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

October 30, 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 on Significant Foreign Trade Barriers for the 2026 National Trade Estimate Report (Docket Number: USTR-2025-0016)

Dear Ambassador Greer:

The Consumer Technology Association (CTA) appreciates the opportunity to provide input into USTR's drafting of the 2026 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 $537 billion U.S. consumer technology industry, which supports more than 18 million U.S. jobs. Our members include 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 medium-sized companies. CTA also owns and produces CES, which showcases and serves as a forum for discussion of global policies, technology, trade and investment, and other innovation. Over 142,000 people attended CES 2025, with over 57,000 from outside the United States.

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 globally. 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 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 commend the current Administration for prioritizing digital trade barriers in the 2025 NTE[1]. Several issue areas that USTR addressed were identified in CTA's comments for the 2025 report[2], for which we are especially grateful.

USTR is statutorily obliged to "identify and analyze" any "barriers to, or distortions of" U.S. electronic commerce[3]. Such measures are problematic in a number of ways, such as through their discriminatory nature, possible infringement of intellectual property rights, and potential violation of trade agreements. USTR should 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 both allies and adversaries.

We therefore strongly urge USTR to incorporate the digital trade barriers outlined below in the 2026 NTE report.

Along the same lines, we call on USTR to take a strong stand against these measures in its reciprocal trade negotiations, other bilateral or regional engagements with our trading partners, and in the context of existing U.S. free trade agreements.

CTA's comments for the 2026 NTE cover a wide range of trade and investment barriers that if addressed could facilitate faster and less costly supply chain resiliency and 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.

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

---

[1] United States Trade Representative. (2025). *2025 National Trade Estimate Report on Foreign Trade Barriers of the President of the United States on the Trade Agreements Program*. Executive Office of the President. https://ustr.gov/sites/default/files/files/Press/Reports/2025NTE.pdf.
[2] CTA Comments to USTR on NTE 2025 Topics, *Consumer Technology Association*, 2025. https://cdn.cta.tech/cta/media/media/pdfs/final-draft-cta-comments-to-ustr-on-nte-2025-topics-(1).pdf.
[3] 19 U.S.C. § 2241(a)(1)(A)-(B).

artificial intelligence (AI).

CTA looks forward to working with you, USTR staff, and the interagency to prevent and address these barriers to trade, strengthen consumer technology supply chains, and secure non-discriminatory treatment for U.S. exports of goods and services and investments. Thank you for reviewing our comments. We are happy to serve as a resource as you draft the 2026 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 – Digital Services Taxes

Austria

Austria's Digital Services Tax (DST) 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.

Colombia

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

France

On October 22, 2025, France adopted an amendment to its 2026 Finance Bill that would increase the rate of the country's DST from 3% to 15%. This comes following the French Constitutional Court's decision on September 12, 2025, that confirmed the legality of the DST regime, including its group-based thresholds, territoriality rules based on the "national presence coefficient," and the exclusion of certain digital services from the tax base.

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.

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

Spain has implemented a three percent DST on three revenue streams: digital intermediation services, digital advertising, and user data sales. 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

Audiovisual Services

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

Ex-ante Regime for Digital Services

In December 2024, AU Treasury launched its long-anticipated consultation on a new ex-ante regime for digital services. The proposed framework adopts aspects of both the EU DMA and the UK DMCCA, which would allow the AU Government to designate digital platform services to broad obligations on matters such as self-preferencing and data use, as well as ‘service-specific obligations’. The proposal would immediately trigger new compliance obligations around preventing self-preferencing, ensuring interoperability, and prohibiting manipulative design practices. The proposal identifies ‘priority services’ for designation as app marketplaces, ad-tech services and social media, although a wide range of digital services are flagged for future consideration, including general online marketplaces, virtual assistants and, potentially, cloud. Designation also opens the way for the ACCC to recommend service-specific (platform-specific) codes of conduct. The scheme would raise similar trade-related concerns to the DMA should only US-headquartered companies meet the criteria for designation (which is possible given the initial sectors identified). Draft legislation is expected Q1’26.

Belgium

Digital Services Tax

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

Brazil

Digital Trade and Electronic Payment Services

Internet Speech

As expressed in the CTA Innovation Agenda, we oppose efforts in the United States that attempt to limit free speech online and remove internet platforms' ability to moderate content without fear of lawsuits.[4] Section 230 of the Communications Decency Act is a foundational law that underpins innovation, free speech, and the startup economy.[5] We extend this advocacy to our global policy priorities, and have successfully supported to include Section 230-style protections in the text of free trade agreements such as the United States-Mexico-Canada[6] and the U.S.-Japan Digital Trade Agreement.[7]

On June 26th, the Supreme Court voted to partially overturn Article 19 of Brazil's Civil Rights Framework for the internet ("Marco Civil") and now holds platforms liable for illegal posts by users.[8] The court replaced the general court order and takedown regime with a notice and takedown process in many cases and made ads generally liable by default. The decision also set general duty of care rules. The public still lacks full details because the court has not published the final decision yet.

