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

March 11, 2025

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

Re: Request for Comments to Assist in Reviewing and Identifying Unfair Trade Practices and Initiating All Necessary Actions to Investigate Harm From Non-Reciprocal Trade Arrangements (Docket Number: USTR-2025-0001)

Dear Ambassador Greer:

The Consumer Technology Association ("CTA") appreciates the opportunity to provide input to the Office of the U.S. Trade Representative ("USTR") on unfair and non-reciprocal foreign trade practices. This effort by the Trump-Vance Administration is important to ensure American businesses are being treated fairly by our trading partners.

CTA represents the more than $537 billion U.S. consumer technology industry, which supports more than 18 million U.S. jobs. Our members are comprised of over 1200 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.

Reciprocity is an Effective Tool to Lower (or Eliminate) Barriers to Trade

The Administration's imposition of tariffs on all imports from Canada and Mexico under the International Emergency Economic Powers Act (IEEPA) on March 4 and from China and Hong Kong on February 4 indicates to us that the Administration's true vision of reciprocity is higher tariff barriers for the United States and for all of our trading partners. We are deeply concerned that the additional threats of tariffs on specific trading partners (e.g., the European Union and the United Kingdom) and specific sectors and products (e.g., agriculture, autos, copper, timber and lumber, oil and gas, pharmaceuticals,

semiconductors, and derivative products in all of these sectors) will increase global barriers to trade and dismantle the global trading system.

Following President Trump's announcement of his intent to impose reciprocal tariffs on other nations, CTA CEO Gary Shapiro said, "Most reciprocal policies as described today by President Trump are common sense. As part of our Innovation Agenda, we support a focus on how countries treat American exports in crafting trade policy. Having some level of reciprocity seems fair, including reducing or eliminating American tariffs for our allies and those treating our exporters fairly."[1]

Therefore, on behalf of our members, CTA first seeks to emphasize that ***the Administration's work on reciprocity should result in the removal, not the creation, of barriers to trade.*** This effort is essential to ensure that American consumer technology companies can compete on a level playing field and access new markets worldwide. By addressing foreign trade barriers, USTR can help foster innovation, support job creation, and maintain the United States' leadership in the global technology sector. We strongly encourage USTR's recommendations to the President to prioritize opening new markets for American consumer technology companies while safeguarding our industry's interests and promoting fair trade practices.

Reciprocity should lead to negotiations that pave the way for fewer barriers to trade. Reciprocity should be pursued in a collaborative manner that does not lead to retaliation from trading partners that will only do harm to America's exporters. As documented by the International Trade Administration, it is plainly evident that trading partners have retaliated against the United States in response to the Section 232 and Section 301 trade actions.[2] Regardless of whether such retaliatory actions were appropriate or consistent with global trading rules in the views of the United States, the fact remains that those actions were imposed and resulted in harm to U.S. interests. USTR should pursue a reciprocity strategy that mitigates this risk.

Among the world's largest economies, trade in information technology ("IT") products is already largely reciprocal due to a longstanding agreement to reduce and bind their tariffs on IT products at zero. Among other things, this agreement reflects a recognition among leading economies—developed and developing alike—that trade in these products is critically important to the functioning of households, businesses, and all types of institutions (in healthcare, education, and beyond). Broad and affordable access to these products is a prerequisite for innovation, productivity growth, and free expression. As such, the imposition of tariffs on these products would mark a U.S.

---

[1] CTA CEO on Tariff Reciprocity Announcement, Consumer Technology Association (Feb. 13, 2025), https://www.cta.tech/Resources/Newsroom/Media-Releases/2025/February/CTA-CEO-on-Tariff-Reciprocity-Announcement.

[2] Foreign Retaliations Timeline, International Trade Administration, U.S. Department of Commerce (Feb. 14, 2025), https://www.trade.gov/feature-article/foreign-retaliations-timeline.

departure from the current landscape of broad existing reciprocity, contrary to the objectives of the Presidential Memorandum and the interests of U.S. consumers and businesses.

