *Crece 367% recaudación de Grandes Contribuyentes por Precios de Transferencia*, 2025, https://www.gob.mx/sat/prensa/crece-367-recaudacion-de-grandes-contribuyentes-por-precios-de-transferencia-026-2025

[111] Deloitte, *Global Trade Advisory Alerts – 03 October 2024*, https://www.deloitte.com/global/en/services/tax/perspectives/global-trade-advisory-alert-3-october-2024.html

insurers by limiting the potential customer pool to those that represent a higher liquidity risk causing the insurer to decline issuing a surety bond in the first place due to the solvency concerns. All of these factors will lead to a decline in the demand for surety bonds, in favor of Mexico's state-owned bank, undermining the current business environment for U.S. surety insurance providers. Finally, the proposed change to Article 141 of the FFC negatively impacts Mexican companies that seek to secure a guarantee. Under the proposal, these businesses will now be required to place their capital with the state-owned bank rather than utilizing those funds in the marketplace. Surety bonds impose significantly less strain on a commercial entity's balance sheet while still providing the government with the necessary security during the tax appeal process. It is important that commercial entities retain the discretion to select the regulatorily approved security option that best suits their needs. We urge the U.S. government to ensure that American insurers continue to be able to provide surety products on a level playing field through the elimination of the proposed changes to Article 141 of the FFC.

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.

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 especially burdensome for 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.

Telecommunications Policy: Despite the strength of Mexico's 2013 Telecom reforms and similar Telecommunications provisions incorporated into USMCA, the competitive landscape in Mexico's telecommunications sector has barely changed over the past five years. Indeed, since USMCA went into effect, the sector's preponderant economic agent, America Movil, has seen its revenue share increase in the first quarter of 2025 while its profit margin has risen. The entrenched position maintained by this dominant supplier, particularly regarding the mobile services market, demonstrates the continued need for the vigilant enforcement of the regulations adopted to

address the supplier's status, and maintain all the aspects related to the major supplier, including the definition of preponderant agent as currently established in the treaty.

In addition, the Mexican Government has discriminated against U.S. carriers by maintaining high and discriminatory annual spectrum fees that are significantly above international benchmarks. According to Mexico's former regulator, the Federal Telecommunications Institute (IFT), annual spectrum fees for the AWS, PCS, 2.5 GHz and 3.5 GHz bands are between 88% and 96% higher than the international median. Regardless of the recommendations of the USTR, the Government of Mexico has dismissed several proposals made by both IFT and the private sector to reduce the cost spectrum to international standards. Additionally, the state-owned carrier Altan which is currently using the 700MHz band pays only 10% of the total spectrum cost compared to what is paid by private operators for equivalent bands.

This imbalanced competitive landscape is exacerbated by these discriminatory spectrum fees that distort the market resulting in a reduction of competitors in the last 3 years (*e.g.,* Telefonica returned its spectrum holdings and operates as a reseller).

Reforming spectrum fees to achieve international standards will help promote investment in mobile broadband service, address inflation, and create more tax revenue which has been lower in the past than expected due to Telefónica exiting its spectrum holdings.

Mexico has one of the most expensive spectrum costs, hindering the digital transformation in the country: spectrum costs are 10 times higher than in Brazil, 4 times more expensive than in Germany; and 40% higher than in Spain.

Earlier this year, the IFT submitted another formal opinion and released a market study on spectrum fees to the Secretary of the Treasury (Secretaria de Hacienda y Credito Publico), showing the spectrum fees in Mexico are among the highest in the world and are a structural barrier to competition that favors the preponderant agent. IFT recommended lowering spectrum fees for all agents in most relevant bands to international standards.

We also are concerned that the Mexican government is providing state subsidies to Altan and CFE Telecom (both State-owned companies) Public subsidies (CFE Telecom's infrastructure and financial injections) that are benefiting Altan and its resellers, are putting anti-competitive pressure on wholesale and retail prices. With this, Altan's MVNOs can sell at prices up to 4 times lower than private network operators.

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 powers were split between two regulatory agencies (the National Antitrust Commission and Telecommunications Regulatory Commission), both controlled by the Executive Branch and thus, with no autonomy. Furthermore, this leads to a conflict of interest between the regulatory agency and the telecommunications state-owned enterprises.

Additionally, 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.

Barriers to access energy: Mexican energy policymakers continue to create hurdles for companies seeking to connect to the electricity grid and purchase clean and reliable energy. These hurdles include directing energy consumers to purchase energy from the state-owned utility, Federal Electricity Commission (CFE), and receiving disproportionate transmission infrastructure requests as part of the process to connect to the grid with the National Center for Energy Control (CENACE). On 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 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.

Security Concerns: Beyond barriers to U.S. exports and U.S. foreign direct investment in Mexico, public security concerns have eroded business environment not only for foreign but also domestic firms. In turn, this situation may impact negatively investment (including foreign), growth, employment and consumption in the country.

Express Delivery and E-Commerce: The Government of Mexico has not complied fully with the letter or spirit of its USMCA customs obligations and instead is moving to erect new customs barriers that harm the ability of American small businesses to benefit from the agreement. Mexico has yet to implement fully key USMCA commitments such as Allowing periodic assessment and payment of duties (Article 7.8.1);permitting the ability to self-file without a broker and removing the “local” broker rule (Article 7.20) by amending or providing guidance on Reglas de Comercio Exterior

(Section 1.4 - Agentes y Apoderados Aduanales); and publishing or otherwise communicating customs regulations that it proposes to adopt, violating the spirit of Article 7.3, as well as the USMCA chapter on good regulatory practices.

Mexico has also failed to fully implement its commitment to reducing customs formalities and simplifying processing to shipments valued up to US$2,500. On May 27, 2021, Mexico's Tax Administration Service (SAT) published revised General Foreign Trade Rules that raised the informal clearance threshold to $2,500. The increase to $2,500 went into effect on June 26 for shipments valued at >$117. However, the Secretary of Economy still needs to harmonize its own regulations to allow for this change to be fully implemented which has not happened to date. Specifically, the SE needs to update Section IX, Article 10 of the Annex 2.4.1, which still requires compliance with all applicable NOM's for those courier shipments with a value of $1,000 or more, which in line with the recent changes to the SAT rules and the USMCA, should be updated to $2,500.

