ACT Association for Competitive Technology

October 29, 2026

Mark A. DiPlacido
Chair of the Trade Policy Staff Committee
Office of the U.S. Trade Representative
600 17th Street, N.W.
Washington, District of Columbia 20508

RE: Comments of the Association for Competitive Technology (ACT), Request for Comments on Significant Foreign Trade Barriers for the 2027 National Trade Estimate Report [91 FR 58247; Docket No. USTR-2026-0498]

In response to the Federal Register notice issued on September 14, 2026,[1] ACT hereby submits comments to the United States Trade Representative (USTR) in response to its request for public input on the 2027 National Trade Estimate (NTE) Report on Foreign Trade Barriers.

ACT is a not-for-profit trade association representing the global small business technology developer community, including innovators and startups in the software development and high-tech space.[2] As the world embraces mobile technologies, our members create the innovative products and services that drive the global digital economy by improving workplace productivity, accelerating academic achievement, and helping people lead more efficient and healthier lives. Today, the U.S. app economy is worth more than $1.8 trillion annually and provides over 6.1 million American jobs.[3]

While the global digital economy holds great promise for ACT member companies, our members face a diverse array of challenges when entering new markets. These challenges, commonly referred to as "trade barriers," are reflected in the laws, regulations, policies, or practices that protect domestic goods and services from foreign competition, artificially stimulate exports of particular domestic goods and services, or fail to provide adequate and effective protection of intellectual property rights. These barriers take many forms but have the same net effect: impeding U.S. exports and investment.

We applaud USTR's efforts to understand and examine the most important foreign barriers affecting U.S. exports of goods and services, foreign direct investment, and intellectual property rights. We

[1] 91 FR 58247 (Sept. 14, 2026).
[2] ACT, About, https://actonline.org/about.
[3] ACT, State of the U.S. App Economy: 2023, https://actonline.org/wp-content/uploads/APP-Economy-Report-FINAL-1.pdf.

1401 K Street, NW, Suite 501
Washington, D.C. 20005

+1 (202) 331 - 2130 www.ACTonline.org /US-ACT @ACTonline

commit to working with USTR and other stakeholders to reduce or eliminate these barriers. With respect to digital trade, the small business innovators we represent prioritize the following principles:

- Enabling Cross-Border Data Flows: The seamless flow of data between economies and across political borders is essential to the functioning of the global economy, and for American small business technology developers as they seek access to new markets.

- **Prohibiting Data Localization Policies:** American companies looking to expand into new markets often face regulations that force them and other foreign providers to build and/or use local infrastructure in the country. Data localization requirements seriously hinder imports and exports, reduce an economy's international competitiveness, and undermine domestic economic diversification.

- **Prohibiting Customs Duties and Digital Service Taxes on Digital Content:** American innovators must take advantage of the internet's global nature to reach customers who live outside of the United States. However, the tolling of data crossing political borders with the purpose of collecting customs duties directly contributes to the balkanization of the internet. Digital services taxes and network usage fees imposed on content and application providers have the same effect, singling out U.S. digital services for new costs that small developers are least able to absorb. These practices jeopardize the efficiency of the internet and effectively block innovative products and services from market entry.

- **Ensuring Market Entry is Not Contingent on Source Code Transfer or Inspection:** Some governments have proposed policies that require companies to transfer, or provide access to, proprietary source code as a requirement for legal market entry. Intellectual property is the lifeblood of app developers' and tech companies' innovation; the transfer of source code presents an untenable risk of theft and piracy. Government policies that pose these requirements are serious disincentives to international trade.

- **Preserving the Ability to Utilize Strong Encryption Techniques to Protect End User Security and Privacy:** Global digital trade depends on the use of strong encryption techniques to keep users safe from harms like identity theft. However, some governments continue to demand that backdoors be built into encryption keys for the purpose of government access. These policies jeopardize the safety and security of data, as well as the trust of end users, by creating known vulnerabilities that unauthorized parties can exploit. From a privacy and security standpoint, the viability of a technology developer's product depends on the trust of its end users.

- **Securing Intellectual Property Protections:** The infringement and theft of intellectual property and trade secrets threatens the success of American innovators and hurts the billions of consumers who rely on their products and services. These intellectual property violations can lead to customer data loss, interruption of service, revenue loss, and reputational damage – each alone a potential "end-of-life" occurrence for a small company. The adequate and effective protection and enforcement of intellectual property rights is critical to the digital economy innovation and growth.

- **Avoiding the Misapplication of Consumer Protection and Competition Laws to New and Emerging Technology Markets:** Various regulators, including key trading partners, are currently considering or implementing policies that would put mandates on nascent and developing emerging technology markets. For example, some regulators are jeopardizing small businesses' ability to compete by upending the functionality of digital platforms that lower overhead costs, greater consumer access, simplified market entry, and strengthened intellectual property protections. Others are considering interventions into undefined and emerging technology markets, such as artificial intelligence. Foreign governments upending technology markets through misguided regulations inconsistent with U.S. law will disadvantage American innovators and serve as significant trade barriers.