Brazil's courts continue to press internet platforms to take responsibility for select third-party content and as a result, companies would likely aggressively remove any content that might come close to violating the law.[9] Furthermore, Brazil issued extraterritorial orders that require U.S. companies to remove content not just in Brazil, but worldwide, including the United States. Although Brazil's courts have jurisdiction over content available within their national borders, they should not dictate what content can be uploaded or viewed in other countries, including the United States. This practice triggers a race to the bottom on free speech and violates the First Amendment rights of U.S. companies and American citizens. President Trump recognized this issue through his

---

[4] The CTA Innovation Agenda: Policies to Maintain U.S. Leadership in Global Technology, *CTA*, 2025. https://www.cta.tech/media/vorlmklh/2025-cta-innovation-agenda.pdf.
[5] 47 U.S.C. § 230.
[6] Article 19.17: Interactive Computer Services, *USMCA*. https://www.trade.gov/sites/default/files/2023-09/fulltext.pdf.
[7] Article 18: Interactive Computer Services, *U.S.-Japan Digital Trade Agreement*. https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf.
[8] Social Media Firms Accountable for Posts, Brazil Judges Conclude, *Bloomberg*, Jun. 11, 2025. https://www.bloomberg.com/news/articles/2025-06-11/brazil-top-court-forms-majority-to-boost-social-media-oversight.
[9] Brazil's Supreme Court Rewrites the Rules to Censor Online Speech, *CATO*, Jun. 27, 2025. https://www.cato.org/blog/brazils-supreme-court-rewrites-rules-censor-online-speech.

memorandum titled, “Defending American Companies and Innovators From Overseas Extortion and Unfair Fines and Penalties.”[10]

Digital Ex Ante Competition Regulations

Brazil is advancing digital regulations that are modeled after the European Union’s (“EU’s”) discriminatory Digital Markets Act.[11] Specifically, Bill No. 2768/2022 would let Brazilian regulators temporarily suspend the operations of American companies and possibly prohibit a platform’s activities in Brazil.[12] The bill uses vague terminology and does not clearly describe the specific requirements needed to comply. Instead, it grants the National Telecommunications Agency (“ANATEL”) significant discretionary authority to define terms and create rules.[13] Because the bill uses unclear wording, U.S. companies cannot easily determine exactly what obligations they would face. At minimum, the bill would drive up compliance costs and could force companies to restructure their business operations.

In addition, the Ministry of Finance’s 2024 proposal, outlined in the report titled “Digital Platforms: Competition Aspects and Regulatory Recommendations for Brazil,” draws on elements of European, United Kingdom, and German digital regulation.[14] It 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 UK’s Digital Markets Competition and Consumer Act (DMCC) and would authorize CADE to investigate, identify certain players, set rules for them, and make sure they follow those rules. At a press conference in October 2024, the Secretary of Economic Reforms Marcos Barbosa Pinto predicted that the seven companies that are currently considered “gatekeepers” by the European Union’s Digital Markets Act will likely meet Brazil’s criteria.[15] This proposal could discriminate against U.S. companies by using quantitative thresholds that are poor indicators of market power and anticompetitive conduct.

---

[10] Presidential Memorandum, *Defending American Companies and Innovators From Overseas Extortion and Unfair Fines and Penalties,* 90 Fed. Reg. 10685 (Feb. 21, 2025). https://www.federalregister.gov/documents/2025/02/26/2025-03188/defending-american-companies-and-innovators-from-overseas-extortion-and-unfair-fines-and-penalties.

[11] Brazil Considering New Digital Competition Legislation, *CSIS*, May 9, 2024. https://www.csis.org/analysis/brazil-considering-new-digital-competition-legislation.

[12] Bill No. 2768/2022, *Camara*. https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2214237&filename=PL%202768/2022.

[13] Brazil’s Digital Markets Act, *ITIF*, May 25, 2025. https://itif.org/publications/2025/05/25/brazil-digital-markets-act/.

[14] Digital Platforms: Competition Aspects and Regulatory Recommendations for Brazil, Oct. 10, 2024. https://www.gov.br/fazenda/pt-br/central-de-conteudo/publicacoes/relatorios/sre/digital-platforms-competition-regulatory-recommendations-brazil-en.pdf.

[15] Press Conference on Digital Platforms, Oct. 10, 2024. https://www.youtube.com/watch?v=cnZt9E_wsN0.

Further, Bill No. 4691/2024 includes provisions related to content moderation and, when necessary, content removal, which resembles Brazil's court actions on internet speech, which we discussed above. The bill seeks to establish ANATEL and CADE share responsibility as co-regulators of digital platforms above a certain size and subject them to certain obligations.[16]

CTA worries that if Brazil adopts these EU-style rules, it could unfairly target U.S. companies and hurt competition and innovation in Brazil, especially if regulators design these rules to only affect dynamic U.S. firms in the digital sector. The United States should push Brazil to commit to not adopt these discriminatory *ex ante* regulations.