In addition, Mexico has also published new regulations that increased import rates on shipments from the US and Canada valued between US$50-117 by 1% (from 16% to 17%). For non-USMCA shipments, the import rate was also increased by 3% (from 16%-19%) for shipments between US$50-1000. These changes were made without warning or following appropriate protocols, and they became effective immediately. While this is a small increase, we view it as a violation of the USMCA and a sign that the AMLO Administration does not intent to implement its customs commitments, and may in fact, take additional steps that will disadvantage US exporters.

We are also concerned with Mexico's June 2020 increase to 17-19 percent of its "Tasa Global," a combination duty and charge on all shipments entering under simplified clearance (de minimis and informal entry) methods, including on shipments from the United States and Canada. This direct increase of trade costs seriously undermines the purpose of the USMCA's customs chapter. In addition, the implementation of Article 7.8.2 remains incomplete as Mexico's latest regulatory update failed to include a key facilitation for shipments valued between US $1,000 and $2,500. Lastly, Mexico has yet to fulfill its USMCA commitment to permit the periodic assessment and payment of duties for express shipments. We urge USTR to request that Mexico resolve these issues.

Audiovisual:
Foreign Ownership Limitations: Mexico currently maintains a 49 percent foreign equity cap for broadcast networks. By comparison, the U.S. FCC has permitted foreign entities to hold up to 100 percent of a broadcaster, subject to a case-by-case review.

Local Content Quotas: On a regular basis, Mexican lawmakers and policymakers propose protectionist policies, such as the imposition of local content quotas in both theatrical and streaming/OTT windows, as well as limits to the number of screens in which a given movie can be exhibited. If adopted, such measures would severely limit the exhibition of U.S. films in Mexico and would potentially contravene Mexico's USMCA commitments.

Trade facilitation and border issues: U.S. exporters continue to face significant challenges at the U.S.-Mexico border. The Government of Mexico has still not fully complied with the letter or spirit of its U.S.-Mexico-Canada Agreement (USMCA) customs obligations, and instead is moving to erect new customs barriers that harm the ability of U.S. small businesses to benefit from the agreement.

Specifically, U.S. exporters are experiencing a significant increase in inspections and competing requests for information from multiple agencies at the same time in order to clear customs. SAT's customs automation interface has also repeatedly failed, including after recent changes were abruptly made to tariff levels, which has further increased border crossing times. U.S. companies have also experienced an increase in security incidents in northern Mexico near the border that have endangered employees and business operations. In addition, the government has begun exploring modifying/eliminating de minimis, along with increasing the global rate (Tasa Global) to fight undervaluing of products entering the country. While it's a mid-term strategy, the modification would greatly increase the cost for SMBs to export to Mexico.

Full implementation of Mexico's commitments in the USMCA's Custom Administration and Trade Facilitation Chapter, including those related to expediting the release of goods, transparency in customs procedures, communicating with traders, the use of information technology, and the adoption and maintenance of a single window, would address these concerns.

Nepal

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

Electronic Payment Services: The Commerce Commission (Commission) has proposed an unprecedented range of new regulations that would cap interchange fees for all types of payment card transactions (including credit and debit, consumer and commercial, domestic and international). Together, the proposed measures would make New Zealand one of the most highly regulated payments market in the world.

The proposed interchange fee caps are arbitrary, lack economic justification and are targeted only at U.S. payment networks. There is no evidence supporting the regulatory actions meeting the purpose of the regulation. The proposed regulation undermines business confidence in the market.

The Commission should engage with U.S. payment networks and other stakeholders and delay finalizing the regulation to find a solution in line with global best practices.

Digital Platform Media Taxes: In August 2023, the New Zealand government introduced the "Fair Digital News Bargaining" Bill[112], modeled on similar laws in Australia and Canada, and designed to make large digital platforms 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.

[112] Fair Digital News Bargaining Bill 2024 (No. 278-1), https://bills.parliament.nz/v/6/fc7faac0-2ec0-4e47-7ab5-08db9ebb2302?Tab=hansard.

Nigeria

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.

Digital Taxation: The 2021 Finance Act introduced a new 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.[113] 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.[114] 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

[113] Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries (2022), https://nitda.gov.ng/wp-content/uploads/2022/10/APPROVED-NITDA-CODE-OF-PRACTIVE-FOR-INTERACTIVE-COMPUTER-SERVICE-PLATFORMS-INTERNET-INTERMEDIARIES-2022-002.pdf.

[114] Vittoria Elliott, *New laws requiring social media platforms to hire local staff could endanger employees,* REST OF WORLD (May 14, 2021), https://restofworld.org/2021/social-media-laws-twitter-facebook/.

mandating local incorporation, which collectively create a high-risk and uncertain regulatory environment for U.S. platforms.

Additionally, 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[115], which it withdrew nearly three years later after little progress[116]. ARCON has since issued similar, largely unenforceable fines to TikTok and Google.

Express Delivery: Nigeria recently passed new postal legislation to establish a new Postal Commission with additional sweeping discretionary powers over other non-postal operators. The legislation would monopolize the carriage of all items up to 1kg, giving exclusive access to the public postal operator, the Nigerian Postal Service (NIPOST), which is a government-owned entity. Presently, the sub-1kg delivery market is a competitive one in which NIPOST and numerous private companies operate. In addition, the law would create a Fund to finance NIPOST's expenses (with minimal oversight) seeded by a levy of 2% of annual turnover on express delivery service providers. These measures present a material conflict of interest for the sector regulator, discriminate against international investors by restricting market access, and give disproportionate treatment to NIPOST over its competitors. For these reasons, the proposed measures are discriminatory toward U.S. express delivery companies and deprive U.S. exporters of choices over who to use to deliver parcels below 1kg. In sum, U.S. express delivery service providers would no longer have access to the market of small parcels below 1kg and would have to pay a fee of 2% of annual turnover for all other deliveries, whereas NIPOST would not. This proposal would significantly impact SMEs, who overwhelmingly use express delivery services to export to global markets, by reducing their choice of service providers (and therefore reducing their connectivity to global markets).

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.

[115] Associated Press, *Nigeria Regulator Seeks $70M Penalty Against Meta*, (Oct. 5, 2022, https://apnews.com/article/technology-africa-business-lawsuits-nigeria-f00313679c07f2a56d844d53b7094643.
[116] https://tribuneonlineng.com/arcon-withdraws-suit-against-meta-restrategises/.