USTR should use an economic approach from existing analyses to more comprehensively understand the actual financial impact these barriers impose on trade. This method will facilitate more effective negotiations by providing concrete data to support arguments for the reduction or elimination of these barriers.

Breaking Down Barriers to Digital Trade is in the U.S. National Interest

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. 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 abroad.

A multi-association analysis during the previous Administration noted that, "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."[3] We commend the current Administration for prioritizing digital trade barriers and urge USTR to address past omissions by reintegrating the digital trade barriers outlined in our comment in USTR's recommendations of actions to the President. Achieving true reciprocity will ensure these barriers are integrated into the Administration's strategy.

We support the Administration's initiative to secure among trading partners a permanent moratorium on customs duties on electronic transmissions. This step is vital as other countries collect duties on electronic transmissions, disadvantaging American companies. For instance, Indonesia imposes duties on digital products through MOF Regulation 190, contravening the agreement by World Trade Organization ("WTO") members during the 13th Ministerial Conference ("MC13") to extend the moratorium.

Target Harmful Digital Services Taxes

As part of the effort ahead, CTA commends the Administration's focus on digital services taxes ("DSTs") imposed by trading partners which pose significant barriers to the export of U.S. digital services. This tax policy unfairly burdens consumer technology

[3] 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-ledmulti-association-memorandumto-congress-expresses-concerns-with-the-ustrs-2024-national-tradeestimate-report/.

companies, hinders digital trade, and disrupts the free flow of services across borders. This decision by other countries hampers innovation and unfairly targets U.S. companies. DSTs hurt U.S. startups, small businesses, and consumers. In this regard, CTA welcomes President Trump's memorandum entitled "Defending American Companies and Innovators From Overseas Extortion and Unfair Fines and Penalties."

Open Markets, Open Markets, Open Markets!

The passage of new Trade Promotion Authority ("TPA") will validate President Trump's authority to negotiate trade deals that remove tariff barriers in key markets, so TPA will be a necessary tool to implement the America First Trade Policy Presidential Memorandum. USTR should work with Congress to pass this authority.

Many countries, especially large emerging markets, maintain high tariff barriers and other border measures to exclude U.S. consumer technology products and promote domestic manufacturers at their expense. India, Brazil, Indonesia, Nigeria, Pakistan and other countries all have higher average tariff bound and applied rates on technology products compared to the United States, the European Union, Japan, South Korea, and even China. USTR should open these markets through trade negotiations. For the consumer technology industry, we are pursuing a world where U.S. companies can provide life-changing, innovative, and affordable products to as many people as possible, anywhere along the economic spectrum, and in all parts of the world.

Supply Chain Resiliency Still Relies on a Multi-Geography "Team Approach"

Correcting unfair trade practices should benefit American businesses and consumers ***and*** should result in stronger supply chain resiliency with our treaty allies and trade partners. To reshore more or all of the consumer technology supply chains to the United States would require a direct investment of well over $500 billion and a more than tenfold increase in workforce for both manufacturing and the indirect supplier ecosystem to meet the expected production output that exists today.[4] Based on our research, we believe a multi-geography "team approach" is the most viable route to greater supply chain resiliency and does not conflict with policy objectives to strengthen domestic manufacturing. By this, we mean using a combination of the United States and its treaty allies and trade partners to provide a long-term alternative to mainland China's and Taiwan's dominance in the global consumer technology supply chain.

[4] "Building a Resilient U.S. Consumer Technology Supply Chain," Consumer Technology Association (Oct. 1, 2023), https://cdn.cta.tech/cta/media/media/resources/research/pdfs/building-a-resilient-u-s-consumer-technology-supply-chain_executive-summary.pdf.

Prioritize Addressing Barriers to Trade that Impact Technology and Innovation

CTA has catalogued three categories of foreign trade barriers impacting technology and innovation to aid in USTR's analysis. These are included in three annexes below relating to: 1) digital services taxes; 2) other proposed barriers; 3) other existing barriers. Barriers identified in Annexes 2 and 3 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 collaborating with you, USTR staff, and the interagency to prevent and correct these foreign 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 initiate actions to investigate the harm from non-reciprocal trade measures.

