1919 S. Eads St.
Arlington, VA 22202
703-907-7600
CTA.tech

October 17, 2024

Ambassador Katherine Tai
United States Trade Representative
Office of the U.S. Trade Representative
600 17th St. NW
Washington DC, 20508

**Re: Request for Comments on Significant Foreign Trade Barriers for the 2025 National Trade Estimate Report (Docket Number: USTR-2024-0015)**

Dear Ambassador Tai:

The Consumer Technology Association appreciates the opportunity to provide input into the Biden-Harris Administration's efforts to compile the 2025 National Trade Estimate (NTE) report cataloguing significant foreign barriers to trade and investment. This report serves as an important national resource for industry participants to communicate their trade barrier concerns to the U.S. government and for the government to prioritize its efforts to address those barriers.

CTA represents the more than $505 billion U.S. consumer technology industry, which supports more than 18 million U.S. jobs. Our members are comprised of over 1,300 companies from every facet of the consumer technology industry, including manufacturers, distributors, developers, retailers, and integrators, with 80 percent of CTA members being start-ups or small and mid-sized companies. CTA also owns and produces CES®—the most influential technology event in the world—which showcases and serves as a forum for discussion of international policies concerning existing and new technologies, international technology trade and investment, and global opportunities and challenges facing the consumer technology industry.

CTA's members sit at the center of the global economy and its digitalization. They design and manufacture technology products for consumers and businesses in the United States and all over the world. They design and deliver software and digital services to consumers through those products. Importantly, they rely on efficient and free flows of data across borders to operate, compete, grow their businesses, and support the needs of their customers. CTA's small business and startup members in particular benefit from U.S. efforts to prevent and proactively address barriers to trade and investment, which enables them to operate at lower costs and scale up quickly to deliver their products to consumers in the United States and global markets.

We are concerned that the Office of the U.S. Trade Representative (USTR) removed a sizable collection of barriers from the 2024 NTE Report that had been included in earlier reports, with a targeted de-prioritization of barriers to digital trade. According to a multi-association analysis, "between 2023 and 2024, USTR reduced the number of country analyses of data localization mandates by over 70 percent (from 24 countries in 2023 to seven in 2024) and removed concerns with respect to at least 80 digital trade-related measures."[1] Several harmful digital trade barriers were omitted from the 2024 NTE report, including measures that restrict cross-border data flows, mandate data localization, require disclosure of source code and/or algorithms, and favor domestic competitors over U.S. firms.

USTR is statutorily obliged to "identify and analyze" any "barriers to, or distortions of" U.S. electronic commerce.[2] The key issue with the 2024 NTE Report is that the measures USTR has excluded are problematic in a number of ways, including through their discriminatory nature, possible infringement of intellectual property rights, and potential violation of trade agreements. While USTR can support the right of our trading partners to regulate, it should also advocate for U.S. businesses and workers by pushing foreign governments to remove these trade barriers. This includes ensuring that regulations are narrowly tailored to address their intended objectives, do not discriminate against U.S. goods and services, provide sufficient time for compliance, are based on the best available evidence, and are developed transparently with the consideration of public comments. Doing so will form a breakwall against the rising tide of global digital protectionism, particularly the egregious digital measures imposed by authoritarian regimes.[3]

We strongly urge USTR to rectify these past omissions by reintegrating the digital trade barriers outlined in our comment in the 2025 NTE report.

Along the same lines, we call on USTR to take a strong stand against these measures in its engagements with our trading partners in its bilateral and regional initiatives and in the context of existing U.S. free trade agreements. If the principle of non-discrimination collapses, U.S. businesses will then operate in far less certain world where the rule of law fades and the rule of the mighty prevails.

CTA's comments for the 2025 NTE cover a wide range of trade and investment barriers that, if addressed, could facilitate faster and less costly supply chain resiliency and

---

[1] *TechNet-Led Multi-Association Memorandum to Congress Expresses Concerns with the USTR's 2024 National Trade Estimate Report*, TechNet (Apr. 15, 2024), https://www.technet.org/media/technet-led-multi-association-memorandum-to-congress-expresses-concerns-with-the-ustrs-2024-national-trade-estimate-report/.
[2] 19 U.S.C. § 2241(a)(1)(A)-(B).
[3] *U.S. Chamber and Other Associations Letter to NSC/NEC on Digital Trade*, U.S. Chamber of Commerce, (Nov. 7, 2023), https://www.uschamber.com/international/trade-agreements/u-s-chamber-and-other-associations-letter-to-nsc-nec-on-digital-trade.

diversification. They also concern barriers that the Administration should address to help U.S. companies operate and compete in other markets by creating a more level playing field for their products and services.