Pakistan

Banking: Carve out for foreign bank branches from Islamic banking laws in Pakistan. On October 21, 2024, amendments were made to the Constitution of Pakistan through the Constitution (Twenty-sixth Amendment) Act, 2024. Amongst these, is an amendment to Article 38(f) which provides that interest/usury (*riba*) should be eliminated by January 1, 2028. The banking sector in Pakistan is actively transitioning from conventional banking towards Islamic Banking, a separate licensed activity in Pakistan. The central bank, State Bank of Pakistan (SBP), while not mandating the transition, is supportive of the same and is routinely issuing guidance and circulars to facilitate the transition. The SBP acknowledges the challenges for branches of foreign banks to convert to Islamic Banking and has maintained that the conversion guidance is only directed towards locally incorporated banks and/or those banks looking to transition and that a dispensation or carve out will be created for branches of foreign banks operating in Pakistan.

Data Localization: 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 2022, Pakistan also launched a Cloud First Policy. This policy imposes data localization requirements on wide and open-ended classes of data ("restricted", "sensitive", and "secret").

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 State Bank of Pakistan (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*[117] 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 2025, Pakistan amended its Prevention of Electronic Crimes Act[118], 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 encouraged investment flight.[119] 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.[120]

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.

---

[117] https://www.pta.gov.pk/assets/media/removal_blocking_unlawful_content_rules_2021_20102021.pdf
[118] *Prevention of Electronic Crimes (Amendment) Act, 2025*, https://www.na.gov.pk/uploads/documents/679b243193585_457.pdf
[119] *Pakistan's 4-day internet shutdown was the final straw for its tech workers*, Rest of World (June 8, 2023) https://restofworld.org/2023/pakistan-internet-outage-tech-workers/.
[120] Ariba Shahid, *Pakistan's internet firewall could cost economy $300 million, association says*, REUTERS (Aug. 15, 2024, 9:02 AM), *https://www.reuters.com/technology/pakistans-internet-firewall-could-cost-economy-300-million-association-says-2024-08-15/*.

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.

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.

Electronic Payment Services: 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.

Panama

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.

Peru

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.

Data Localization: In January 2020, Peru's Digital Trust Framework (Decree 007)[121] 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.

[121] Thomson Reuters Practical Law, *Doing business in Peru: overview*, https://uk.practicallaw.thomsonreuters.com/0-500-7812.

Philippines

Audiovisual
Foreign Ownership Restrictions: Foreign investment in mass media, including film distribution and the pay-TV and terrestrial broadcast sector, is prohibited under the Philippines Constitution of 1987. However, 40 percent foreign direct investment is allowed in the telecom sector. Disparate treatment of these related network-based industries not only discourages business development in a capital-intensive sector. These restrictions impede investment in innovative and creative sectors, limit consumer choice, and favor domestic investors. Such restrictions are also outdated in the digital and internet era, which has upended traditional definitions and structures in the "mass media" industries. Such restrictions should be removed.

Taxation: Film companies doing business in the Philippines are subject to some of the highest taxes in the Asia-Pacific region. Foreign companies are burdened with a 30 percent income tax on net profits, a 5 percent withholding tax on gross receipts chargeable to income tax liability, and a 10 percent tax on the distributor's share of the box office. A municipal license tax of 0.75 percent of a company's prior year gross receipts is also imposed on motion picture companies. Moreover, the Philippines imposes a tax on all related advertising materials and royalty remittances. The combined effect is an oppressive tax regime that harms the continued development of a legitimate audiovisual marketplace.

Data Localization: A new executive order (EO) on data residency and data classification has been drafted, potentially requiring all data, including non-sensitive and commercial data that is in any way connected to government work to be processed and stored in the Philippines. The draft EO mandates that only "Non-Sensitive Government Data" can be stored in off-shore infrastructure. It further requires the following data categories and systems to utilize infrastructure located physically in the Philippines: core operations of Bangko Sentral-supervised financial institutions deployed on private cloud; health information systems of health service providers and insurers; subscriber information of service providers located in the Philippines; all national security systems; and all sensitive personal information processed by private entities for the government. The EO has yet to be issued, but we have heard the government intends to move quite quickly to finalize. It warrants close monitoring by the U.S. government, as it applies so broadly that commercial services would be highly likely to be subject to the data localization mandates, which will severely restrict the ability for U.S. service providers to operate in the Philippines.

DICT has subsequently created a similar draft circular and it is unclear if both the EO and circular will be issued. The draft circular on Policy Guidelines on Data Residency for Government Agencies, dated October 27, 2025, introduces data residency broadly for both secret and sensitive government data, and includes sovereign cloud provisions that require all secret, sensitive, and confidential government data remain within Philippine territory or sovereign jurisdiction, restricting data transfers.

The push for data be localized can also be seen in other recent legislative developments. 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 was circulated to the business community, but its authenticity could not be verified.

Additionally, public procurement preferences for domestic entities extend to the cloud sector, restricting foreign and U.S. suppliers' activities in the Philippines market absent domestic partnerships. 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.[122] 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.

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 the push for data localization in the Philippines. 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.

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.

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 (GPRA)[123] 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. Additionally, Executive Order No. 120, issued in 1993 directs government departments and agencies, including government-owned and controlled corporations, to exert best efforts to negotiate countertrade equivalent to at least 50 percent of the value of contracts on foreign capital equipment, machinery, products, goods, and services worth at least $1 million. Government Procurement Policy Board Resolution 14-2005 states that a

[122] *Government Procurement Policy Board Resolution No. 14-2021*, https://www.gppb.gov.ph/wp-content/uploads/2023/05/GPPB-Resolution-No.-14-2021.pdf.
[123] https://www.gppb.gov.ph/assets/pdfs/Updated 2016 IRR_31 March 2021.pdf

government agency must comply with the provisions of RA9184 if it decides to adopt countertrade as an internal procurement policy. Republic Act No. 12009 (otherwise known as ”the New Government Procurement Act” orNGPA), was signed into law on July 20, 2024, looks to enhance the existing procurement systems implemented by the 21-year-old GPRA. The NGPA 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.

Telecommunications Services: 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 own more than 50 percent of public services engaged in the operation and management of critical infrastructure, subject to reciprocity requirements.

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 the 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).