Traditionally, USTR has been a consistent supporter of pursuing the above principles in international trade discussions. During the previous Administration, USTR withdrew its support for several of these policies in its NTE for 2024, including enabling cross-border data flows, avoiding forced data localization mandates, protecting source code, and ensuring digital products are not unduly discriminated against, a shift that ACT and a coalition of small business associations opposed.[4] We commend USTR for returning to these principles. The Administration has directed USTR to respond to foreign digital services taxes and other discriminatory measures that target U.S. companies,[5] and the Agreements on Reciprocal Trade concluded in 2025 and 2026 include commitments by trading partners to refrain from imposing digital services taxes, to support a permanent moratorium on customs duties on electronic transmissions, and to allow the transfer of data across trusted borders.[6] In the August 2025 framework with the United States, the European Union also confirmed that it will not adopt or maintain network usage fees.[7] We also support USTR's response after the World Trade Organization (WTO) moratorium on customs duties on electronic transmissions lapsed at the Fourteenth Ministerial Conference in Yaoundé in March 2026, when the United States and other WTO members committed in a joint statement to continue not imposing such duties among themselves.[8] The OECD/G20 Inclusive Framework's January 2026 agreement on a side-by-side system for the global minimum tax did not resolve digital services taxes, which several trading partners continue to impose or propose.[9] Predictable, rules-based digital trade commitments

[4] Letter from ACT and Small Business Cosigners re USTR Digital Trade (Nov. 3, 2023), https://actonline.org/wp-content/uploads/Small-Business-Ltr-re-USTR-Digital-Trade-3-Nov-2023-w-cosigners-1.pdf.

[5] The White House, Memorandum on Defending American Companies and Innovators From Overseas Extortion and Unfair Fines and Penalties (Feb. 21, 2025), https://www.whitehouse.gov/presidential-actions/2025/02/defending-american-companies-and-innovators-from-overseas-extortion-and-unfair-fines-and-penalties/.

[6] USTR, Fact Sheet: The United States and Malaysia Reach an Agreement on Reciprocal Trade (Oct. 2025), https://ustr.gov/about/policy-offices/press-office/fact-sheets/2025/october/fact-sheet-united-states-and-malaysia-reach-agreement-reciprocal-trade; Digital Policy Alert, Digital Trade Commitments in US Tariff Deals (Apr. 2, 2026), https://digitalpolicyalert.org/blog/us-priorities-tariff-deals.

[7] Congressional Research Service, U.S.-EU Tariffs and Trade Framework Agreement, IF13107 (Sept. 18, 2025), https://www.everycrsreport.com/files/2025-09-18_IF13107_d3cc0bb6fb1dbc209383cf6e005b19e985882597.html.

[8] USTR, Press Release Regarding the WTO's 14th Ministerial Conference (Mar. 30, 2026), https://ustr.gov/about/policy-offices/press-office/press-releases/2026/march/press-release-regarding-wtos-14th-ministerial-conference; Third World Network, WTO: US & allies revive plurilateral E-com moratorium amid deadlock (Sept. 2026), https://twn.my/title2/wto.info/2026/ti260902.htm.

[9] Department of Finance (Ireland), OECD Side-by-Side Agreement Statement (Jan. 5, 2026), https://www.gov.ie/en/department-of-finance/press-releases/oecd-side-by-side-agreement-statement.

matter most to U.S. small technology firms, which have limited capacity to navigate divergent foreign regulatory regimes and rising compliance costs. We therefore urge USTR to hold trading partners to these commitments, to monitor whether they are implemented, and to use the 2027 NTE report to identify measures that conflict with them.

Next, we would like to highlight specific trade barriers related to intellectual property (IP). The infringement and theft of IP online threatens consumer welfare by undermining the ability of creators of digital content to innovate, invest, and hire. App developers that drive the global economy lose billions of dollars in revenue each year due to pirated apps and IPR violations. In the five years before 2018, mobile app developers and publishers lost an estimated $17.5 billion to pirated apps.[10] Such a loss of revenue presents a major threat to the success of ACT's members, their consumers, and the workforce that supports the creation and growth of digital products and services. Each kind of IPR (copyrights, trademarks, patents, and trade secrets) represents distinct utilities upon which ACT members depend. IPR violations lead to customer data loss, interruption of service, revenue loss, and reputational damage – each alone is a potential "end-of-life" occurrence for a small app development company. Common IPR violation scenarios include:

- **Copying of an App:** An infringer will completely replicate an app but remove the digital rights management (DRM) component, enabling them to publish a copy of an app on illegitimate websites or legitimate app stores.