Even in the absence of specific legislation, CADE aggressively targets U.S. technology companies, seeking to force them to follow DMA requirements locally through "interim measures" that essentially introduce tough European regulations that Brazil has not yet adopted.[17]

Data Localization

We urge USTR to uphold high-standard digital trade rules to ensure cross-border data flows. In successive comments to USTR for the National Trade Estimate ("NTE") reports, CTA categorizes data localization as a top-priority digital trade barrier. In fact, we include "Allows Cross Border Data Flows" as a scoring category for the annual Global Innovation Scorecard.[18] Countries with data localization laws or requirements have a lower score, while those facilitating free data movement receive a higher score. Unfortunately, Brazil earned a "D-" score in this category.[19] We support USTR ensuring that Brazil does not impose overly broad restrictions on the transfer of data.

Preferential Treatment of Local Content

The Brazilian Senate has approved Bill No. 2331/2022, directly targeting U.S. video platforms while favoring Brazilian broadcasters and imposing a platform-wide tax to fund Brazilian content development. The bill does not exempt platforms with user-generated content. Furthermore, the bill includes new provisions mandating minimum quantities of Brazilian audiovisual content that service providers must make available to the Brazilian market.[20] The President is expected to issue a decree that adopts these same requirements.

[16] *Id.* at 11.
[17] CADE issues interim measure against Apple, Mar. 11, 2025. https://www.gov.br/cade/en/matters/news/cade-issues-interim-measure-against-apple.
[18] *Id.* at 2.
[19] *Id.* at 2.
[20] *Id.* at 11.

Digital Services Tax

Brazil's Congress is moving forward with Digital Services Tax ("DST") proposals that could disproportionately impact U.S. companies. Lawmakers are debating seven DST bills, and President Lula has publicly backed these initiatives.[21] These measures clash with Brazil's current tax system and planned reforms, risking double taxation and placing U.S. firms at a considerable disadvantage compared to Brazilian competitors offering the same services.[22] By implementing these unilateral taxes, Brazil threatens fair competition, international tax cooperation, and creates greater barriers for U.S. businesses operating in the country.

Proposed AI Regulation

Bill No. 2238/2023, which recently passed the Senate and awaits in the Chamber of Deputies, raises serious concerns. In its current form, this legislation risks creating substantial barriers for U.S. artificial intelligence ("AI") developers and U.S. businesses seeking to export AI-related products and services to Brazil.[23] Addressing Bill No. 2238/2023 will directly promote the goals of the American AI Exports Program, as outlined in President Trump's Executive Order on July 23, 2025.[24]

The bill labels many types of AI as "high-risk," causing legal uncertainty and forcing developers and users to meet strict rules that may not match the real risks. The bill also fails to clearly separate the rules for companies that build AI from those that use it, especially for high-risk situations.[25]

CTA is particularly concerned about the bill's strict copyright provisions. The bill would require AI developers to pay for and disclose the use of Brazilian copyrighted materials used in AI model training, and it would apply these rules retroactively. Such provisions could place heavy burdens American AI companies, making it harder to provide U.S. AI solutions in the Brazilian market and creating bigger issues for cross-border digital trade.

In addition, the bill grants wide powers to a central regulatory authority, further contributing to legal uncertainty. Obligations for General Purpose AI ("GPAI") developers

---

[21] Exclusive: 'I won't humiliate myself': Brazil's president sees no point in tariff talks with Trump, *Reuters*, Aug. 6, 2025. https://www.reuters.com/world/americas/i-wont-humiliate-myself-brazils-president-sees-no-point-tariff-talks-with-trump-2025-08-06/.
[22] Brazil's Digital Tax Policy, *ITIF*, Feb. 27, 2025. https://itif.org/publications/2025/02/27/brazils-digital-tax-policy/.
[23] Bill No. 2238/2023, *LexML*, Apr. 28, 2023. https://www.lexml.gov.br/urn/urn:lex:br:camara.deputados:projeto.lei;pl:2023-04-28;2238.
[24] Executive Order 14320, *Promoting the Export of the American AI Technology Stack,* 90 Fed. Reg. 35393 (Jul. 23, 2025). https://www.federalregister.gov/documents/2025/07/28/2025-14218/promoting-the-export-of-the-american-ai-technology-stack.
[25] *Id.*

are considered inadequate. By forcing developers to fully comply even for low-risk uses, the bill could slow innovation and make them spend money on unnecessary requirements for safe applications.

Data Center Obligations

Brazil's ANATEL Resolution No. 780/2025 sets broad new requirements on data centers connected to telecommunications networks, mandating conformity assessment and certification to continue operating.[26] These rules set tough standards for operations, security, energy use, and the environment. Regulators adopted these measures without public input or a conducting a regulatory impact study, raising serious concerns about transparency, predictability, and following proper regulatory steps. For U.S. tech companies heavily invested in Brazil's cloud and data center market, these sudden, unilateral rules create a lot of uncertainty and drive up compliance costs. Skipping normal review processes also increases the risk of discriminatory rules or non-tariff barriers that block foreign companies.