Customs Treatment of Subsea Cable Installation and Repair Ships: While the customs laws related to fiber optic cables in the Philippines have remained unchanged for many years, the Bureau of Customs has in recent years revised its interpretation of the rules regarding fiber optic

cable repair vessels. The Bureau has taken the position that foreign-built and specialty-constructed repair vessels entering Philippine waters for subsea cable installation, repair, or survey work should be treated as permanent imports, subject to duties and taxes as high as 12% of the vessel's full value. Instead of a temporary bond to guarantee re-export, as was previously the practice, firms are now forced to pay a non-refundable "insurance premium" of 2% of the import tax simply to secure a permit to operate. This shift in interpretation and departure from international norms appears rooted in the specific omission of Annex C ("Means of Transport") from the Philippines' 2022 implementation of the Istanbul Convention on Temporary Admission[124], which 75 other countries committed to. The resulting "Marina Special Permits" regime in the Philippines has left companies with the untenable choice of paying exorbitant fees or risking impoundment of vessels, which would delay or prevent urgent cable repairs. The current regime threatens to deter investment in subsea cable projects and slow urgent repair work, leaving cables idle for extended periods.

Reconfirmation of Tax Treaty Benefits: The US and the Philippines executed an Income Tax Convention in 1976. Under this treaty, "taxation of business profits derived by a resident of the other country is governed by the standard treaty concept that tax liability will arise only to the extent that the profits are attributable to a "permanent establishment" in the taxing country." To access benefits under the tax treaty, the Philippines Bureau of Internal Revenue (BIR) requires that income payors file a request for confirmation (RFC) with the BIR. The BIR has issued guidelines to administer such annual pre-approval which comes with onerous documentation requirements which undermines the benefit of the existing tax treaty. The BIR also indicates possible penalties and criminal liabilities for non-compliance. There is significant ambiguity on how long BIR will take to review the RFC and there is no guarantee of a positive outcome. Such requests have to be made by each and every income payor (customers) of US non-resident service providers selling to the Philippines.

Internet Transactions Act (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.[125] 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.

[124] https://www.wcoomd.org/en/about-us/legal-instruments/~/media/2D53E23AA1A64EF68B9AC708C6281DC8.ashx
[125] Including the *Special Economic Zones Act* (RA 7916, as amended), the *CREATE Law* (RA 11534), and the *CREATE MORE Law* (RA 12066).

Saudi Arabia and Gulf States (United Arab Emirates, Qatar, and Oman)

Saudi Arabia**:** 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 and a broad range of other organizations, from financial services and aviation to oil and gas. 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. The Regulation covers a broad range of organizations, from financial services and aviation to oil and gas.

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[126], 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 National Cybersecurity Authority 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[127] and a new Data Sovereignty Public Policy[128], 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[129] and controls for data protection service providers[130]. 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.

---

[126] *Cloud Computing Services Provisioning* (2023), https://www.cst.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/CCRF_En.pdf

[127] *Rules Governing the National Register of Controllers within the Kingdom* (Apr. 01, 2024) https://istitlaa.ncc.gov.sa/en/Transportation/NDMO/RulesGoverningtheNationalRegister/Pages/default.aspx

[128] *Data Sovereignty Draft Public Policy* (March 10, 2024) https://istitlaa.ncc.gov.sa/en/Transportation/NDMO/DataSovereigntyPolicy/Pages/default.aspx

[129] *Draft General Rules for Secondary Use of Data,* https://istitlaa.ncc.gov.sa/en/transportation/ndmo/secondaryuserules/Documents/Draft%20General%20Rules%20for%20Secondary%20Use%20of%20Data.pdf

[130] *Draft Controls Governing Commercial, Professional and Non-Profit Activities Related to Personal Data Protection* (May 2025), https://istitlaa.ncc.gov.sa/en/transportation/ndmo/rulesgoverningpdplactivities/Documents/Draft%20Controls%20Governing%20Commercial,%20Professional,%20and%20Non-Profit%20Activities%20Related%20to%20Personal%20Data%20Protection.pdf

Artificial Intelligence Regulation: 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 flows. Its effectiveness is limited by a lack of clarity on security standards, legal conflict resolution, and government intervention rules – resulting in uncertainty over industry's 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.[131] The draft regulations include concerning provisions like: arbitrary thresholds for designating platforms; vague definitions of prohibited conduct, such as for companies to "inappropriately and anti-competitively" favor 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.[132] 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[133], 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[134], 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

[131] *Competition Regulations for Digital Content Platforms* (2022), https://istitlaa.ncc.gov.sa/en/transportation/citc/crdcp/Documents/Competition%20Regulations%20for%20Digital%20Content%20Platforms.pdf.
[132] *CCIA Comments on the Saudi Arabian CITC's Draft Competition Regulations for Digital Content Platforms*, CCIA (Nov. 30, 2022), https://ccianet.org/library/ccia-comments-on-the-saudi-arabian-citcs-draft-competition-regulations-for-digital-content-platforms/.
[133] *Deepfake Guidelines* (Sep. 2024), https://istitlaa.ncc.gov.sa/en/transportation/ndmo/deepfakesguidelines/Documents/SDAIA_Deepfakes%20Guidelines.pdf?trk=public_post_comment-text
[134] Amendments to the Telecommunications and Information Technology Act (July, 2024). https://istitlaa.ncc.gov.sa/en/Transportation/Mcit/information/Pages/default.aspx

publication.[135] 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.[136]

Government Procurement: In 2021, the Saudi government also announced that it would ban any company which does not host its regional headquarters in Riyadh from winning any government contracts. The measure was expected to be fully implemented in January 2024. Such a measure will serve as a market access barrier for U.S. companies.

Internet of Things: In September 2019, the Saudi Communications, Space and Technology (CST) (formerly CITC) published a new IoT Regulatory Framework (including later amendments) setting out licensing and operational requirements for IoT services in the Kingdom. The framework outlines the necessary authorizations for entities providing IoT connectivity and platform services and mandates that all IoT SIMs using in devices imported or deployed within Saudi Arabia must be issued by a locally licensed operator. While there was no specific reference to any provisions applicable to permanent roaming SIMs in respect to IoT services (e.g. connected cars), this requirement effectively prohibits the use of foreign or roaming SIMs (permanent or otherwise) for IoT services in Saudi Arabia.