Our comments below are divided into three Annexes: 1) proposed barriers; 2) existing barriers; 3) existing data localization requirements. The types of barriers include tariffs, trade facilitation and customs measures, restrictions on cross-border data flows, forced localization requirements, technical barriers to trade, good regulatory practices, digital regulatory measures, and measures concerning critical and emerging technologies, such as artificial intelligence (AI).

CTA looks forward to working with you, USTR staff, and the interagency to prevent and address these barriers to trade, diversify consumer technology supply chains, and reestablish the rule of law in the multilateral trading system. Thank you for reviewing our comments. We are happy to serve as a resource as you draft the 2025 NTE.

Sincerely,

Ed Brzytwa
Vice President of International Trade
Consumer Technology Association

Michael Petricone
Senior Vice President of Government Affairs
Consumer Technology Association

## Table of Contents for Annexes to CTA Comments

# Annex 1 – Proposed Measures

## Brazil

### Digital Trade Barriers

On November 2022, Brazil's Congress introduced Bill 2768, inspired by the European Union's Digital Markets Act (DMA), that designates the National Telecommunications Agency (ANATEL) as the primary regulator of "digital platforms" in Brazil. The bill also establishes a regulatory framework for the organization, functioning, and operation of "digital platforms" that offer services to users in Brazil. The bill uses vague terminology and does not clearly describe the specific requirements needed to comply. Instead, it grants ANATEL significant discretionary authority to define terms and create rules. While the vague language in the bill makes it hard to determine the specific obligations that would apply to U.S. companies, but overall, the bill would, at minimum, increase compliance costs and may require the restructuring of business operations. The bill has not yet passed and is waiting for the Rapporteur's Opinion at the Economic Development Committee in the Brazilian Chamber of Deputies.

### Privacy

The Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act, which were introduced in Bill C-27, are currently being studied in a clause-by-clause review by the House of Commons Industry Committee. The bills aim to update Canada's current privacy law for the private sector and introduce new privacy protections for minors, bringing Canada's privacy approach in closer alignment with European data protection and privacy standards. While the Canadian 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, 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

The Artificial Intelligence and Data Act (AIDA), which was introduced in Bill C-27 alongside the two federal privacy proposals above, is loosely modeled on the EU's AI Act. AIDA would require those responsible for AI systems to assess potential harm of outputs, develop mitigation plans to manage risk, and publicly disclose when high-impact systems are used. Penalties would include administrative monetary penalties, and criminal liability in some instances. While the Government appears open to amendments that address some concerns voiced by industry – including lack of clarity on developer/deployer responsibility, no clear definition for "high impact systems" –

there remain concerns that the government will take an overly burdensome regulatory approach to AIDA, which could risk interoperability across North America.

## Korea

### Monopoly Regulation and Fair Trade Act

On September 9, 2024, South Korea abandoned its controversial Platform Competition Promotion Act (PCPA), which had been criticized for its ex-ante regulation approach. The government will now amend the Monopoly Regulation and Fair Trade Act to adopt an ex-post regulatory framework. This change means that companies will be assessed for dominance only after potential violations occur, rather than being preemptively targeted. U.S. firms would still be significantly impacted, facing stricter regulations and higher fines—up to eight percent of related sales—if they meet thresholds of 60 percent market share, 4 trillion won in sales ($3.07 billion), and more than 10 million users. The Korean Fair Trade Commission will soon consult with the National Assembly on these amendments. This approach risks creating an uneven playing field for U.S. companies competing against rapidly growing foreign competitors and may potentially breach the U.S.-Korea Free Trade Agreement.

## Indonesia

### Restrictions on imports under $100

On September 27, 2023, the Ministry of Trade (MOT) issued Regulation No. 31/2023 (Reg 2023), which prohibits foreign merchants from selling any goods valued below $100 to Indonesian customers via online marketplaces and includes several other discriminatory requirements that will restrict imports and foreign investment in Indonesia. For example, the regulation requires foreign ecommerce platforms to receive a permit from the MOT 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.

## The Philippines

### Data Localization

The Philippines' President's Office is considering a draft Executive Order that would mandate data localization for its public sector, healthcare and health insurance sector, any financial service institutions supervised by Bangko Sentral, and any private sector entity that processed sensitive personal information or subscriber information. If issued, the Executive Order would be a significant step back in the country's digital trade policy,

which historically has been one of the more progressive in the ASEAN region. While the Executive Order appears to have lost much of its traction for now due to industry outcry, significant concerns remain that proponents of the measure will attempt to move this policy through the Philippines legislature or as an Executive Order at a later time.