Network Usage Fee

Brazil is weighing a network usage fee that would require U.S. technology and content companies to pay major local internet service providers, helping to fund telecommunications infrastructure.[27] Brazil's telecommunications regulator, ANATEL, introduced this proposal in a 2023 public consultation, using a "cost-sharing" approach that targets companies generating large amounts of data traffic with higher charges.[28] If Brazil approves this fee, U.S. firms would be hit hardest, facing costs that undermine their investments in Brazilian infrastructure and force them to subsidize local competitors by paying more than smaller, non-U.S. companies.

Brazil's Unfair, Preferential Tariffs

Information Technology Agreement

Brazil does not participate in the World Trade Organization ("WTO") Information Technology Agreement of 1997 ("ITA-1") or its 2015 expansion ("ITA-2"),[29] hence its low score in our Global Innovation Scorecard. Information and communication technologies account for just 0.32 percent of the country's exports and 9.79 percent of the country's imports. If Brazil joins the Information Technology Agreement (ITA), it could boost its economic growth by nearly a full percentage point over 10 years compared to not

---

[26] ANATEL Resolution No. 780/2025, *ANATEL*, 2025. https://informacoes.anatel.gov.br/legislacao/resolucoes/2025/2054-resolucao-anatel-780.
[27] Cost-Sharing Models Undermine the Global Internet, *Internet Society,* Dec. 1, 2023. https://internetsociety.org/resources/internet-fragmentation/brazils-cost-sharing-proposal/.
[28] *Id.*
[29] Information Technology Agreement, *WTO*. https://www.wto.org/english/tratop_e/inftec_e/inftec_e.htm.

joining.[30] Since the United States already participates in both ITA and ITA-2, encouraging Brazil to lower tariffs on tech products would provide a clear, "easy win" and increase U.S. tech exports to Brazil. In addition, USTR should urge Brazil to work with its Southern Common Market ("MERCOSUR") partners on accessing to ITA-1 and ITA-2 simultaneously, thereby integrating South America more broadly into global technology supply chains.

Intellectual Property Protection

Gray Market for Connected Devices

Brazil enforces strict regulations on cell phones and other protectionist policies designed to throttle imports of these products, such as rigorous certification mandates by ANATEL and multiple layers of taxation on imports. These measures create an environment of smuggled devices sold at much lower prices relative to legitimate products have flooded the Brazilian market.[31] This gray market severely undermines companies that comply with regulations, creating a major obstacle to investment and growth for consumer technology companies in Brazil. According to Brazil's Association of Electronics Manufacturers ("Abinee"), gray market channels account for 10% of smartphone sales, with Chinese brands like Xiaomi, Oppo, and Realme becoming top sellers.[32] These informal economy dynamics also hinder trade by discouraging foreign companies from entering the Brazilian market. To address this challenge, Brazil should simplify regulations and remove import barriers, not only for cell phones but for all connected devices, particularly televisions.

The widespread presence of gray market devices raises significant intellectual property ("IP") concerns, as these devices often bypass IP protections, leading to losses for legitimate manufacturers. The Government of Brazil must discourage retailers from carrying gray market devices, uphold IP standards, and foster a fair competitive environment. If Brazil fixes these issues with broad regulatory reforms, it can attract more investment, support responsible businesses, and help the consumer tech sector grow sustainably.

---

[30] Assessing How Brazil Would Benefit from Joining the ITA, *ITIF*, March 2019. https://www2.itif.org/2019-brazil-ita-exec-summary.pdf.
[31] *See,* Smartphone Smuggling in Brazil Reaches Unprecedented Scale. https://www.forbes.com/sites/angelicamarideoliveira/2024/04/01/smartphone-smuggling-in-brazil-reaches-unprecedented-scale/.
[32] *Id.*

Canada

Artificial Intelligence and Data Act (Bill C-27)

The framework for the Artificial Intelligence and Data Act (Bill C-27) should be amended to reflect industry standards. In addition, and in alignment with Article 11.4 of USMCA, Canada should explicitly balance the risk of overregulating against the benefits of innovation in the emerging artificial intelligence markets.[33] Aligning with the U.S. framework would ensure a more proportionate and effective regulatory environment, fostering innovation while addressing potential risks associated with AI.[34]

Quebec Bill 109

On May 21, 2025, Québec's Minister of Culture et des Communications introduced the now-tabled Bill 109, with a stated purpose to promote discoverability of and access to original French-language cultural content in the digital environment. It will have major implications for U.S.-based streaming companies, as well as manufacturers of connected devices. It grants broad authority to the Québec Cabinet to enact regulations that will impose new registration requirements, reporting and potential French content quotas, accessibility and discoverability requirements on digital platforms and manufacturers of TVs and connected devices. It also creates a new administrative unit within the Ministère de la Culture et des Communications under the name "Bureau de la découvrabilité des contenus culturels" (the BDCC) and gives the BDCC broad powers to enforce the bill. Similar to the Online Streaming Act, Bill 109 would hamper North American providers from accessing the market in Québec, thereby reducing regional integration, which runs antithetical to the goals of the CUSMA.