SASO Arabic Labeling Requirement: The Saudi Standards, Metrology, and Quality Organization (SASO) mandates that all products sold in Saudi Arabia include Arabic labeling on packaging, manuals, and instructions, regardless of industry or use case. This requirement increases compliance costs due to mandatory translation, delays market entry for U.S. products, and creates an unfair barrier for U.S. exporters while favoring regional competitors.

SASO Retesting Requirement for Product Age Limit: SASO requires periodic retesting and recertification of IT and electronic products based on their age, even if they have already passed international safety and compliance standards. The requirement creates supply chain disruptions due to additional testing requirements; imposes unnecessary compliance costs, reducing profitability; and delays product approvals, limiting U.S. companies' ability to compete efficiently.

Gulf States (UAE, Qatar, Kuwait, and Oman)

[135] Aymen, *In Saudi Arabia, no safe harbor for free speech*, ACCESSNOW (Mar. 1, 2024), https://www.accessnow.org/saudiarabiasafeharbor/.
[136] Hassan, *Saudi Arabia issues major update to social media rules for businesses* (Sep. 25, 2025), https://www.caterermiddleeast.com/saudi-arabia/saudi-arabia-issues-major-update-to-social-media-rules-for-businesses

Data privacy and AI rules have been developing across the Gulf region, and particularly in the UAE, Qatar, and Oman. Issues stem from cross-border data restrictions in all three markets, including the within the development of AI regulation in the UAE and updates to its Health Data Law and privacy data law; burdensome AI regulations with the Qatari financial authority; and data privacy measures in Oman within still-developing technological markets. We continue to work with each government but seek greater flexibility in the development of data and AI-related legal frameworks.

Electronic Payment Services: U.S. payment networks face significant regulatory challenges in the Gulf Cooperation Council (GCC) region. Recent geopolitical developments and regional sovereignty efforts have accelerated localization initiatives that threaten market access and operational efficiencies. The geopolitical landscape has prompted the United Arab Emirates (UAE) to prioritize the development of its domestic processing capabilities. By April 2022, the UAE had initiated efforts to establish its payment processing infrastructure, aligning with the other five GCC countries in ending reliance on U.S. payment networks for debit transactions. This move is driven by sovereignty motives, ensuring control over the payments system and protection against potential U.S. sanctions. UAE, Oman, Kuwait, and Qatar have or are developing local schemes. Qatar Central Bank (QCB) is expanding its domestic payment scheme, Himyan, and **has** approached U.S. payment networks to explore co-badging option. We urge USTR to encourage a level playing field for U.S. companies. 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. Moreover, 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.

Qatar has taken a more stringent approach by announcing to discontinue the acceptance of international cards at government outlets, both for locally issued credit cards and internationally issued cards altogether, citing risks of data integrity. This sets a dangerous precedent that could spread to other GCC countries, potentially leading to widespread disintermediation of U.S. payment networks. GCC countries have also emphasized data sovereignty, compelling U.S. payment networks to localize their global infrastructure. The Saudi Central Bank has mandated the localization of certain services offered by U.S. payment networks. Several GCC countries are challenging the rationale behind international schemes charging issuing and acquiring fees on domestic transactions processed outside of U.S. payment networks.

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 localization and sovereignty for CSPs serving public sector and regulated industries has evolved slightly 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 on 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..

Internet of Things: Across the Gulf region, the IoT regulation reflects each country's emphasis on data sovereignty network security and local operator control. In UAE, the Telecommunications and Digital Government Regulatory Authority (TDRA) enforces the IoT Regulatory Framework (2018), requiring IoT service providers to operate through UAE-licensed telecom operators and utilize locally issued SIMs to ensure device traceability and data residency. While permanent roaming for IoT devices is not explicitly prohibited, in practice TDRA requires that devices operating long-term in the UAE use local IMSIs or eSIM profiles provisioned by licensed local operators. In Oman, the Telecommunications Regulatory Authority (TRA), has taken a similar stance by requiring that IoT connectivity be provided via Omani-licensed operators and that devices relying on foreign IMSIs or global SIMs cannot operate on a permanent roaming basis. In Qatar, the Communications Regulatory Authority (CRA) governs IoT deployment under its national spectrum and licensing policies, with IoT services required to comply with Qatari data handling, cybersecurity and lawful interception obligations. While none of the Gulf regulators explicitly prohibit short-term roaming , their combined frameworks effectively localize IoT connectivity and limit the use of foreign or global eSIM profiles within national borders.

South Africa

Data Localization: South Africa's 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.

Public Procurement: 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.

Electronic Payment Services: 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.

Audiovisual
Broadcast Quota: In 2021, the Independent Communications Authority of South Africa (ICASA) reinstated local content quotas for television. This followed ICASA's 2020 decision to fully exempt "television broadcasting service licensees" from compliance with local television content quotas during the COVID-related National State of Disaster.

"Must Provide" Requirements: In 2019, ICASA published its draft findings on the '*Inquiry into Subscription Television Broadcasting Services*.' This report suggests regulatory intervention in the pay-TV market to address perceived and alleged anti-competitive conduct from dominant market players. In January 2025, ICASA revived the inquiry by publishing a Supplementary Discussion Document expanding the market definition to include over-the-top (OTT) services. Notably, the document does not propose any regulatory intervention and acknowledges that the market is competitive. Industry stakeholders are closely monitoring this inquiry and hopes that the South African government will ensure that any regulatory interventions into the pay-TV and OTT market are informed by international best practices, current market realities, and preserve the contractual freedoms of all parties concerned, all while developing a legislative and regulatory framework that is conducive to investment and growth.

Digital Platform Media Taxes: The South African government is advancing new regulations to force revenue transfer from online platforms to through two key initiatives. A draft White Paper on Audio

and Audiovisual Media Services[137] 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[138] 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 Services: 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 we urge USTR to work to assure a level playing field for U.S. companies.

[137] Department of Communications and Digital Technologies (2025), *The Draft White Paper on Audio and Audiovisual Media Services and Online Safety*, https://www.gov.za/sites/default/files/gcis_document/202507/52972gen3369.pdf
[138] Competition Commission, South Africa, *Media and Digital Platforms Market Inquiry* (February 2025), https://www.compcom.co.za/wp-content/uploads/2025/02/CC_MDPMI-Provisional-Report_Non-Confidential-Final.pdf

Taiwan

Government Procurement– 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.