# Annex 2 – Existing Measures

## Canada

**Digital Services Tax (DST)**

The Digital Services Tax Act came into force on June 28, 2024. The Act imposes a three percent tax on revenue from certain digital services provided by businesses with gross

revenues of at least €750 million and in-scope Canadian revenues of at least $20 million (CAD). The tax would still apply retroactively to relevant revenues earned as of January 1, 2022, and would not be creditable against Canadian income tax. Canada moved forward with the DST despite the agreement from nearly all 140 economies participating through the Organization for Economic Cooperation and Development's (OECD) negotiations on international tax rules to extend a moratorium on DSTs through December 31, 2024. Canada's DST discriminates against U.S. companies and contravenes Canada's obligations under both the U.S.-Mexico-Canada Agreement (USMCA) and the World Trade Organization (WTO).

## China

### 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 its Personal Information Protection Law (PIPL) and Data Security Law (DSL), which, along with the Cybersecurity Law (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.

With respect to security assessments, the Cyberspace Administration of China (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 Critical Information Infrastructure (CII) operators and other companies that reach certain thresholds of data. The Measures put forward specific requirements for the data exit security assessment, stipulating that data processors shall conduct a data exit risk self-evaluation before applying for a 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.

The mechanism imposes heavy compliance burdens and costs on data processors. Furthermore, it requires foreign companies to reveal corporate data mapping and cross-border data flow transfer routes, which carry high risks of divulging trade secrets and key IP rights.

As noted above, in addition to personal data, cross-border flow of "important data" also triggers a security assessment. However, the definition of 'important data' and important data catalogues have yet to be finalized, resulting in significant uncertainty for data handlers in some key sectors. More, we have seen the trend of Chinese industry regulators leveraging and expanding the concept of "important data" within their areas of authority, proposing data localization and cross-border data flow restrictions in

various industries, such as financial services, auto, ride hailing, internet publication, mapping, and pharmaceutical sectors.

Perhaps understanding 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 issued new rules and requirements regulating and promoting cross-border data flows, which would limit instances in which a data exit security assessment would be necessary. In particular, the final rules state that personal data transfers due to human resource management and contractual transactions, such as cross-border e-commerce, cross-border payments, plane ticket purchases and hotel bookings, and visa applications be exempted under the aforementioned cross-border personal data flow management mechanism. While somewhat helpful, these new rules and regulations do very little to address the broader concerns with China's approach to cross-border data transfers.

## Colombia

### Digital Services Tax

In August 2022, the Colombian government introduced a significant economic presence (SEP) proposal, a new tax on gross income derived by overseas providers of goods and digital services into Colombia. In November 2022, the Colombian government approved the SEP rule (Law 2277/22, Article 57). The tax applies to both the sale of tangible goods, but also to an enumerated list of digital services, including cloud services. As such, the SEP provisions apply to more than companies operating in the digital services sector. For goods and services, a person is in scope if it has a deliberate and systematic interaction with the Colombian market (maintaining a marketing interaction with 300,000 or more users or customers located in Colombia) and if it obtains gross income of approximately USD 300,000 or more from users in Colombia. The SEP rule entered into force on January 1, 2024 as the first digital services tax (DST) imposed in the Latin American region.

The rule imposes a 10 percent withholding tax on a non-resident with a deemed SEP in Colombia. The tax is imposed at the source, on the total payment made to the non-resident for the sale of goods and/or provision of services. Using other enacted DSTs and other relevant similar measures as a benchmark, the 10 percent proposed rate for withholding is unusually high. There is an elective, alternative regime, whereby the non-resident can elect to pay a three percent tax on the gross income derived from the sale of goods and/or the provision of digital services from abroad, sold, or provided to users in Colombia when registered.

The Colombian rule represents a significant departure from international tax norms, which allocate taxing jurisdiction on the basis of nexus (i.e., the concept of permanent establishment, physical operations, workforce, etc.) or source (the location of income-

generating activity), rather than destination-based criteria. The proposal does not align with the current ongoing negotiations at the OECD/G20 Inclusive Framework and violates the spirit of both the 2021 DST standstill agreement, and the conditional, one-year extension reached in July 2023. The Colombia government agreed to both extensions, but still moved forward. A new gross-basis tax imposed on non-residents of Colombia on income derived from sales to the Colombian market and would create barriers to trade to U.S. companies engaging with the Colombian market.