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.

---

[33] CUSMA – Chapter 11 – Technical barriers to trade, https://www.international.gc.ca/tradecommerce/trade-agreements-accords-commerciaux/agr-acc/cusma-aceum/text-texte/11.aspx?lang=eng.

[34] National Institute of Science and Technology, AI Risk Management Framework, (rel. Jan. 23, 2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

Ecuador

Restrictive Artificial Intelligence Regulations

Ecuador's proposed artificial intelligence regulations, introduced by the Data Protection Authority (SPDP), represent a significant trade barrier that threatens U.S. companies' market access and operational capabilities. The "Regulation for the Guarantee of Personal Data Protection Rights in the Use of Artificial Intelligence" creates multiple compliance challenges through jurisdictional overreach, as it conflicts with Ecuador's Digital Transformation Law (LOTDA) which designates MINTEL as the AI governance authority. The regulation imposes discriminatory operational burdens on foreign technology providers through mandatory human supervision requirements, complex traceability standards, and expansive audit rights. Of particular concern are the blanket prohibitions on crucial AI applications, including real-time biometric identification systems and synthetic content generation, which effectively bar U.S. companies from deploying innovative technologies in the Ecuadorian market. These restrictions, coupled with excessive compliance costs, create disproportionate barriers for U.S. businesses, especially affecting technology startups and SMEs. The proposed framework contradicts Ecuador's international commitments to facilitate digital trade and promote technological innovation, while establishing unnecessary obstacles that particularly impact U.S. companies' ability to compete effectively in Ecuador's digital economy.

EU and EU Member States

EU Corporate Sustainability Due Diligence Directive and Sustainability Omnibus Package

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

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

Germany

Competition / Ex Ante Rules

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

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.

Data localization

Indonesia is currently planning to revise Government Regulation No. 71/2019 ("GR71") that, based on the 2024 draft, potentially includes the expansion of data localization mandate to include five (5) broadly defined categories of data: civil registration, immigration, health, financial and 'other' data as determined by relevant ministries or institutions. The 'other' category is intentionally vaguely defined to allow for practically unlimited scope of data that must be stored in Indonesia. Data localization requirements limit the ability of international service providers to serve Indonesian customers with features and services that may not be available locally, as well as potentially restrict

Indonesian enterprises from providing their services to global customers. Expanding data localization requirements will also result in significant expenses that could otherwise be allocated to research and development to benefit Indonesian enterprises. Meanwhile, given the advances of technology and the cross-border nature of cyber threats, such restrictive policy may not necessarily improve the security posture and sovereignty of data that the government wishes to achieve.

Korea

Online Platform Monopoly Act (OPMA)

In September 2024, President Lee Jae-myung's campaign promise to implement prescriptive European-style digital trade regulations through a proposed Online Platform Monopoly Act (OPMA) disproportionally targets U.S. companies while exempting South Korea's powerful conglomerates and Chinese digital giants operating in the Korean market. Alarmingly, OPMA would "pre-designate" prominent American firms operating in Korea (Google, Apple, Meta, Coupang) through a mix of carefully tailored sectoral definitions and arbitrary market thresholds to apply heightened regulatory burdens, including forced transfer of source code and severe business restrictions. The Korean National Assembly has made passing OPMA a top priority, with proponents touting a "consensus to push forward quickly." Despite clear warnings from the Trump administration, Korea continues to pursue EU-style regulation including by expanding the Korea Fair Trade Commission (KFTC) to establish a new internal "Platform Bureau" to target the "online platform sector". These proposals mark a departure from Korea's traditional competition policy and threaten discriminatory application and innovation stifling results.

Notably, the new KFTC Chair plans to expedite platform legislation and has announced that he will ramp up regulations targeting such online platforms and expand targeted enforcement against these (largely American) companies.

Fairness in Online Platform Brokerage Transactions

In addition to OPMA, other bills proposing ex-ante regulation of U.S. digital service providers including the Fairness in Online Platform Brokerage Transactions ("Fairness Act") under consideration in Korea's National Assembly would apply only to specific sectors and set arbitrary revenue and user-base thresholds that are similarly designed to target successful U.S. companies. President Lee's administration has promised to fast-track the Fairness Act – which includes many of the excessive regulatory requirements and interventions in OPMA that would discriminate against major U.S. companies – and slow their ability to innovate and compete with South Korean and Chinese conglomerates.

Korea’s pursuit of discriminatory legislation against U.S. firms is an unnecessary irritant– and potential KORUS violation – to the longstanding bilateral relationship that creates an unlevel playing field for U.S. firms competing against rapidly growing Chinese e-commerce companies.