Duplicative Local Testing Requirements: 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, create 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.

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.

Media Taxes on Online Platforms: 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.

Content Moderation and Advertising Restrictions: The Taiwan Tobacco Hazards Prevention Act aims to regulate illicit sponsored user content. The Act's critical flaw is its failure to assign any liability to the content creator—the party that procured the advertising. Instead, it improperly holds the intermediary platform solely responsible, defining sponsored posts as commercial "advertisements" and ignoring the fundamental distinction between paid advertising and user-generated content. This results in severe, repeated fines for platforms over content they did not commission. . This not only constitutes a non-tariff barrier to trade but undermines the free flow of information online which, in some instances, is essential to U.S. business interests and hinders the development of a vibrant digital public sphere.

Thailand

Audiovisual:
Foreign Ownership Restrictions: Foreign ownership of terrestrial broadcast networks is prohibited in Thailand. Further, rules established in 2015 require National Broadcasting and Telecommunications Commission (NBTC) approval when a television license holder seeks to either invest more than 25 percent directly or more than 50 percent indirectly in another licensed company. This rule severely limits investment and creates new barriers to entry for U.S. companies.

Screen Quota: Section 9(5) of the Motion Picture and Video Act (MPVA) allows the Film Board to establish ratios and quotas for foreign films. If implemented, such restrictions would create new barriers and reduce consumer choice. The Ministry of Culture proposed replacing the MPVA with a new Film Law in June 2025; the latest draft helpfully removes the screen quota.

Television Must-Carry Requirements: Recent media reports suggest the 2012 rules will finally be reversed by the NBTC. Until this happens the regulations raise important IPR issues, precluding the ability of rightsholders to enter exclusive distribution arrangements in Thailand.

OTT/VOD Regulation: Various government agencies, including the NBTC, have publicly noted their interest in regulating OTT, including the possibility of requiring streaming operators to set up a local presence to respond to government requests around content that the government finds objectionable (a form of mandatory content moderation) as well as to "promote" local content via local content investment obligations. Additionally, Thailand is considering a proposal to revise the Film Law, expanding the definition of "film" to include streaming and online audiovisual content. The proposal also introduces new rating, notification and registration obligations that increase compliance burdens for service providers.

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.

Platform Economy Act (PEA): Thailand is drafting legislation to regulate digital services, adopting concepts from the EU's Digital Services Act (DSA) and Digital Markets Act (DMA). Once the proposed PEA becomes law, it will supersede other existing laws, such as the DPS Decree and the

relevant provisions under the Electronic Transactions Act of 2001. Under the proposed PEA, 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 Services (DPS) Decree: The DPS Decree came into force in 2023 and 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. However, the implementation of this regulatory framework has evolved beyond its original scope, with the Electronic Transaction Development Agency (ETDA) extending registration requirements to a broader range of digital service providers, including 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 DPS Decree imposes significant obligations on digital service providers, including: requirements for relevant services to notify the government prior to starting business operations, with large-scale services subject to additional requirements such as mandatory risk management systems and internal compliance managers; requirements for local representatives with unlimited liability; reporting requirements; unclear user ID verification rules; and 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: The 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[139], the Ministry

[139] *Computer-Related Crime Act B.E. 2550 (2007) (as amended in 2017)*, https://www.mdes.go.th/law/detail/3618-COMPUTER-RELATED-CRIME-ACT-B-E--2550--2007-

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.[140] Similarly, the controversial Cybersecurity Act[141] grants officials broad authority to search and seize data and equipment in what are vaguely defined as "national emergencies," enabling potential government surveillance.[142]

Logistics Regulation: The Electronic Transactions Development Agency (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.

Digital Platform Fair Competition Draft Rule: 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.

Customs: Thailand Customs incorrectly classifies specific monitors for used in collaboration products under HS Code 8528.59.10 at 20% instead of HS Code 8528.52.00 at 0%. The United States' duty rate for HS Code 8528.59.10 is zero, making this an example of an unfair non-reciprocal tariff.

[140] *Freedom on the Net 2023: Thailand*, FREEDOM HOUSE (last visited Oct. 14, 2024), https://freedomhouse.org/country/thailand/freedom-net/2023; *Over a million pieces of fake news posted online in two years*, THE NATION (Dec. 29, 2021), https://www.nationthailand.com/in-focus/40010570

[141] *Cybersecurity Act B.E. 2562 (2019)*, https://www.mdes.go.th/law/detail/3572-Cybersecurity-Act-B-E-2562--2019-

[142] Techcrunch, *Thailand Passes Controversial Cybersecurity Law*, https://techcrunch.com/2019/02/28/thailand-passes-controversial-cybersecurity-law/.

Türkiye

Digital Services Tax: Türkiye continues to administer a DST that took effect in March 2020 and that USTR determined to be discriminatory in a Section 301 investigation. We are extremely concerned that a bill submitted to the Turkish Parliament in October 2025 threatens to boost the DST from 7.5% to 12.5%. The 12.5% rate would only apply to foreign providers, while domestic suppliers subject to the tax would retain the 7.5% rate (which is already not only an extremely steep tax, but also discriminatory in nature).

The global revenue threshold for the current 7.5% tax is €750 million, with a local threshold of ₺20 million and it applies to revenue generated from the following services: (1) digital advertising, (2) online streaming and sales of audio and audiovisual content, and (3) social networking services.

Additionally, in 2024, Türkiye amended Law No. 6563[143], 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.

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. The Ministry of Industry and Technology's R&D body (TUBITAK) introduced strict data localization requirements for cloud usage.

Strict data localization requirements are also applied to the financial services industry where the banking regulation and supervision agency require primary and secondary information systems to be hosted in Turkey.

The Regulation on Information Systems of Banks, published on March 15, 2020, requires banks and financial services to keep their primary (live/production data) and secondary (backups) information systems in Türkiye.[144] While the Regulation establishes a framework for use of cloud services as an outsourced service, it only applies to services located 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.

---

[143] *Turkey: New Era On Turkish E-Commerce Law*, INAL LAW OFFICE (last visited Oct. 14, 2024), https://www.inal-law.com/new-era-on-turkish-e-commerce-law/.

[144] Ilay Yilmaz et. al, *New Regulation on Bank IT Systems and Electronic Banking Services*, Lexology (Mar. 18, 2020), https://www.lexology.com/library/detail.aspx?g=820f9766-219b-4196-9554-bfc715fd1676.