The SEP may constitute a violation of several provisions of the U.S.-Colombia Trade Promotion Agreement (USCTPA), including the non-discrimination obligation, prohibitions against local presence requirements, and goods market access. The new tax imposed on a U.S. company that is deemed to have an SEP is the equivalent of a tariff in that it raises the price of imported goods and does not affect domestically produced products. With regard to the SEP imposed on providers of digital services, the tax de facto discriminates against U.S. service suppliers of digital services. Additionally, the decreased three percent tax rate for those non-residents who elect to file a return creates an incentive to establish a local presence, as Colombian legislation does not have procedures for foreign entities without a permanent presence in Colombia to file an income tax return. Consequently, in order for a non-Colombian to benefit from the lower rate, it is *de facto* necessary for the non-resident to establish a local presence.

### Trade facilitation

Under the USCTPA, Colombia committed to modernize its customs procedures through automation and the use of electronic systems. For example, Colombia agreed to "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. 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 has yet to implement these commitments and still requires physical documents at the border.

## EU and EU Member States

### Digital Services Act (DSA)

The DSA creates new rules for the handling of illegal third-party content on cloud hosting and intermediary services in Europe, 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 is almost entirely made up of 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 additional restrictions on targeted advertising and obligations for VLOPs and Very Large Online Platforms and Search Engines (VLOSEs) to provide alternative recommendation systems, despite the lack of any clear evidence that the size of a company indicates additional risk. The EU announced the designation of VLOPs on April 25, 2023, and of the 19 services announced, 16 were American, two were Chinese (AliExpress and TikTok), and one was European (Zalando). The 19 designated VLOPs were required to be in full compliance by August 25, 2023, seven months earlier than all other companies, even though VLOPs and VLOSEs face a significantly larger compliance burden.

**Digital Markets Act (DMA)**

The DMA, which was concluded in the first half of 2022 and entered into force in November 2022 despite U.S. government concerns regarding the discriminatory treatment of U.S. companies, creates significant and burdensome requirements for only a small set of American firms. The regulatory approach to impose “one-size-fits-all” obligations to different digital services with different business models is inadequate and could hamper innovation. The DMA restricts the use of data, creates new data access and portability obligations, and introduces interoperability requirements with a short implementation period and the threat of significant penalties. Despite commitments made by the European Commission (EC) to the Biden Administration before the DMA was finalized, no European companies were designated as “gatekeepers.” On September 6, 2023, the EC designated 22 core platform services as gatekeepers from 6 companies: Amazon, Alphabet, Apple, ByteDance, Meta, and Microsoft as gatekeepers. These six Gatekeepers – five U.S. headquartered companies and one company headquartered in China – will need to comply with DMA’s substantive obligations within 6-months, with the EC as the main enforcer. By May 13, 2024, the EC designated two additional core platform services and the U.S. travel technology company Booking under the DMA.

**Internet Infrastructure Levy**

The EC launched a consultation exploring the possibility of requiring over-the-top providers “of a certain size” to bear the cost of the development of telecom infrastructure in Europe. The internet infrastructure levy, supported by European telecommunications companies, would initially require six U.S. companies to pay €20 billion annually to telecommunications operators to support infrastructure development. Introducing an internet levy to subsidize EU telecommunications companies would have significant consequences for the digital economy and would directly discriminate against U.S. companies who are already significantly invested in European networks and internet infrastructure. The EC opened a consultation on this proposal on February 23, 2023 and comments were due on May 19, 2023. Despite strong opposition to the

proposal through the consultation, including from the National Telecommunications and Information Administration, and opposition from a large group of EU Member states, the EC is pushing forward with the proposal.

**Data Act**

The Data Act regulates access to and transfer of data generated by connected products and related services. It forces sharing of data and the transfer of trade secrets under certain conditions. It also creates new discriminatory barriers for "gatekeepers" designated under the DMA. In particular, users will not be able to utilize a new portability right established by the Data Act to transfer their data to "gatekeepers." The Data Act further creates new obligations on cloud service providers on the access and transfer of non-personal data following third country access requests, leading to a new potential conflict of EU and third-country law. According to the Data Act's impact assessment, concerns over unlawful access to data by authorities not subject to EU legislation is one of the main drivers for the data access and transfer restriction, which implies an equivalence between U.S. and Chinese surveillance laws. Lastly, it imposes switching obligations on cloud service providers where the associated costs will disproportionately fall on U.S. CSPs because of their customer base and the maturity and complexity of their service portfolio. The EU Institutions reached a final political agreement on the Data Act in July 2023, formal adoption occurred in November 2023 with rules applying on September 12, 2025.