- **Extracting and Illegally Reusing App Content:** An infringer will steal content from an app—sounds, animations, characters, video, and the like—and repurpose it elsewhere or within their own app.

- **Disabling an App's Locks or Advertising Keys:** An infringer will change advertising keys to redirect ad revenue from a legitimate business to theirs. In other instances, they will remove locked functions like in-app purchases and security checks meant to prevent apps from running on devices with removed software restrictions (jailbroken devices).

- **"Brand-Jacking" of an App:** An infringer will inject malicious code into an app that collects users' private information and republishes a copy of the app. The republished app looks and functions like the original—often using the same name, logo, or graphics—ultimately luring customers who trust the brand into downloading the counterfeit app and putting their sensitive information at risk. A survey of ACT members indicates that one-third of sampled members with trademarks have experienced brand-jacking.[11]

- **Sideloading of an App:** Piracy has rapidly adapted to new technologies in the app ecosystem and, in some instances, has artificially capped customer beneficial use of digital platforms - with 80 percent of piracy attributable to illegal video streaming through devices and apps.[12]

[10] John Koetsier, The Mobile Economy Has a $17.5B Leak: App Piracy, Forbes (Feb. 2, 2018), https://www.forbes.com/sites/johnkoetsier/2018/02/02/app-publishers-lost-17-5b-to-piracy-in-the-last-5-years-says-tapcore/.
[11] ACT, Survey Says: IP is Essential to Innovation (June 21, 2022), https://actonline.org/2022/06/21/survey-says-ip-is-essential-to-innovation/.
[12] David Blackburn, PH.D. et. al., Impacts of Digital Video Piracy On The U.S. Economy (June 2019), https://www.theglobalipcenter.com/wp-content/uploads/2019/06/Digital-Video-Piracy.pdf.

Apps themselves have become the conduit through which all other content is pirated. The reality is that apps providing access to pirated movies, music, and television are available on all platforms, although less so on mobile platforms thanks in large part to app store prohibitions on content piracy and measures to prevent sideloading (downloading software onto a smart device from outside the main app store). A report by the Digital Citizens Alliance on ad-supported piracy highlighted several examples of apps being used to provide free access to content. Apps like MyMuzik and YTSMovies are just two of hundreds of results from a simple search for "free streaming apps." Some piracy apps, such as Cine Vision V5 and MegaFlix have outperformed legitimate applications by stealing their streaming content.[13] Piracy, like illegal streaming, is costing content owners billions each year.

- **Misappropriation of a Trademark to Intentionally Confuse Users:** Disregarding trademark rights, an infringer will seek to use an app's name or trademarked brand to trick users into providing their information to the infringer for exploitation.

- **Illegal Use of Patented Technology:** An infringer will utilize patented technology in violation of the patent owner's rights. Our members commonly experience such infringement in both utility patents and design patents (e.g., graphical user interfaces).

- **Government Mandated Transfer of IPR To Gain Market Entry:** A market regulator will impose joint venture requirements, foreign equity limitations, ambiguous regulations and/or regulatory approval processes, and other creative means (such as source code "escrowing") that force U.S. companies to transfer IPR to others in order to access their market.

- **Government Failure to Protect Trade Secrets:** An infringer will intentionally steal a trade secret, and subsequently benefit from particular countries' lack of legal protections and/or rule of law. The victim of the theft will be unable to protect their rights through the legal system.

Relatedly, ACT notes our growing concern with third-party litigation funding (TPLF) used as a mechanism to abuse patent process in the United States and internationally against U.S. companies. While this issue is faced globally, we focus on its impact to the U.S. market. Non-practicing entities (NPEs) initiate a majority of the abusive and frivolous patent infringement suits in the United States[14] and many NPE suits are financially backed by unnamed investors hidden through shell corporations or wealth funds that may have a real interest in the outcome of litigation.[15] TPLF has affected critical U.S. technology industries, including telecommunication, automotives, and semiconductors. Funders may be individual entities seeking economic gain or competing countries strategically undermining essential U.S. industries and U.S. national security. The serious harms to

[13] Ernesto Van der Sar, 'Pirate' Streaming Apps Beat Netflix and Disney in Brazil's Play Store (June 16, 2022), https://torrentfreak.com/pirate-streaming-apps-beat-netflix-and-disney-in-brazils-play-store-220616/.
[14] Love, Brian J. and Lefouili, Yassine and Helmers, Christian, Do Standard-Essential Patent Owners Behave Opportunistically? Evidence from U.S. District Court Dockets (November 8, 2020), 17, https://www.tse-fr.eu/sites/default/files/TSE/documents/doc/wp/2020/wp_tse_1160.pdf/.
[15] See In re Nimitz Technologies LLC, No. 23-103 (Fed. Cir. 2022); see also Unified Patents, Litigation Investment Entities: The Investors Behind the Curtain (Feb. 21, 2023), https://www.unifiedpatents.com/insights/2023/2/21/litigation-investment-entities-the-investors-behind-the-curtain.