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 – Digital Services Taxes

Australia

Since July 2017, Australia has applied a ten percent goods and services tax (GST) on digital services provided by nonresident companies to Australian consumers. This tax covers a broad range of digital services, including streaming platforms, software, cloud computing, and online advertising.

Austria

Austria's Digital Services Tax imposes a 5 percent levy on revenues from online advertising, applying specifically to companies with global revenues exceeding €750 million and Austrian revenues above €25 million. It targets various forms of online advertising, including banner ads, search engine ads, and comparable digital advertising services directed at Austrian users. The tax unfairly burdens U.S. companies due to the significant presence in the market, while most domestic players are spared. On February 15, 2024, U.S. Treasury announced the extension of the agreement between the United States and Austria allowing DST liability accrued by U.S. companies

through June 30, 2024 to be creditable against future income taxes accrued under the OECD's Pillar 1.

Belgium

In 2025, the new ruling government of Belgium put forward a plan to implement a 3 percent “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.

Canada

In July, Canada implemented a unilateral DST that disproportionately targets U.S. companies and contravenes its trade commitments, including under the U.S.-Mexico-Canada Agreement (USMCA). The DST took the form of a 3 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). Implementing legislation – the Digital Services Tax Act - retroactively imposes the DST to 2022.

Colombia

A tax on gross income derived by overseas providers of goods and digital services into Colombia based on the concept of “significant economic presence” (SEP) (Law 2277/22, Article 57). The tax entered into force on January 1, 2024 as the first digital services tax (DST) in Latin America. 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 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.

Czech Republic

The Czech Republic has proposed a five percent DST on online advertising, transmission of user data, and digital interface to facilitate the provision of supplies of goods and services among users. There was a proposed amendment to reduce the tax rate from seven percent to five percent.

France

France has implemented a three percent DST on revenue from services connecting users through a digital platform and the sale of advertising space and digital data. The threshold is for companies with worldwide revenue of €750 million and local revenue of €25 million. On February 15, 2024, U.S. Treasury announced the extension of the agreement between the United States and France allowing DST liability accrued by U.S. companies through June 30, 2024 to be creditable against future income taxes accrued under the OECD's Pillar 1. As the French government casts about for revenues to

address its budget deficit, parliamentarians are considering an amendment (I-735) to the 2025 budget to raise the DST from three percent to five percent, purportedly raising €500 million.

Indonesia

In August 2020, Indonesia's Directorate General of Taxes implemented an 11 percent value-added tax (VAT) on digital services supplied by nonresident companies to Indonesian consumers. This tax applies to a wide range of digital products and services, including streaming media, software, applications, and online advertising. Nonresident providers meeting certain thresholds – annual sales exceeding IDR 600 million (approximately $38,000), or more than 12,000 Indonesian consumers annually – are required to comply.

Italy

Italy has implemented one of Europe's most comprehensive digital taxation frameworks, centered on a three percent DST on gross revenues from digital advertising, multilateral digital interfaces, and user data transmission. The system applies to companies with global revenues exceeding €750 million. The 2025 Budget Law eliminates the €5.5 million Italian revenue threshold for the application of the DST, increasing the number of potential taxpayers subject to the tax. The Budget Law also amends the payment deadline by introducing an advance payment due by November 30, equal to 30% of the DST due for the previous calendar year. The balance is due by May 16 of the subsequent calendar year. Prior to the change, DST payment for the calendar year was due May 16 of the following year. On February 15, 2024, U.S. Treasury announced the extension of the agreement between the United States and Italy allowing DST liability accrued by U.S. companies through June 30, 2024 to be creditable against future income taxes accrued under the OECD's Pillar 1.

Kenya

Kenya has introduced a comprehensive digital taxation system. The core element of this system is the significant economic presence (SEP) tax, effective December 2024, which replaces the previous DST. The SEP tax imposes a three percent levy on the gross turnover of non-resident entities operating within digital marketplaces.