### EU Foreign Subsidies Regulation (FSR) Implementation

In July 2023, the EU's FSR entered into force, giving the EC new powers to target economic distortions in the EU market caused by foreign subsidies. While the EC claims that the FSR targets subsidies from non-market economies, the FSR will subject 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 percent of companies' global revenue.

In July, the EC published an Implementing Regulation (IR) laying out procedural mechanisms for the application of the FSR. The IR significantly reduced the scope of

the FSR by, inter alia: (i) limiting the most onerous and in-depth reporting obligations to a narrow range of subsidies considered "most likely to distort"; (ii) excluding from the reporting obligations all contracts for the supply/purchase of goods/services on market terms; and (iii) exempting the notification of general tax measures and incentives valued below €1M. While these changes are a significant step in the right direction, and will help reduce unnecessary red tape for businesses, there are still some problematic elements in the FSR. Most significantly, certain incentives fall within the scope of the FSR, but would not have to be notified if granted by an EU Member States (e.g., certain audiovisual incentives and R&D tax credits). In addition, the EC has failed to offer any guidance on how it will operationalize the FSR's *ex officio* tool; thus, creating significant uncertainty for businesses and opening the door for discriminatory enforcement.

**Artificial Intelligence Act (AIA)**

In April 2021, the EC introduced the AIA, a comprehensive framework for regulating the development and deployment of AI across the 27 EU member states. The AIA was adopted in August 2024 and will come into effect in August 2026.

AIA is a first-of-its-kind regulation, with the potential to set standards worldwide as businesses adapt to EU-specific requirements. As it stands, AIA presents four key problems: (i) AI is defined broadly, capturing common software not traditionally understood as "AI;" (ii) AIA would regulate based on "risk level," but creates significant uncertainty around how this risk is assessed; (iii) compliance requirements for "high risk AI" are administrative and technically unfeasible (e.g., requiring "error-free datasets") with unclear allocation of responsibility between AI developers (providers) and deployers (users); and (iv) AIA would prohibit use of some systems, but the scope of systems to be prohibited varies widely between the Commission's proposal and positions adopted by the Parliament and Council.

These four issues are likely to stifle innovation and limit market access for U.S. companies in Europe. The discussions and proposals regarding targeted rules for general purpose AI, and generative AI, as high-risk classification is also influenced by the broader EU "digital sovereignty" agenda aimed at reducing dependency on U.S. and Chinese technologies. The proposed regulation is entering its final and most critical phase, and adoption may happen as early as November.

## India

**Violation of WTO Information Technology Agreement Commitments**

Since 2014, India has increased its tariff rates by 10 to 20 percent on various ICT products, such as mobile phones, base stations, telecommunication equipment, and printer supplies for which India promised to provide duty-free treatment under the Information Technology Agreement (ITA). In 2019, the EU challenged India's rate increases. Japan and Taiwan filed similar complaints that same year. A WTO dispute

settlement panel on April 17, 2023 found that India had violated its ITA commitments. India notified its decision to appeal the panel report on May 25, 2023. Due to the appeal and the absence of a functioning WTO Appellate Body, India has not changed course to meet its ITA commitments and thus continues to reclassify and levy WTO-inconsistent tariffs on various Information and Communication Technology (ICT) products.

### Import Management System

In September 2023, India proposed an import licensing regime for computers with near immediate effect. Fortunately, implementation was delayed for a year and the measure was reconfigured as an "import management system." The measure was further delayed until December 2024 following lack of clear guidance to industry. The troubling fact remains that India intends to apply quantitative quotas on computers and other IT goods, in an effort to stimulate domestic production. We encourage USTR to continue pushing back on this measure through the Trade Policy Forum and other bilateral discussions.