the U.S. market evidenced by TPLF will undermine equity for U.S. businesses, workers, and consumers. We urge the USTR to consider all potential motivations of TPLF and how to address its abusive presence in the U.S. IP system and in IP systems around the world that are utilized by U.S. companies. The availability of anonymous investment sources enables bad actors to flood adjudicating bodies with potentially illegitimate claims. The Unified Patent Court (UPC) in Europe, now in operation, risks escalating this issue by allowing abusers to engage in multi-jurisdictional litigation and collect significant damages from European and U.S. companies that allegedly infringe on European patents. USTR should lead the U.S. government (USG) in examining the motivations of individual entities and competing economies to use TPLF and adopting strong disclosure requirements in all relevant U.S. venues, including the U.S. International Trade Commission (USITC), the U.S. Patent and Trademark Office (USPTO), and the U.S. federal courts, building on the funding disclosure orders that some courts, such as the U.S. District Court for the District of Delaware, already apply.[16] Legislation pending in Congress would advance this goal, including the Litigation Transparency Act of 2025 (H.R. 1109), which would require parties in federal civil actions to disclose and produce third-party funding agreements, and the Protecting Our Courts from Foreign Manipulation Act of 2025 (H.R. 2675), which would bar litigation funding from foreign states and sovereign wealth funds and require disclosure of other foreign funding.[17] The USTR should similarly encourage affected foreign jurisdictions to adopt the same or similar requirements to ensure full transparency in global IP litigation proceedings.

We also draw USTR's attention to activities in certain international fora that are responsible for the creation of potential digital trade barriers or seek to legitimize policies that inhibit digital trade. For example, ACT is a leading advocate against efforts within the United Nations' International Telecommunication Union (ITU) to develop pro-regulatory approaches to "over-the-top" (OTT) services – any service accessible over the internet or utilizing telecommunications network operators' networks.[18] In the ITU, ACT worked to highlight the benefits of OTT to economies of all sizes across sectors. We continue to work to educate the public and other governments on how a new layer of regulation over OTT services will stifle growth, and we continue to oppose pro-regulatory OTT service proposals, including draft guidelines on cost contribution mechanisms between OTT providers and telecommunications operators that ITU-T Study Group 3 is developing in its 2025-2028 study period, which would lend ITU support to network usage fees on content and application providers.[19] In July 2026, ACT joined a broad coalition of associations in a letter urging ITU-T member delegations to oppose mandatory network usage fees and support an open, innovative, and

[16] U.S. District Court for the District of Delaware, Chief Judge Colm F. Connolly, Standing Order Regarding Third-Party Litigation Funding Arrangements, https://www.ded.uscourts.gov/judge/chief-judge-colm-f-connolly.

[17] Litigation Transparency Act of 2025, H.R. 1109, 119th Cong. (introduced Feb. 7, 2025), https://www.govinfo.gov/app/details/BILLS-119hr1109ih; Protecting Our Courts from Foreign Manipulation Act of 2025, H.R. 2675, 119th Cong. (introduced Apr. 7, 2025), https://www.govinfo.gov/app/details/BILLS-119hr2675ih.

[18] Comments of ACT to the ITU Council Working Group on International Internet-Related Public Policy Issues Regarding its Open Consultation, Public Policy Considerations for OTTs, ITU, August 18, 2017, available at https://www.itu.int/en/Lists/consultationJune2017/Attachments/31//App%20Assn%20Comments%20re%20ITU%20OTT%20Consultation%20081817.pdf.

[19] ITU-T Study Group 3, Executive Summary of ITU-T Study Group 3 Meeting (Nov. 2025), https://www.itu.int/en/ITU-T/studygroups/2025-2028/03/Documents/SG3_Executive_Summary_Nov-2025.pdf.

sustainable internet.[20] We appreciate that the United States disassociated itself from a Study Group 3 technical report on OTT reporting in November 2025. ACT has called on the ITU to seek consensus across stakeholder groups to reduce barriers to the digital economy, which will benefit the billions of internet users around the globe. We recommend that the Trade Policy Staff Committee include the concerning proposals from international fora like the ITU that inhibit the free flow of data and digital commerce in the NTE, and we urge USTR to work with its interagency partners to oppose such proposals at the ITU Plenipotentiary Conference in Doha, Qatar, from November 9 to 27, 2026.[21]

Several of the barriers described below concern the licensing and enforcement of standard-essential patents (SEPs). ACT's comments in the 2026 Special 301 Review address these issues in detail, consistent with the core principles for SEP licensing set out in CEN-CENELEC Workshop Agreement CWA 95000,[22] so we summarize them briefly here and ask USTR to reflect them in the 2027 NTE report as barriers to market access for U.S. businesses that build on technical standards.