Electronic Payment Services: 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.

Competition/Ex Ante Rules: : In October 2022, Türkiye proposed an amendment[145] to its competition law that largely mirrors the EU's Digital Markets Act. The draft law imposes significant obligations on large digital platforms, 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 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.[146] These excessive regulatory requirements, *de facto* preference for Turkish companies, and pressures for localization represent clear barriers for U.S. companies.

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)[147], 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

[145] *Law No. 4054 on the Protection of Competition*, MONDAQ (April 11, 2019), https://www.mondaq.com/advicecentre/content/1540/Law-No-4054-on-the-Protection-of-Competition-Competition-Law

[146] U.S. Department of State, *2024 Investment Climate Statement: Turkey*, https://www.state.gov/reports/2024-investment-climate-statements/turkey.

[147] *Regulation of Publications Made on the Internet and Fighting against Crimes Committed Through Publications Law on Amendment of the Law*, https://www.resmigazete.gov.tr/eskiler/2020/07/20200731-1.htm

moved quickly to enforce these rules, imposing fines[148], advertising bans[149], and bandwidth restrictions on non-compliant firms.

The government further intensified its control with Law No. 7418 (Amendment of Press Law, and Certain Laws)[150] 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.[151] Subsequent regulations in April 2023[152] 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.

Internet of Things: Türkiye has implemented measures restricting permanent roaming, which create barriers to the deployment of global IoT services. The Information and Communication Technologies Authority (BTK) issued Decision No.2019/DK-TED/053 limiting international permanent roaming to 90 days within a 120-day period and requiring all equipment to operating on e-Sims to use profiles provisioned by Turkish licensed operators. Furthermore, the decision mandates that all related data and infrastructure associated with these services be hosted within Türkiye. Operators were required to comply by February 2020.

---

[148] AP News, *Türkiye Fines Social Media Giants for Breaching Online Law* (Nov. 4, 2020), https://apnews.com/article/business-Türkiye-media-social-media-560de2b21d54857c4c6545c1bd20fc25.
[149] Reuters, *Türkiye Slaps Ad Ban in Twitter Under New Social Media Law* (Jan. 19, 2021), https://www.reuters.com/article/us-Türkiye-twitter/Türkiye-slaps-ad-ban-on-twitter-under-new-social-media-lawidUSKBN29O0CT.
[150] Available at https://www.tbmm.gov.tr/Yasama/KanunTeklifi/316898.
[151] 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.[5]
[152] Lexology, *New Regulation from ICTA on Social Network Providers*, https://www.lexology.com/library/detail.aspx?g=a799c704-d8c6-4235-a0cc-2f40dc78d586.

Ukraine

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 Kingdom

In May 2025, as part of the announcement for the General Terms for the United States of America and the United Kingdom of Great Britain and Northern Ireland Economic Prosperity Deal,[153] the White House said the US and UK plan to negotiate "an ambitious set of digital trade provisions that will include within its scope services, including financial services." CSI strongly supports such an effort and urges USTR to begin negotiations as soon as possible.

Digital Services Tax: The UK imposes a 2% DST on 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, and 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. In 2024, a UK political party called for raising the DST from 2% to 6% in its election platform,[154] highlighting the continued salience of this issue. USTR should resume its earlier Section 301 process to compel removal of the discriminatory and burdensome tax.

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 October 2025.

[153] https://www.whitehouse.gov/briefings-statements/2025/05/general-terms-for-the-united-states-of-america-and-the-united-kingdom-of-great-britain-and-northern-ireland-economic-prosperity-deal/

[154] *Triple tax on social media giants to boost mental health in schools*, Liberal Democrats (Sept. 27, 2023), https://www.libdems.org.uk/press/release/triple-tax-on-social-media-giants-to-boost-mental-health-in-schools.

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. The intention of the Act was that the most onerous rules would apply to a small number of "Category 1" firms – the largest social media services. However, there is now discussion on whether to include services like marketplaces as well. 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.

Vietnam

Data Law and implementing Decrees 165 and 169: In November 2024, the National Assembly passed the Law on Data (No. 60/2024/QH15, or Data Law). The Data Law went into force together with its implementing Decrees 165 and 169 on 1 July 2025. The Data Law and its implementing decrees have duplications with the PDP Law on regulations on personal data governance and impose sweeping restrictions on the classification and cross-border transfer of data, effectively creating data localization obligations that disadvantage foreign firms. The Prime Minister Decision No. 20/2025 dated 1 July 2025 supporting the execution of the Data Law and its Decree introduces new broad 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 service to Vietnamese customers.

Personal Data Protection Law (PDPL): The PDPL passed in June 2025 and will go into effect January 1, 2026. A draft implementing decree (draft PDPD) has been issued 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 data). The PDPL and the draft PDPD expands 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 measures would impede the ability of companies that need to process cross-border data from continuing to offer services to customers in Vietnam.

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.[155] 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 favouring local service providers.

The 2018 Cybersecurity Law is currently undergoing revision. However, the draft revisions (September 2025 version) continue to import the 2018 Cybersecurity Law's broad and vague data localization requirement. The draft reivisions would also require service providers on telecom network, 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 their cross-border provision of services.

National Digital Transformation Strategy – Domestic Preferences: Under its 2020 National Digital Transformation Strategy[156], Vietnam is implementing policies to control cross-border platforms and promote domestic industry. The government has issued cloud standards[157] 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.

Draft 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 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.

---

[155] Khank Vu, *Vietnam Says Facebook Violated Controversial Cybersecurity Law*, REUTERS (Jan. 8, 2019, 12:49 AM), https://www.reuters.com/article/us-vietnam-facebook/vietnam-says-facebook-violated-controversial-cybersecuritylaw-idUSKCN1P30AJ; Jeff Olson & Mai Phuong Nguyen, *Vietnam Quick to Enforce New Cybersecurity Law*, HOGAN LOVELLS CHRONICLE OF DATA PROTECTION (Mar. 6, 2019), https://www.engage.hoganlovells.com/knowledgeservices/news/vietnam-quick-to-enforce-new-cybersecurity-law.