Mexico

“Kill-Switch” and Article 30-B in the 2026 Economic Package

A proposal in Mexico’s Economic Package would require digital service providers to grant the Tax Administration Service (SAT) permanent, real-time online access to their systems and records related to operations in Mexico. Non-compliance could result in the temporary blocking of digital – widely referred to as the “kill-switch” - as outlined under the Value-Added Tax Law (LIVA). Additionally, the SAT would coordinate with the newly created National Agency for Digital Transformation and Telecommunications to manage the technological infrastructure and data analysis associated with this obligation. These authorities have stated that the intention of this proposal is to capture Chinese ecommerce companies, but the language is broad and captures all providers. Both the new provision and the existing “kill-switch” provision raise serious concerns regarding Mexico’s USMCA commitments.

Changes to Customs Duty Rates

A proposal to amend Mexican customs Law would significantly change its customs duty structure by eliminating the simplified tariff classification system for Low-Value Shipments under US$2,500, previously known as "T1". Under the new system, the Secretariat of Finance will replace the current flat duty rates (tasa global) with variable rates. Without an exemption for USMCA partners, shipments valued between US$50 and US$2,500 will likely incur higher duties than the current flat rates of 17 to19%. This change not only increases operational burden but also introduces new risks related to misclassification and heightened regulatory scrutiny.

In addition, authorities now require extensive supporting documentation to confirm the authenticity of transactions and the accuracy of duty calculations. The commercial invoice alone will no longer be sufficient to meet compliance requirements, adding administrative burden and increasing the risk of procedural errors.

Nigeria

Data localization

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.

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

Ecommerce Guidelines

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

Vietnam

Data localization

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.

Digital Transformation Law (DTL)

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

Annex 3 – Other Existing Measures

Canada

Online Streaming Act

The Online Streaming Act, which entered into force in April 2023, updated Canada's Broadcasting Act to regulate online streaming services and provided discretion to the Canadian Radio-television and Telecommunications Commission (CRTC) on how to implement it. On June 4, 2024, the CRTC issued a decision to require foreign, largely U.S.-based music and audiovisual streaming service providers to pay 5% of their gross in-country revenue to certain Canadian cultural funds. In addition to the levy, the CRTC is designing additional discriminatory measures that target U.S. companies, including local content quotas and content discoverability mandates. The CRTC may also increase the financial levy to as high as 30%. In total, the Online Streaming Act could cost the U.S. industry $7 billion by 2030, which could have a chilling effect on streaming service providers in North America.

Process for Correction of Entries

The Canada Border Services Agency's (CBSA) Assessment and Revenue Management System (CARM) has eliminated the ability for importers to make blanket corrections to customs entries. Before the transition to CARM, importers were able to do this through the creation and correction of a CBSA Facility Information Retrieval Management System (FIRM) report. CARM instead requires individual correction of entries which can become exceedingly cumbersome when making annual corrections per agreed-upon Adjustment Regimes. The estimated correction times have skyrocketed from a single filing of the FIRM report by broker(s) to roughly 10 days for semi-annual corrections. Canada should commit to scalable corrective actions in automated systems CARM.

Copyright Act

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

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.

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.

Divergent Copyright Levy Systems

The EU's copyright levy system rests on Directive 2001/29/EC (the InfoSoc Directive), which harmonizes certain aspects of copyright and related rights in the information society[35]. Article 5(2)(b) lets Member States introduce private-copying exceptions so long as rightsholders receive "fair compensation," providing the legal basis for national levy schemes. Because the Directive grants Member States broad discretion in how they implement compensation, the system remains highly fragmented across the EU. In practice, stakeholders report widely divergent national measures: some jurisdictions apply no levies on certain devices, while others impose device-based charges and maintain complex, impractical reimbursement mechanisms for business users. These inconsistencies distort pricing, impede cross-border trade, and create heavy administrative burdens for firms operating in multiple Member States, and the lack of harmonization can result in de facto double charges on consumers—first via levies and again through licenses embedded in subscription streaming services. Although Article 12(2) requires the European Commission to evaluate implementation every three years, the Commission has not conducted a systematic review, even as digital consumption rises and private copying declines.

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"

---

[35] Directive 2001/29/EC. *On the harmonisation of certain aspects of copyright and related rights in the information society*. European Parliament and Council. https://eur-lex.europa.eu/eli/dir/2001/29/oj/eng.

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.

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.

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.