The Philippines

In October 2024, the Philippines imposed a 12 percent DST 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.

Spain

Since 2021, there is a Tax on Certain Digital Services. It is an indirect three percent tax, and the taxable base is constituted by the amount of income, excluding, where applicable, VAT or other equivalent taxes, obtained by the taxpayer for each of the digital services subject to the tax, namely online advertising, online intermediation and data transmission services, carried out in Spain. The tax applies to companies with global revenues exceeding €750 million and Spanish revenues above €3 million. The DST has a disproportionate impact on U.S. companies, with 64 percent of the affected entities being based in the United States, compared to only 5.1 percent that are Spanish.

Turkey

Turkey imposes a 7.5 percent DST on gross revenues from digital services, which is higher than the rates in many other countries. This tax covers a wide range of digital activities, including digital advertising, content sales, and platform operations. Companies are required to pay the tax if they have Turkish revenues above TRY 20 million and worldwide revenues above €750 million. Additionally, Turkey has implemented a 15 percent withholding tax on digital advertising payments, with proposals for withholding taxes up to 25 percent on e-commerce transactions. The President has the authority to adjust the DST rate between one percent and 15 percent, introducing potential policy variability for digital businesses operating in Turkey.

United Kingdom

The United Kingdom introduced a DST in 2020, imposing a two percent levy on revenues from social media platforms, internet search engines, and online marketplaces that derive value from UK users. This tax applies to companies with global revenues exceeding £500 million and UK revenues above £25 million, with an exemption for the first £25 million of taxable UK revenues. A majority of the revenue this tax has generated came from U.S. technology companies.

Annex 2 – Other Proposed Measures

Australia

Investment obligation for streamers

A bill targeted at U.S. streaming providers, which will require them to invest at least 10% of their local program expenditure on creating new Australian drama programs. The

definition of Australian content is still uncertain, but will likely be very difficult to meet. It would also include additional sub-quotas, including to produce children's content – even if the streaming provider does not produce that sort of content.

Ex-ante competition regime

A proposed framework that borrows from the EU's Digital Markets Act and UK's DMCC, which would allow the government to subject digital platform services to broad obligations on matters such as self-preferencing and data use, as well as more detailed rules. 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)

Brazil

AI Bill 2338/2023

This bill, which has been passed by the Senate and is awaiting House approval, would make it more difficult for U.S. AI developers and U.S. businesses to export their AI services to Brazil. Moreover, it departs from using a risk-based approach to AI, does not differentiate between the developer and deployer for high-risk AI systems, and contains copyright provisions that requires developers to pay for Brazilian content to train AI models.

Ex-ante competition bills and proposals

The Ministry of Finance is preparing to send a bill to Congress that would create a Digital Markets Unit within the Administrative Council for Economic Defense (CADE), and grant CADE broad new powers to designate select companies as "systemically relevant platforms. The proposal mirrors the United Kingdom's Digital Markets Competition and Consumer Act (DMCC), in which CADE would conduct a prior investigation to designate, impose remedies, and ensure compliance with such remedies on certain players. The Secretary of Economic Reforms predicted that the seven companies that are currently considered "gatekeepers" by the European Union's Digital Markets Act will likely fall under Brazil's criteria. There are concerns that this proposal could discriminate against U.S. companies through quantitative thresholds that are poor indicators of market power and anticompetitive conduct. The Brazilian Congress has introduced two other ex ante related bills that would harm US companies. Bill 2768, inspired by the DMA, designates the National Telecommunications Agency (ANATEL) as the primary regulator of "digital platforms" in Brazil, and establishes a list of obligations designated companies would have to follow. Bill 4691 seeks to establish ANATEL and CADE as co-regulators of digital platforms above a certain size and subject them to certain obligations. The bill also includes provisions related to content moderations.

Network usage fee

Brazil's Telecommunications Agency (ANATEL) is interested in imposing a network fee tax that a small group of U.S. content providers and technology companies would have to pay to large internet service providers to fund telecommunications infrastructure.

Canada

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.