[156] https://english.luatvietnam.vn/decision-no-749-qd-ttg-on-approving-the-national-digital-transformation-program-until-2025-with-a-vision-184241-doc1.html

[157] Under *Official Letter No. 1145/BTTTT-CATTT* (https://thuvienphapluat.vn/cong-van/Cong-nghe-thong-tin/Cong-van-1145-BTTTT-CATTT-2020-tieu-chi-chi-tieu-ky-thuat-danh-gia-Chinh-phu-dien-tu-439232.aspx) and *Official Letter No. 783/THH-HTDLS* (https://thuvienphapluat.vn/cong-van/Cong-nghe-thong-tin/Cong-van-783-THH-HTDLS-2020-Tai-lieu-huong-dan-ung-dung-dich-vu-dien-toan-dam-may-487024.aspx).

Audiovisual
The amended Cinema Law (2022) requires 15% of annual screen time to be devoted to Vietnamese feature films, which will be increased to 20% in 2026. In the television sector, foreign content is limited to 50 percent of broadcast time, and foreign programming is not allowed during prime time. Foreign channels on pay-TV services are capped at 30 percent of the total number of channels the service carries, with additional onerous requirements on editing and translation, restrictions on commercials, and censorship requirements.

Decree 71 expanded the scope of existing pay-TV regulations in 2022 to include SVOD services. Most concerning is a non-transparent licensing scheme that applies to the investment law, which requires a local presence or joint venture in addition to onerous censorship provisions for any SVOD service that offers any content not considered to fit within a narrow definition of "film" (which would be regulated separately under the Cinema Law). To date, no SVOD service has been granted a licence, and the only beneficiary of the current regulatory environment is piracy operators in Vietnam.

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.

Artificial Intelligence: In July 2024, the Vietnam government proposed provisions relating to artificial intelligence (AI) in its draft Digital Technology Industry Law (DTI Law).[158] 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. 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.

[158] Thai Gia Han & Nguyen Trung Nghia, *Vietnam: A New Chapter for Digital Technology Industry*, LEXOLOGY (Aug. 22, 2024), https://www.lexology.com/library/detail.aspx?g=b0d22a3f-52d6-4d12-b20d-0586de47dc98; *See also Vietnam: New draft Law on Digital Technology Industry and draft Data Law*, BAKER MCKENZIE (July 9, 2024), https://insightplus.bakermckenzie.com/bm/data-technology/vietnam-new-draft-law-on-digital-technology-industry-and-draft-data-law.

Electronic Payments: SBV Circular 18/2024/TT-NHNN), 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.

E-Commerce: Vietnam has unveiled a new *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.

Decree 85/2021 includes in its scope cross-border platforms without a local presence in Vietnam (including websites in Vietnamese language or exceeding 100,000 transactions per year). The Decree also requires local and cross-border e-commerce platforms to provide vendors' information to authorities upon request and take-down information on goods that violate Vietnamese laws within 24 hours.

Express Delivery Services: Decree No. 68/2016/ND-CP requires that customs clearance operations only take place on land that is designated adjacent to the airport, rendering some carriers' long-held land and operations non-compliant., Decree 67/2020/ND-CP (amending Decree 68) allows enterprises designated under postal law to clear express shipments without being located within the designated adjacent airport land. The only enterprise that satisfies this description is Vietnam Post.

Advertising: Decree 70/2021/ND-CP (amending decree 181/2013/ND-CP) regulates advertising content, including Apps and social media. The draft lacks clarity on definitions, procedures and restrictions, imposes onerous reporting requirements, and obliges providers to actively manage ad content and placement. The draft revised Law on Ads that is being submitted to the National Assembly in May 2025 continues requiring proactive screening of violative content for ad placement in Decree 70. This approach is operationally infeasible for platforms based on the sheer volume of content that is uploaded by users on a continuous basis.

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.

Digital Services Taxes: The Tax Administration Law, effective July 1, 2020, taxes cross-border e-commerce and other digital services.[159] The Ministry of Finance issued Circular 80 providing guidance on the Law and its Decree 126 in September 2021.[160] 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.

VAT on exported services: The Law on VAT defines exports of services subject to the 0% VAT rate as "Services provided directly to organizations and individuals abroad and consumed outside of Vietnam…," but it lacks clear and specific guidance on the criteria for determining whether an intangible service is "consumed outside of Vietnam". As interpretations among provincial tax authorities vary, companies face uncertainty in expense planning. The forthcoming Decree and Circular detailing the implementation of the VAT Law should provide clear guidance on the criteria for zero-rating exported services that aligns with international standards. Services that are provided to overseas entities and have their economic benefit realized outside of Vietnam should be recognized as qualifying for 0% VAT.

Civil Cryptography Trading and Import License Requirements: The Government Cipher Committee (GCC) requires that the importation and exportation of any product containing specific cryptographic functionality obtain specific permits and licenses. Such licenses take months to obtain, sometimes due to unclear follow-up requests by the GCC. Companies have also experienced inconsistent/non-transparent approval or rejection of their applications. These burdensome requirements, and the required follow-ups by the applicants, limit the ability for companies investing in Vietnam to import/export critical hardware. A new regulation for cryptographic certification equipment, the Circular 23/2022/TT-BQP of Ministry of Defense, has introduced further uncertainty, requiring 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

[159] Alberto Vettoretti, *Vietnam's Tax Administration Law Takes Effect*, R Global (Aug. 7, 2020), https://www.irglobal.com/article/vietnams-tax-administration-law-takes-effect-in-july-2020-0f67/.
[160] *See* Nguyen Thuy Han & Duong Chau Thanh, *Circular 80/2021/TT-BTC guiding the Law on Tax Administration, Decree 126/2020*, THU VIEN PHA PLUAT (Oct. 9, 2021, 8:13 AM), https://thuvienphapluat.vn/tintuc/vn/thoi-su-phap-luat/chinh-sach-moi/37945/thong-tu-80-2021-tt-btc-huong-dan-luat-quan-ly-thue-nd-126-2020.

documentation are unclear, and company's 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 import 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. This policy is unfair, because refurbished products are "like" products to new, so prohibiting their import violates Vietnam's international trade commitments. Products and components are essential in order to continue supporting customer 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.

Banking: Each foreign bank branch (for instance Hanoi Branch and HCMC Branch) is required to maintain a separate balance sheet, report separate audited financials and maintain prudential ratios separately. These requirements create an administrative burden and limits operational and financial flexibility. Foreign banks should have the ability to maintain a single balance sheet across branches.