## Indonesia

### Import Duty Collection on Electronic Transmission of Digital Goods

In 2018, the Indonesian Ministry of Finance (MOF) issued Regulation No. 17/2018, which established five HS lines at the 8-digit level (with import duty rates currently set at zero percent) for software and other digital products transmitted electronically, including applications, software, video, and audio. In December 2022, the MOF issued Regulation No. 190/PMK.04/2022 (MOF Regulation 190), which came into force on 13 January 2023, introducing the new import declaration procedure for intangible goods. This measure effectively established a customs administrative regime that would enable Indonesia to start collecting duties on intangible goods, and would result in significant compliance costs and administrative burdens for businesses of all sizes operating in Indonesia. Imposition of any duties on digital products under this regulation would raise serious concerns regarding Indonesia's longstanding WTO commitment, renewed on a multilateral basis in June 2022, not to impose duties on electronic transmissions. In addition, using a tariff schedule for the application of such duties on non-physical products raises fundamental questions and challenges related to the harmonized tariff system, the role of customs authorities in the digital space, and the determination of country of origin for electronic transmissions. If implemented on a mandatory basis, these customs duties would be levied on the same electronically supplied services (ESS) that are subject to a VAT in Indonesia.

### Violation of WTO Information Technology Agreement (ITA) Commitments

Indonesia continues to contravene its WTO binding tariff commitments by charging tariffs on a range of imported technology products that are covered by Indonesia's commitments under the 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 sought to re-classify technology goods that have similar functions into dutiable HS codes that are outside of the 5 categories to raise revenue, but in most cases the reclassified HS codes are also themselves covered by Indonesia's ITA commitments. This practice widely affects the IT industry and negatively impacts U.S. investors and their workers.

### Localization under E-Commerce Regulations

Indonesia's Government Regulation No. 80/2019 (GR80) on E-Commerce draws a clear distinction between domestic and foreign e-commerce business actors, and prohibits personal data from being sent offshore unless otherwise approved by the MOT through a list of countries which can store Indonesian e-commerce data. This effectively requires e-commerce business actors to locally store personal data for e-commerce customers. Trade Regulation No. 50/2020 (TR50) on E-Commerce, an implementing regulation of GR80, also requires e-commerce providers with more than 1,000 domestic transactions annually to appoint local representatives, promote domestic products on their platform, and share corporate statistical data with the government. Both GR80 and TR50 thereby impose *de facto* data localization measures and local content requirements, which increase overhead costs for foreign entities and create undue market barriers.

## Mexico

### Trade facilitation and border issues

U.S. exporters continue to face significant challenges at the U.S.-Mexico border. Mexico has still not fully complied with the letter or spirit of its 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. Servicio de Administración Tributaria's (SAT) 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. Furthermore, SAT is aggressively auditing U.S. multinational corporations, asserting that millions of dollars are owed on customs transactions, and threatening to suspend importing licenses[4] unless these payments are made. This issue

[4] Foreign Trade General Rules for 2024, Rule 1.3.3, section XLVI.

extends beyond the consumer technology industry, affecting a wide range of sectors operating within the country.

**Temporary Tariff Increases**

In an April 2024 presidential decree, Mexico imposed temporary import tariffs ranging from five to 50 percent for 544 HS codes. These codes include items such as steel, aluminum, textiles, apparel, footwear, wood, plastic, and products related to plastics, chemicals, paper and cardboard, ceramics, glass, electrical material, transportation material, musical instruments, and furniture, among others – and were imposed without prior public notice or opportunity for interested parties to comment. The decree states these changes are needed to stabilize domestic industry and eliminate distortions in trade, and sets a general expiration date of April 23, 2026 (with certain exceptions).

This is an increase from an August 2023 presidential decree, in which Mexico imposed temporary five to 25 percent tariff rate increases on various categories of imports. The rate changes cover a broad range of products - including metals, textiles, chemicals, oil, soap, paper, electronics, and furniture. In addition to imposing the rate increases, the August 2023 decree also suspended previously-planned tariff rate reductions. In sum, the tariff rate changes increase the cost of importing into Mexico with little adjustment time for importers.

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 help address these concerns.

**Judicial reforms**

While the Mexican government has the sovereign right to amend its constitution, the constitutional amendment that overhauls Mexico's judiciary risks damaging the long-standing trade and investment relationship between the United States and Mexico, as well as the rights of U.S. companies under the USMCA. As enacted, this judicial reform introduces significant uncertainty into our commercial relations and jeopardizes the upcoming USMCA review discussions. The Sheinbaum administration should adopt a more deliberate and thoughtful approach. This reform to remove all existing appointed judges and replace them through popular election poses serious risks to the rule of law and the administration of justice in Mexico. Without fair and predictable legal recourse for U.S. investors, the USMCA implementation and enforcement may face additional challenges.