Copyright Act

Canada is reviewing and updating the Canadian Copyright Act, and how it applies to AI systems, including how text and data mining ("TDM") activity and the training of AI using copyright- protected works can legally function in Canada. There is risk that it will fail to align with U.S. policy and limit the ability of U.S. AI companies from providing AI services and training AI in Canada.

Colombia

Network usage fee

The Colombian Communications Regulation Commission (CRC) discussed the possibility of introducing a network fee tax that U.S. content providers and technology companies would have to pay to local internet service providers to fund telecommunications infrastructure.

Czech Republic

Data localization

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.

EU and EU Member States

EU Cybersecurity Certification Scheme for Cloud Services (EUCS)

The EU Agency for Cybersecurity (ENISA) has been developing a European Cybersecurity Certification Scheme for Cloud Services (EUCS) since 2020. In June 2022, ENISA amended the draft certification scheme to introduce four new criteria – including immunity from foreign law – for CSPs to qualify for the highest cybersecurity certification level in EUCS. If this proposal were adopted, only companies with their head office and global headquarters in an EU Member State would be eligible to certify at the highest level of EUCS. This would effectively prevent U.S. CSPs from providing services to the public sector and regulated industries in the EU. The EU Commission has suspended EUCS negotiations for the time being, but the EU Commission is likely to leverage the upcoming revision of the EU Cybersecurity Act (CSA) - the legal basis for EUCS - to facilitate the inclusion of discriminatory requirements in future certification schemes.

Proposal for a Foreign Investment Screening Regulation

The Regulation would require all Member States to impose an ex-ante authorization requirement on all foreign investments targeting companies that (i) are active in one of 42 listed “critical technology areas” (which includes 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. Initial engagement with EU policymakers on this regulation suggests that it is likely to have a significant impact on US companies.

Space Law

The Commission has publicly stated its intention to create an asymmetric regulatory regime where ‘small’ satellite operators are subject to a lighter regime than ‘larger’ operators (e.g., constellations). This asymmetric approach would impose higher compliance costs on U.S. constellations than EU operators. The EU Space Law may also restrict certain communications services to EU-headquartered satellite operators (similarly to EUCS).

Proposal for a Financial Information for Data Access (FIDA) Regulation

The European Parliament and the Council of the EU are evaluating the exclusion of DMA gatekeepers from the framework of the draft FIDA Regulation and considering establishing additional safeguards preventing platforms as a whole from accessing financial services data-sharing schemes.

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.

Germany

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.

Korea

Monopoly Regulation and Fair Trade Act

In September 2024, the Korean Fair Trade Commission (KFTC) announced plans to amend the Monopoly Regulation and Fair Trade Act (MRFTA) to address presumptively anti-competitive behavior among some but not all market participants. In October 2024, a similar proposal was introduced in the Korean National Assembly. These proposals mark a departure from Korea’s traditional competition policy and threaten discriminatory application and innovation stifling results. Despite abandoning its controversial Platform

Competition Promotion Act (PCPA), which had been criticized for its ex-ante regulation approach, the KFTC's new proposal still retains problematic elements such as disproportionately targeting U.S. companies through an arbitrary mix of hand-crafted sectoral definitions and financial and other market thresholds to narrowly focus on online services that U.S. firms provide in Korea. As such, the proposed thresholds largely capture American tech companies. Moreover, Chinese platforms like Temu, which have significantly increased their market share over the past year in the Korean e-commerce market through aggressive pricing strategies, are also excluded and can therefore engage in acts and pursue business strategies not available to competing U.S. platforms.

Meanwhile, other bills proposing ex-ante regulation of U.S. digital service providers are under consideration in Korea's National Assembly. These bills are modeled on the EU's Digital Markets Act. Korea's pursuit of discriminatory legislation against U.S. firms is an unnecessary irritant to the longstanding bilateral relationship that creates an unlevel playing field for U.S. firms competing against rapidly growing Chinese e-commerce companies and a potential violation of the U.S.-Korea Free Trade Agreement.

AI Basic Act

Korea has pending legislation that will require AI providers to establish an in-country representative to ensure products comply with prescribed safety and governance requirements.