Import Authorization for Ultra-small Form Factor Computers and Servers and Information and Communication Technology (ICT) Equipment

In August 2023, the Indian government announced that beginning November 1, 2023, import authorizations are needed to import laptops, tablets, all-in-one personal computers, and ultra-small form factor computers and servers. The Ministry of

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

Restrictions on Multi Brand Retail

India has restricted American e-commerce providers from operating in the market on a level playing field as domestic companies, including through limitations on foreign companies operating in “multi-brand retail trading (MBRT).” This means that any company with foreign investment, including American e-commerce companies, cannot sell its own inventory directly to customers, requiring significant changes to their business models. These rules, which began in 2012 but were expanded in 2016 and 2018, establish several obstacles to American companies operating in India. American companies cannot invest more than 51% in a firm operating in India, with a minimum investment requirement of $100 million that carries obligations micromanaging companies’ business decisions. For example, at least 50% of this initial FDI must fund backend infrastructure such as processing, storage, distribution, and logistics, and at least 30% procurement of manufactured or processed products must be from Indian micro, small, and medium industries. American companies are prohibited from selling their own inventory directly to consumers and are only permitted to operate a marketplace business model. They also face severe restrictions for marketplace e-commerce operations, including being unable to set prices, facing limitations on inventory management, and being prohibited from entering seller exclusivity arrangements. Specifically, American marketplaces and their group entities cannot provide more than 25% of the inventory for any of the vendors using their service. The regulation undermines American companies’ ability to efficiently reach Indian consumers and optimize their supply chains. None of the above restrictions apply to domestic, non–FDI-funded entities. Domestic companies are permitted to operate inventory-based models without any additional conditions and have complete flexibility in pricing, inventory management, and seller exclusivity agreements for their e-commerce operations. These restrictions prevent leading U.S. e-commerce companies from accessing the rapidly growing Indian market, undermine current and potential investments in the U.S., and diminish U.S. technology leadership.

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 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 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.

Electronic Transaction Tax (ETT)

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

Kenya

Data localization

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 by the Korea Fair Trade Commission (KFTC)

Korea has long used antitrust law and competition policy to advance protectionist aims and promote discriminatory outcomes, but in recent years the Korea Fair Trade Commission (KFTC) has emerged as the primary mechanism to accomplish these ends, targeting U.S. companies with frequent dawn office raids, hyper-aggressive enforcement measures, and threats of criminal prosecution for common industry practices that are not considered criminal in any other country. Such excessive and unpredictable "competition law enforcement" not only leads to unjustified investigations and unwarranted penalties but also greatly constrains U.S. business operations in Korea.

For example, Google and YouTube face burdensome regulatory scrutiny over platform integration and network usage fees—even though Google's infrastructure supports nearly 30 percent of Korea's Internet traffic. Korea's restrictions on exports of location-based data services, such as Google Maps, disadvantages American companies seeking to optimize products globally. The KFTC is also threatening to disrupt Netflix's subscription-cancellation practices, demanding novel pro-rata refunds and signaling likely sanctions for non-compliance. The KFTC last year fined Coupang nearly $100 million for common retail practices like algorithm-based product placement, despite courts later suspending enforcement.

These unfair and abusive practices lead to significant compliance costs and in practice constitute major de facto barriers for U.S. companies seeking to compete in the Korean market – while Chinese and domestic firms expand with few restrictions. To enhance fairness, transparency, and due process in Korea, the U.S. government must ensure that the KFTC can no longer target or disproportionately disadvantage U.S. companies and interests by prioritizing updates to Chapter 16 of KORUS and/or implementing relevant USMCA provisions to prohibit regulatory frameworks and enforcement practices that disproportionally impact U.S. firms.

Mexico

Judicial Changes

While the Mexican government has the sovereign right to amend its constitution, the constitutional change in 2024 that has reshaped the country's judicial system will damage the long-standing trade and investment relationship between the United States and Mexico, as well as the rights of U.S. companies under USMCA. We respectfully urge the United States government to raise these concerns and recommend that the Sheinbaum Administration reverse course and adopt a more deliberate and thoughtful approach. The reform to remove all 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 American investors, the enforcement of USMCA may face additional challenges in the Investment chapter.

Constitutional Appeal Law (Amparo Law) Reforms

The reforms to the Amparo Law raises regulatory risk by limiting courts' ability to suspend administrative acts and narrowing eligibility relief, reducing predictability for businesses that rely on permits or authorizations. If the changes are perceived as limiting the ability to challenge government actions or weakening constitutional safeguards, investors may fear increased risks and less recourse in disputes. Such perceptions could deter both domestic and foreign investors, undermining confidence in the rule of law and the stability of the investment climate. Moreover, if these reforms result in prolonged or more complex judicial processes, they could increase costs and delays, which are unfavorable for business operations and investments. We respectfully urge the United States government to raise these concerns and recommend that the Sheinbaum Administration reverse course on these reforms.

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 commitments in the Custom Administration and Trade Facilitation Chapter. 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. Tax Administration Service'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[36] unless these payments are made. This issue extends beyond the consumer technology industry, affecting a wide range of sectors operating within the country.

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.

Barriers for Cloud in Financial Services

Mexico continues to enforce a 2021 regulation which requires electronic payment fund institutions to maintain a business continuity plan in the case of disaster recovery that

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

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

Abrupt Customs Changes

Mexico routinely makes major changes to its customs rules with no implementation period, which creates operational disruptions. Mexico should adhere to good regulatory practices in customs, including by providing notice and comment periods before making changes its customs rules and providing longer implementation periods before these changes enter into force, to provide stability for the shipment of goods.