## The Philippines

**Digital Services Tax**

In October 2024, the Philippines imposed a 12 percent value added tax on digital services provided by both residents or non-residents and consumed in the Philippines. Republic Act No. 12023 was approved and signed by the President of the Philippines on October 02, 2024, and posted on the Official Gazette on October 03, 2024. The new law covers online search engines, media, advertising, platforms, as well as digital marketplaces and goods, and cloud services.

# Annex 3 – Data Localization

*CTA's aim for Annex 3 is to highlight various types of localization measures for USTR and to ensure that USTR is aware of the general proliferation of these measures. In identifying these measures, we emphasize the importance of clear scoping and definitions in all of these measures such that they are not interpreted or applied in an overbroad manner, even where there may be legitimate underlying policy objectives. For example, we recognize that, as a general policy, it is reasonable for governments to require the storage of sensitive government data within their territories.*

## Chile

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, the regulator authorized a narrow exception exclusively for banks that maintain adequate operational risk management per CMF's assessment. 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 financial institutions to local infrastructure offerings.

## Czech Republic

The Czech government, through the National Cyber and Information Security Agency (NÚKIB), is currently implementing the EU NIS 2 Directive with a 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.

## Hungary

In Hungary, the rules on the data management of state and local government bodies and organizations 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 the state and local government bodies under the Act, which form part of the national data assets, may only be processed in electronic information systems operated and stored in the territory of Hungary, and in closed electronic information systems used for defense and diplomatic information purposes. This type of data may

be processed in electronic information systems operated within the territory of the EEA States, if authorized by the supervisory authority for the security of electronic information systems or by an international treaty. This restriction applies to the following state and local government bodies: central government administration bodies,“Sándor-palota” (the office of the President of Hungary), Office of the Parliament (National Assembly), Office of the Constitutional Court of Hungary, National Office for the Judiciary and courts, Prosecution offices, Office of the Commissioner for Fundamental Rights of Hungary, State Audit Office of Hungary, Central Bank of Hungary, Metropolitan and county government offices, Offices of the representative body of local governments, and Hungarian Defence Forces. Any entity not registered in Hungary operating an electronic information system under the Act must appoint a representative based in Hungary, who is responsible for the implementation of the provisions of the Act in accordance with the rules applicable to the head of such organization. The electronic information systems of organizations providing crucial services may also be hosted in the European Union Member States. Organizations providing crucial services include those in the energy, transport, agricultural, and health sectors.

## Indonesia

The Ministry of Communication and Information Technology is now privately floating a data localization proposal for the private sector as a response to a major cybersecurity incident involving government data. In June 2024, several Indonesian government offices were hit by a series of ransomware cyberattacks for which the data was not backed up. There is not much public information surrounding the data localization proposal at the time of this submission. We encourage USTR to monitor this situation as it develops to ensure that any resulting proposals avoid discriminatory localization requirements.

## Kenya

The Data Protection Act does not require the localization of personal information, and Section 50 leaves it to the Cabinet Secretary (CS) to stipulate which personal data should be stored and processed in Kenya on grounds of strategic interests of the state or for the protection of revenue. However, 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.

## Nigeria

Nigeria’s National Information Technology Development Agency’s (NITDA) Content Data Development Guidelines of 2019/2020 requires all "sovereign data" to be stored in the

country. While sovereign data remains undefined in the Guidelines, it is understood that all public sector workloads would be captured under its definition. In 2023, under the previous administration, the NITDA Bill and National Shared Services Corporation (NSSC) Bill were presented to the National Assembly. The NITDA Bill intended to (i) extend NITDA's supervisory rights over digital services providers and the private sector's use of ICT; (ii) extend NITDA's one percent tax on foreign digital platforms; (iii) introduce new ICT requirements and (iv) grant NITDA oversight rights over the telecom industry. The NSSC Bill aimed to centralize under a single, state-owned corporation the provision of ICT infrastructure and services (including cloud) to Nigerian government bodies. The intent was for government-controlled Galaxy Backbone to become the exclusive provider of ICT infrastructure, services, and operations to the Federal Government of Nigeria. Neither of the two Bills was approved by the National Assembly before the elections, but they could be revived under the new administration. Earlier this year, the National Digital Economy and E-Governance Bill was introduced and includes similarities to the other two Bills.

## Pakistan

Pakistan launched a Cloud First Policy in 2022. This policy imposes data localization requirements on wide and open-ended classes of data ("restricted", "sensitive", and "secret"). In the financial sector, the State Bank of Pakistan (SBP) prohibits financial sector institutions from storing and processing core workloads on offshore cloud. These data localization requirements are ineffective at enhancing data protection, and significantly increase costs for U.S. firms, potentially deterring market entry. The Ministry of Information Technology and Telecommunications introduced the Personal Data Protection Bill in 2023, which creates more strict measures for data localization.