Below, we highlight numerous country-specific trade barriers that our members face, and we urge their inclusion in the Trade Policy Staff Committee's (TPSC) 2027 NTE report. The practices highlighted below include both implemented and proposed policies, both of which should be considered by USTR.

ARGENTINA

Issue: Data Localization for Public Sector Disaster Recovery

In May 2026, Argentina's National Cybersecurity Center (Centro Nacional de Ciberseguridad) issued Disposition 1/2026, a technical regulation on contingency and recovery plans for National Public Sector entities that requires them to maintain backup data centers at least 1,500 kilometers from their primary site, with 180 days to comply.[23] Requirements tied to physical facilities at fixed distances do not reflect how modern cloud services provide resilience across multiple regions, and they risk steering public sector customers away from the cloud services that U.S. providers, and the small developers that build on them, offer. We urge USTR to press Argentina to adopt technology-neutral, outcome-based resilience requirements that recognize multi-region cloud architectures as compliant.

Issue: Cross-Border Data Transfers

Argentina does not recognize the United States as an adequate destination for transfers of personal data, so U.S. companies must rely on contractual safeguards that add cost and delay. In the U.S.-

[20] Joint Letter to ITU-T Member Delegations (July 2026).
[21] ITU, What is PP-26?, https://pp.itu.int.
[22] Association for Competitive Technology, Comments on the 2026 Special 301 Review (2026); CEN-CENELEC, CWA 95000, Core Principles and Approaches for Licensing of Standard Essential Patents (2019), https://2020.standict.eu/sites/default/files/CWA95000.pdf.
[23] Centro Nacional de Ciberseguridad, Disposición 1/2026, Boletín Oficial de la República Argentina (May 13, 2026), https://www.boletinoficial.gob.ar/detalleAviso/primera/341893/20260513; Convercom, Ciberseguridad: la administración nacional deberá tener datacenters de respaldo a más de 1500 km del principal, posiblemente en la Patagonia (May 2026), https://convercom.info/comunidades/conectividad/ciberseguridad-administracion-nacional-debera-tener-datacenters-respaldo-mas-1500-km-del-principal-posiblemente-patagonia/.

Argentina Agreement on Reciprocal Trade and Investment signed in February 2026, Argentina committed to recognize the United States as a jurisdiction that provides adequate protection for cross-border data transfers.[24] We urge USTR to ensure that Argentina implements this commitment promptly.

AUSTRALIA

Issue: Prohibitions on the Use of Strong Encryption

ACT remains concerned with Australian policymaking efforts that stand to undercut the ability to leverage end-to-end encryption and otherwise undermine privacy protection practices, notably through its failure to revise the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018. ACT continues to work with the Australian government to reform surveillance and privacy frameworks while protecting online privacy and security.

Issue: Digital Platform Regulation

In 2020, the Australian Competition and Consumer Commission (ACCC) launched its Digital Platform Services Inquiry at the behest of the Australian government.[25] ACCC provided the Australian government's Treasurer with an interim report on the inquiry on September 30, 2020,[26] and provided further interim reports every six months until the inquiry concluded with a final report, which ACCC published on June 23, 2025. In December 2024, the Australian Treasury officially proposed a new digital competition regulatory intervention, with comments due February 14, 2025,[27] and as of mid-2026 the proposed regime remained under development.[28] ACT provided detailed views on digital platforms and competition, as well as reactions and feedback on specific conclusions raised by ACCC in its September 2022 interim report[29] and participated in a stakeholder hearing that took place in June 2022.

---

[24] Office of the U.S. Trade Representative, Fact Sheet: The United States and Argentina Agree to a Framework for an Agreement on Reciprocal Trade and Investment (Nov. 2025), https://ustr.gov/about/policy-offices/press-office/fact-sheets/2025/november/fact-sheet-united-states-and-argentina-agree-framework-agreement-reciprocal-trade-and-investment; Digital Policy Alert, United States and Argentina signed Agreement on Reciprocal Trade and Investment, including measures recognising US as an adequate jurisdiction for cross-border data transfers (Feb. 2026), https://digitalpolicyalert.org/event/38807-united-states-and-argentina-signed-agreement-on-reciprocal-trade-and-investment-including-measures-recognising-us-as-an-adequate-jurisdiction-for-cross-border-data-transfers.

[25] https://www.accc.gov.au/inquiries-and-consultations/finalised-inquiries/digital-platform-services-inquiry-2020-25.

[26] https://www.accc.gov.au/inquiries-and-consultations/finalised-inquiries-and-monitoring/digital-platform-services-inquiry-2020-25/september-2020-interim-report.