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 e-commerce 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.

Data localization

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.

Norway

Digital Sovereignty and Ownership requirements

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

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.

Thailand

Platform Economy Act (PEA)

Thailand is drafting a law that aims to regulate digital services by bringing in DSA/DMA concept from the EU. Cloud service might be designated as 'intermediaries' and may be subject to 'gate keeper' obligation.

Turkey

Competition/ex-ante rules

Amendment to Turkish Competition Act would impose EU-style restrictions and mandatory data sharing obligations disproportionately on U.S. companies, with fines of up to 20% of annual turnover.

Annex 3 – Other Existing Measures

Argentina

Customs release delays

Customs detains shipments in "channels" when it has a question about the shipment or import documentation (yellow channel) or decides to perform a physical inspection (red channel). Argentine Customs often detains such shipments for up to one year, even after all inspections are complete and the importer answers all inquiries, resolves any discrepancies or disputes, and pays any fines imposed. This practice causes significant delay to delivery timelines, creating disruption and unpredictability in the supply chain. It also imposes costs on importers, who may need to reorder goods and incur additional fees for storage.

Canada

Online Streaming Act (C-11)

As part of implementation of C-11, the Canadian Radio-television and Telecommunications Commission required that foreign, largely U.S.-based, streaming service providers with revenues over $25M contribute five percent of their gross in-country revenue to a set of Canadian cultural funds, which they cannot access. The CRTC is considering a range of additional regulations targeting U.S. streamers, including local content quotas.

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, 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.

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

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.

Cyprus

Data localization

U.S. cloud service providers (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.

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. A mandatory review of the DMA by May 2026 could expand its scope to include new services (e.g., GenAI, cloud). Some political operators and competition authorities are already suggesting such an expansion.

Data Act

Regulates access to and transfer of data generated by connected products and related services in the EU. The Regulation entered into force in January 2024, and its main provisions will begin to apply from September 2025. The Regulation will force 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.

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. Establishes a horizontal risk-based framework to regulate AI systems in the EU. It will now be supplemented by Implementing Acts and standards to operationalize its requirements for general-purpose AI, foundation models and high-risk AI.

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.

France

National Cybersecurity Certification Scheme for Cloud Services (SecNumCloud)

In March 2022, France's national cybersecurity agency (ANNSI) revised its cybersecurity certification and labeling program SecNumCloud 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", 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 provider in order to provide cloud services to covered entities. SecNumCloud certification is a prerequisite to compete in cloud contract tenders with European governments and critical infrastructure operators. Article 19.6 of SecNumCloud appears to be a clear violation of Article 3 of the WTO Government Procurement Agreement. The French legislature continues to

contemplate amendments that would expand SecNumCloud requirements to private entities in other sectors.

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, requiring an import declaration for intangible goods. This measure effectively established a customs administrative regime that would enable Indonesia to start collecting duties on intangible goods if Indonesia decides to increase the applicable duty rate from zero percent 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 March 2024, 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 imposes customs 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. These duties are in direct violation of Indonesia's commitments to maintain zero duty on these products under the WTO Information Technology Agreement. 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.

Data localization

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.

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

Local Content Regulations

Indonesia maintains a regime of highly restrictive and opaquely administered local content requirements that frustrate the ability of U.S. companies to sell goods in the market and that are used by the government to extract concessions from companies seeking to do business in the country. In several information technology sectors, including wireless broadband and 4G/5G devices, Indonesia imposes local content requirements of up to 40 percent. Specific regulations include MOCI Regulation No. 27/2015, MOCI Regulation No. 13/2021, MOI Regulation No. 29/2017, and MOI Regulation No. 22/2020. These measures are blatantly violative of Indonesia's WTO commitments but have not been seriously addressed by the country's trading partners.

Japan

Competition/ex-ante rules

On July 5, 2022, the Ministry of Economy, Trade and Industry (METI) released a Cabinet Order stipulating that the digital advertising sector would be regulated under the 2020 Act on Improving Transparency and Fairness of Digital Platforms (TFDPA). Japan is undertaking a process to amend the Act in 2025, and there is a risk that they may add DMA-like provisions targeting U.S. companies as part of that process.