## Saudi Arabia

The National Cybersecurity Authority (NCA) has implemented data localization under the form of Essential Cybersecurity Controls (ECC-1: 2018) for government- and state-owned enterprises and Critical National Infrastructure (CNI). This regulation has a data localization requirement for these entities, stating that an "organization's information hosting and storage must be inside the Kingdom of Saudi Arabia" (ECC-1: 2018, 4-2-3-3). ECC-1: 2018, 4-1-3-2 sets another localization requirement relating to cybersecurity services, stating that "cybersecurity managed services centers for monitoring and operations must be completely present inside the Kingdom of Saudi Arabia". This covers a broad spectrum of customers, including financial services, aviation, and resource extraction, that by their nature need the safe and free flow of data across borders to maintain and enhance their operations and keep them safe and secure by cyber threats.

There are additional localization requirements including in the Cloud Cybersecurity Controls (CCC-1: 2020) issued by the NCA. CCC-1: 2020, 2-3-P-1-10 and 11 require

that companies provide cloud computing services from within KSA, including systems used for storage processing, disaster recovery centers, and systems used for monitoring and support. While they do allow for level 3 and 4 data to be hosted outside KSA, this is heavily reliant on the entity seeking this exception.

The April 2024 Amendments to the Regulation on Personal Data Transfer Outside the Kingdom limits the permissible legal bases for data transfers outside of adequacy decisions. The international best practice is to allow transfers not only within the framework of adequacy decisions or appropriate safeguards by adopting one of the legal mechanisms, but also in specific circumstances such as those adopted in EU's General Data Protection Regulation (GDPR). By curtailing the existing data transfer regime in the Regulation, the Draft Amendment risks isolating the Kingdom from the benefits of global data flows, impacting the operational capability of businesses and stifling innovation and growth by erecting barriers to international trade.

## South Africa

South Africa's Cloud Computing Policy was implemented in May 2024 by the Department of Communications and Digital Technologies (DCDT) and contains references to data sovereignty and explicitly encouraged the use of local providers (indigenous providers) in government cloud outsourcing.

## Vietnam

In June 2018, Vietnam's National Assembly passed the Law on Cybersecurity containing a broad and vague data localization requirement (Article 26.3). The Law states that data localization requirements will only be enforced after issuance of detailed guidance in the form of an implementing decree (Article 26.4). The implementing Decree (Decree 53) was issued on August 15, 2022 (entered into force on October 1, 2022) contained data localization measures for all domestic companies. Such measures disrupt the cross-border provision of cloud services and business software service suppliers. If all domestic companies are required to localize data under this implementing decree, U.S. cloud service providers and software service suppliers will be unable to sell services in Vietnam unless they build local data centers or localize their software data, which serves as a market access barrier that favors local telecommunications and cloud providers. The Cybersecurity Administrative Sanctions Decree was unveiled by the Vietnamese Ministry of Security to the Ministry of Justice in mid-May 2024 and lays out the fines for companies violating personal data protections provided in Decree 53.

In August 2024, the National Assembly introduced the draft Data Law, which contains significant restrictions on cross-border data transfers. The bill grants authorities broad powers to identify core data, critical data, and important data – and imposes restrictions on overseas transfers of these data categories following a government impact

assessment and government approval. Core data is defined broadly, and it is unclear if any data that organizations collect or produce as part of its services will amount to core data. What constitutes core, important, and critical data will also be determined by various state officials, including but not limited to the Prime Minister and ministers. The bill further states when transferring data, the "data administrator agencies" must apply necessary measures to ensure that the data processing activities of the foreign data recipients meet the data protection standards specified in this Law. For example, it remains unclear what measures organizations need to take to ensure that foreign data recipients meet the data protection standards under the Draft Law.

In September 2024, the National Assembly introduced the long-awaiting draft Personal Data Protection (PDP) Law. Article 45 introduces very broad examples of what constitutes transfers of personal data abroad, requires consent for all cross-border data transfers (thus limiting the options for additional legal bases as seen in other internationally recognized frameworks), and grants the government broad authorities to suspend overseas transfers if the transferred personal data is “used in activities that violate the national interests and security of the Socialist Republic of Vietnam.” Furthermore, the draft PDP Law requires the completion of a dossier prior to international transfer, which is redundant with the dossier requirement for international data transfers in the PDP Decree.