[27] https://treasury.gov.au/consultation/c2024-547447; ACT, Comments of ACT to the Treasury, Proposal Paper: A New Digital Competition Regime (Feb. 14, 2025), https://actonline.org/post/comments-of-act-the-app-association-to-the-treasury-requests-for-comments-proposal-paper-a-new-digital-competition-regime/.

[28] Australian Government, Competition and Consumer Policy in Digital Markets, Contribution from Australia, OECD Competition Committee, DAF/COMP/WD(2026)27 (June 2026), https://one.oecd.org/document/DAF/COMP/WD(2026)27/en/pdf

[29] https://www.accc.gov.au/inquiries-and-consultations/finalised-inquiries-and-monitoring/digital-platform-services-inquiry-2020-25/september-2022-interim-report.

ACT has significant concerns with the apparent positioning of the Australian government by ACCC and Treasury to interject itself into the digital economy without an evidence base to support such an intervention, which would jeopardize the functionality of mobile operating systems and software distribution platforms that have enabled countless American small businesses to grow, including with respect to intellectual property enforcement at the platform level. We therefore request that Australia's digital platform regulatory efforts, and the risks they pose to American small business innovators that rely on software distribution platforms for intellectual property rights protections, be captured in the 2027 NTE report and that the U.S. government work with Australia to mitigate the risks such an intervention would pose while supporting U.S. small business digital economy trade and leadership.

Issue: Artificial Intelligence Regulation

In December 2025, the Australian government released its National AI Plan, which set aside earlier proposals for mandatory guardrails on high-risk AI, including general-purpose AI models, and instead relies on existing laws to address AI risks.[30] ACT supports this approach, which is consistent with a risk-based framework that applies existing law first. However, following the Prime Minister's July 2026 announcement that AI laws will be introduced, the Department of the Prime Minister and Cabinet has proposed conditions on frontier AI training in Australia, including incident reporting to Australian authorities and contributions to local research and compute access.[31] ACT is concerned that new AI-specific obligations would impose substantial compliance burdens on U.S. companies offering AI products and services in Australia and inhibit our members' ability to compete there, and we ask USTR to encourage Australia to keep any new measures risk-based and grounded in existing law.

Issue: Data Center Standards and AI Infrastructure Conditions

In September 2026, the Department of the Prime Minister and Cabinet released a consultation paper proposing mandatory national minimum standards for data centers with 30 MW or more of capacity, including requirements to engage meaningfully with communities, draw on local suppliers and content where possible, and support workforce training, as well as conditions on frontier AI training that could include making compute available to Australian start-ups, researchers, and small businesses.[32] At the state level, the New South Wales Data Centre Policy Framework released in August 2026 anticipates local content and procurement requirements,[33] and Victoria expects data center permit applications lodged on or after September 23, 2026, to meet a ministerial Statement of Expectations that addresses local jobs, skills, and benefit.[34] ACT filed comments on the federal

[30] Region Canberra, Mandatory AI guardrails put on hold with the release of National Plan (Dec. 2, 2025), https://region.com.au/mandatory-ai-guardrails-put-on-hold-with-the-release-of-national-plan/926410/

[31] Department of the Prime Minister and Cabinet, Getting it right: Building AI infrastructure that works for Australia, Consultation Paper (Sept. 2026), https://www.pmc.gov.au/sites/default/files/resource/download/ai-consultation-paper.pdf

[32] Department of the Prime Minister and Cabinet, Getting it right: Building AI infrastructure that works for Australia, Consultation Paper (Sept. 2026), https://www.pmc.gov.au/sites/default/files/resource/download/ai-consultation-paper.pdf

[33] NSW Government, NSW Data Centre Policy Framework (Aug. 2026), https://www.infrastructure.nsw.gov.au/media/iosp3yuo/id0073_nsw-data-centre_policy-framework.pdf

[34] Victorian Department of Transport and Planning, Sustainable Data Centre Action Plan (Sept. 2026), https://www.planning.vic.gov.au/guides-and-resources/guides/sustainable-data-centre-action-plan

consultation in October 2026. ACT is concerned that local supplier, local content, and compute-sharing conditions could operate as de facto local content requirements and impose disproportionate costs on the U.S. cloud and AI providers that small developers rely on. We ask USTR to monitor these measures and encourage Australia to keep them non-discriminatory and consistent with its commitments under the U.S.-Australia Free Trade Agreement (AUSFTA).

Issue: Merger Policy Reform

Since January 1, 2026, Australia has required mandatory notification of acquisitions that meet revenue and transaction value thresholds, including thresholds that aggregate acquisitions over the previous three years and that require a very large acquirer to notify the purchase of a target with as little as A$10 million in Australian revenue, creating new challenges for small businesses seeking to enter pro-competitive transactions.[35] For ACT members, acquisition is often a critical path for future growth. While we share the goals of creating an efficient and transparent process for mergers and acquisition (M&A) review in Australia, ACT continues to encourage the Australian government to ensure that the new regime does not unfairly increase burdens on small companies or prevent pro-competitive transactions.[36] Relatedly, in August 2024, more than 50 of ACT's small business technology developer members signed an open letter to global regulators advising caution when updating existing merger rules, and to emphasize the importance that M&A has in the startup ecosystem. Building on its longstanding advocacy to Australian policymakers on competition issues, ACT will continue to work with its members to advocate for merger policy reform that supports small company innovation and growth and will work to bring the voice of small technology developers to the table as the Australian government implements the new regime.