Kenya

Data localization

The Computer Misuse and Cybercrimes Act of 2018, and the Computer Misuse and Cybercrime Regulations of 2024, impose data localization and reporting obligations on providers of "Critical Information Infrastructure" (e.g., CSPs) with respect to defined categories of data. Operators of 'Critical Information Infrastructure' are required to establish a local Cybersecurity Operations Centre to monitor and report compliance to the Communications Authority.

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.

Korea

Targeted enforcement

In addition to specific legislation like the MRFTA proposal, the Korea Fair Trade Commission (KFTC) continues to unfairly target U.S. companies including Coupang,[5] Google,[6] ChatGPT,[7] Netflix,[8] and others with unprecedented fines, office raids, threats of prosecution, criminal allegations, and erroneous investigations. This enforcement culture in Korea is a troubling anomaly for a closely allied U.S. trading partner and clearly represents "unfair or harmful acts, policies, or practices" that present a "structural impediment to fair competition" per the Trump administration's recent Reciprocal Trade Memo. The KFTC's ongoing targeted enforcement and harassment of U.S. companies is perhaps the greatest impediment for ensuring a strong U.S.-Korea trade and security relationship.

---

[5] "Coupang under antitrust regulator's probe over service bundling allegations," Yonhap News Agency (Aug. 26, 2024), https://en.yna.co.kr/view/AEN20240826005300320.
[6] "KFTC's two-year YouTube Music investigation continues, hurting local services," Chosun Ilbo (Feb. 2025), https://www.msn.com/en-xl/news/other/kftc-s-two-year-youtube-music-investigation-continues-hurting-local-services/ar-AA1zkZt1.
[7] "S. Korean government to investigate monopolistic practices by foreign AI firms," Chosun Ilbo (Apr. 8, 2024), https://www.chosun.com/english/national-en/2024/04/08/L5EPMOINVZBFZOKWGIRC6EFNUQ/.
[8] Regulator launches probe into Netflix, Wavve over alleged unfair biz practices," Yonhap News Agency (Mar. 18, 2024), https://en.yna.co.kr/view/AEN20240318006000320.

Nigeria

Data localization

The Nigerian National Information Technology Development Agency's (NITDA) Content Data Development Guidelines of 2019/2020 require all "sovereign data" to be stored within the country. While the scope of 'sovereign data' remains undefined in the Guidelines, it is understood that all public sector data is captured. In 2023, a NITDA Amendment Bill and a National Shared Services Corporation (NSSC) Bill were presented to the National Assembly. The NITDA Bill aimed 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 compliance requirements, and (iv) grant NITDA oversight rights over the telecoms industry. The NSSC Bill aimed to centralize the provision of ICT infrastructure and services to Nigerian government bodies under a single state-owned corporation (Galaxy Backbone). The NITDA Amendment Bill and the NSSC Bill met with opposition from the telecoms and ICT industries, and, although approved by the National Assembly, were not signed into law by President Buhari. The Bills have yet to be re-tabled in Parliament under the new administration of President Bola Tinubu.

Pakistan

Data localization

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

Data localization

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

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.

Turkey

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 (DTO) published Guidelines clarifying that the scope of the localization requirements was limited to certain critical information and data. However, the loosely-defined localization requirements in the Presidential Decree remain a challenge, as they override the DTO Guidelines. Strict

data localization requirements are also applied to the financial services industry, where the Banking Regulation and Supervision Agency requires primary and secondary information systems to be hosted in Turkey. The Central Bank of Turkey implements similar restrictions for the outsourcing of cloud services, and prohibits the use of cloud for certain workloads.

United Kingdom

Competition/ex-ante rules

The Digital Markets, Competition, and Consumer Act established regulations aimed at U.S. technology companies. For designated entities, it would enforce stringent conduct requirements, with potential penalties reaching up to 10% of global revenue.