Customs Valuation Methods

Mexico has instituted the use of reference prices for several product types rather than standard valuation methods, which results in importers having to declare artificially high customs values for these products. Mexico should recommit to standard valuation rules and address perceived dumping through anti-dumping investigations.

Other SAT Taxation Issues

Another serious concern is SAT's decision to reinterpret Mexico's Value Added Tax ("VAT") law retroactively. SAT's new approach denies companies the ability to claim refunds for VAT amounts included in claims paid to third party suppliers, even though this practice was previously permissible. SAT's retroactive application of the law, extending back to 2015, has led to demands for repayment of previous refunds and the imposition of fines and interest on U.S. and global companies that had complied with practices recognized by SAT.

Furthermore, some companies report VAT double taxation issues. SAT has asserted that, in addition to already-paid import VAT under Mexico's Industria Manufacturera, Maquiladora y de Servicios de Exportación ("IMMEX") virtual export program, companies must also pay input VAT on the same goods. These developments raise concerns for U.S. and global companies using IMMEX as a component of their North American manufacturing strategy.

Constitutional reforms on independent regulatory bodies

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

Tax ID registration affecting US SMEs

In 2020, Mexico passed legislation requiring U.S. businesses that store inventory in Mexico to register for a local tax ID with the Tax Administration Service (SAT) and file monthly tax reports. While this process alone is not novel, the process to obtain this tax ID, known as a Registro Federal de Contribuyentes (RFC), is extremely complicated and costly. This process alone has become the primary barrier for U.S. small and medium-sized enterprises (SMEs) that seek to sell their products to Mexican consumers and businesses.

To receive an RFC, U.S. businesses are required to have a local Mexican address and a local Mexican legal representative that shares 50% of the company’s tax liability, as well as pay income tax on all income generated in Mexico. The registration process is slow and bureaucratic, and involves 1) apostilling of documentation in the U.S., 2) translating all documentation to Spanish by a certified translator, 3) legalizing documentation with a Mexican Notary, 4) obtaining a SAT appointment (which can take one to four months due to limited availability), and 5) registering the RFC in SAT’s offices. All of these steps are offline and in-person and can take over five months, costing over $5,000, in addition to the costs of complying with income tax obligations.

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 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.

Taiwan

Tax Reciprocity

The absence of a U.S.–Taiwan tax reciprocity agreement continues to impede cross-border investment by imposing unequal tax treatment on American companies in Taiwan. Concluding such an agreement remains one of the most significant outstanding issues in the bilateral relationship and would reduce double taxation, lower compliance burdens, and facilitate capital flows. While the United States requires legislative authorization to finalize an accord, Taiwan does not require pre-conclusion authorization; once negotiated, the agreement would be ratified by the Legislative Yuan (LY). The current gap raises the cost of financing and operations, discourages small and medium-sized enterprises, and complicates talent mobility. As the United States and Taiwan advance trade negotiations, stakeholders urge both governments to prioritize resolution of this tax issue on a parallel track. Addressing this barrier would materially support increased bilateral investment and collaboration across sectors.

Thailand

Digital Platform Services (DPS) Decree

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

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

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

United Kingdom

Digital Markets, Competition, and Consumers Act

The Digital Markets, Competition and Consumers Act (DMCCA) is a new competition framework that came into force in January 2025. It is designed to regulate digital markets by designating firms with 'Strategic Market Status' (SMS) and imposing behavioral requirements and 'pro-competition interventions'. The regime empowers the UK Competition and Markets Authority (CMA) to address alleged competition issues in digital markets, particularly focusing on companies with 'substantial and entrenched market power', 'strategic significance', and turnover thresholds of over £25 billion globally or £1 billion in the UK. This framework represents a shift from traditional ex post market investigations to permanent regulatory oversight, enabling the CMA to impose forward-looking conduct requirements. While the CMA has not yet designated a firm with SMS, it has provisionally decided to designate Apple and Google with SMS in specific areas. A final decision is expected by 22 October 2025.

Vietnam

Data Law and its implementing decrees - Decree 165 and Decree 169

In November 2024, the National Assembly passed the Data Law. The Law went into force together with its implementing Decrees 165 and 169 on 1 July 2025. The Law and its implementing decrees have duplications with the PDP Law on regulations on personal data governance. The Prime Minister Decision No. 20/2025 dated 1 July 2025 supporting the execution of the Data Law and its Decree introduces new categories of “important data” and “core data” similar to China’s Data Security Law that can have chilling effects on foreign investors in Vietnam. The Data Law and Decree 165 impose onerous obligations on individuals and organizations for authenticating and ensuring the accuracy of created data as well as approvals for cross border transfers of core data. The Data Law and Decree 169 mandate licensing and regulating data products and services such as data intermediary, data analysis and aggregation products and services, and data exchange services. An implication of such requirements is that offshore enterprises not incorporated or registered in Vietnam would not be allowed to offer any of the above service to Vietnamese customers.