Issue: News Bargaining Incentive

In August 2026, Australia enacted the News Media Bargaining Charge Act 2026 and related legislation implementing the News Bargaining Incentive announced in December 2024.[37] The scheme imposes a 2.75 percent charge on the Australian digital advertising revenue of significant social media and search services whose relevant revenue exceeds A$250 million, for reporting periods starting on or after January 1, 2025, and grants an offset only to platforms with new agreements with at least eight different news business groups.[38] The charge applies whether or not a platform carries news content.[39] ACT is concerned that the charge operates as a discriminatory digital levy that falls primarily on U.S. companies and sets a precedent that other governments may

[35] Australian Competition and Consumer Commission, About thresholds and exemptions, https://www.accc.gov.au/business/mergers-and-acquisitions/thresholds-for-notifying-acquisitions

[36] ACT, Comments to the Australian Competition and Consumer Commission on the Draft Merger Assessment Guidelines (Apr. 17, 2025), https://actonline.org/post/act-the-app-associations-comments-to-the-australian-competition-and-consumer-commission-draft-merger-assessment-guidelines/.

[37] News Media Bargaining Charge Act 2026 (Cth), No. 78, 2026, https://www.legislation.gov.au/C2026A00078/latest/text

[38] News Media Bargaining (Administration) Act 2026 (Cth), ss. 7-9, 13, 17, https://www.legislation.gov.au/C2026A00077/asmade/2026-08-26/text/original/epub/OEBPS/document_1/document_1.html

[39] The Hon Stephen Jones MP, Albanese Government to establish News Bargaining Incentive (Dec. 12, 2024), https://ministers.treasury.gov.au/ministers/stephen-jones-2022/media-releases/albanese-government-establish-news-bargaining-incentive

follow. We ask USTR to include the charge in the 2027 NTE report and to press Australia to reconsider it consistent with its AUSFTA commitments.

Issue: Online Safety Obligations on App Stores and Developers

Australia's social media minimum age obligation, which requires age-restricted platforms to take reasonable steps to prevent users under 16 from holding accounts, took effect on December 10, 2025, with civil penalties of up to A$49.5 million.[40] Separately, industry codes registered under the Online Safety Act 2021 have required app stores since March 9, 2026, to take appropriate steps to prevent users under 18 from downloading apps rated R18+, with age checks required by September 9, 2026.[41] In September 2026, the government released an exposure draft of the Online Safety Amendment (Digital Duty of Care) Bill 2026, which would impose a broad statutory duty of care on online services, including app distribution services, backed by civil penalties of up to 60,000 penalty units.[42] ACT supports protecting young people online, but layered and overlapping obligations on app stores and on the developers who distribute through them raise compliance costs for small businesses and create legal uncertainty. We ask USTR to encourage Australia to keep these measures proportionate, risk-based, and consistent with its trade commitments.

Issue: Privacy Act Reform

On August 31, 2026, the Attorney-General's Department released an exposure draft of the Privacy Amendment (Personal Data Protection) Bill 2026, the second tranche of Privacy Act reforms, with submissions due September 18, 2026.[43] The draft would require consent for trading in personal information, including disclosures for direct marketing and online behavioral advertising, and would give individuals a right to erasure against large digital platforms defined by A$500 million in group revenue or 2.5 million average monthly Australian users.[44] ACT filed comments on the exposure draft. Platform thresholds of this kind fall primarily on U.S. companies, and new consent rules for advertising-supported services would raise costs for the small developers that rely on them to reach customers. We ask USTR to engage with Australia to ensure the final bill is interoperable with international privacy frameworks and does not discriminate against U.S. providers.

Issue: Tax Treatment of Software Payments

On September 4, 2026, the Australian Taxation Office finalized Taxation Ruling TR 2026/2, which treats many cross-border payments under software distribution arrangements as royalties subject

[40] eSafety Commissioner, Social Media Minimum Age Compliance Update (Mar. 2026), https://www.esafety.gov.au/sites/default/files/2026-03/SocialMediaMinimumAgeComplianceUpdateMarch2026.pdf

[41] eSafety Commissioner, Frequently asked questions about access to online porn and other adult content, https://esafety.gov.au/industry/codes/faq-access-to-online-porn-and-other-adult-content

[42] Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts, Exposure Draft, Online Safety Amendment (Digital Duty of Care) Bill 2026 (Sept. 2026), https://www.infrastructure.gov.au/sites/default/files/documents/exposure-draft-online-safety-amendment-digital-duty-of-care-bill-2026-september2026.pdf

[43] Attorney-General's Department, Privacy Reform, Consultation on Exposure Draft legislation (Aug. 31, 2026), https://consultations.ag.gov.au/rights-and-protections/privacy-reform/

[44] PPC Land, Australia would force ad tech to get consent before sharing pixels (Sept. 2026), https://ppc.land/australia-would-force-ad-tech-to-get-consent-before-sharing-pixels/

to withholding tax, including where the arrangement involves download or cloud access, and which applies to periods both before and after its issue.[45] The ruling departs from the OECD Model Tax Convention commentary, under which payments by distributors that acquire copies of software for resale are generally not royalties, and it raises costs and uncertainty for U.S. software developers that sell through Australian distributors and resellers. We ask USTR to include this ruling in the 2027 NTE report and to urge Australia to align its treatment of software payments with the OECD approach.

Issue: Scams Prevention Framework

Australia's Scams Prevention Framework designates digital platforms, alongside banks and telecommunications providers, as regulated sectors, with ACCC as the digital platforms sector regulator. Regulated entities had to join the Australian Financial Complaints Authority scheme by September 1, 2026, and most obligations apply from March 31, 2027, while sector codes and rules are still being developed.[46] ACT shares the goal of reducing scams,[47] and we ask USTR to encourage Australia to develop the digital platform codes and rules in a way that is proportionate, technology-neutral, and workable for the small businesses that build on these platforms.

AUSTRIA

Issue: Digital Services Taxation

Austria has implemented a DST that imposes a 5 percent tax on the advertising revenues of U.S. digital companies.[48] For reasons discussed above, ACT is significantly concerned with the imposition of DSTs in this key market and calls for USTR support in opposing it.

BANGLADESH

Issue: Data Protection and Data Localization

In April 2026, Bangladesh enacted the Personal Data Protection Act, 2026, the National Data Management Act, 2026, and the Cyber Security Act, 2026, which followed ordinances approved by the interim government in late 2025.[49] ACT is concerned that these laws and their implementing rules could require certain data to be stored in Bangladesh, condition transfers abroad on government

[45] Australian Taxation Office, Taxation Ruling TR 2026/2, Income tax: royalties - character of payments in respect of software and intellectual property rights (Sept. 4, 2026), https://www.ato.gov.au/law/view/view.htm?docid=TXR/TR20262/NAT/ATO/00001

[46] Australian Competition and Consumer Commission, Scams Prevention Framework, https://www.accc.gov.au/about-us/scams-prevention-framework

[47] ACT, Comments on the Scams Prevention Framework Draft Legislation (Oct. 4, 2024), https://actonline.org/post/comments-of-act-the-app-association-scams-prevention-framework-draft-legislation/.

[48] Tax Foundation, Digital Services Taxes in Europe, 2026 (May 4, 2026), https://taxfoundation.org/data/all/eu/digital-services-taxes-europe/

[49] Information and Communication Technology Division, Government of Bangladesh, Laws (accessed Oct. 19, 2026), https://ictd.gov.bd/pages/laws; Prothom Alo (BSS report on advisory council approval of the Personal Data Protection Ordinance-2025) (Oct. 9, 2025), https://en.prothomalo.com/bangladesh/ovdfi8qd4b.

approval, and impose criminal liability for compliance failures. Requirements of this kind would raise costs for U.S. small business technology developers that rely on cloud services hosted outside Bangladesh to serve customers there and would deter market entry. We urge USTR to review the enacted laws, to press Bangladesh to allow personal data to move across borders under interoperable safeguards, and to include any localization requirements in the 2027 NTE report.

BELGIUM

Issue: Digital Services Taxation

Belgium's government has pledged to introduce a 3 percent DST by 2027 absent a global or European agreement,[50] and a bill introduced in the Chamber of Representatives in 2026 would apply a 3 percent DST to groups with worldwide revenue above €750 million and Belgian revenue above €3 million from January 1, 2027.[51] For reasons discussed above, ACT is significantly concerned with the imposition of DSTs in this key market, and calls for USTR support in opposing it.

BRAZIL

Issue: Section 301 Investigation

On July 15, 2025, USTR initiated an investigation under Section 301 of the Trade Act of 1974 into Brazil's practices on digital trade and electronic payment services, intellectual property protection, and other issues, and ACT submitted comments in the investigation.[52] On June 1, 2026, USTR determined that certain of these practices are unreasonable or discriminatory and burden U.S. commerce, citing secret court orders that require U.S. platforms to remove content and suspend accounts, the preferential treatment of the central bank's Pix payment system, and weak enforcement against counterfeiting and online piracy.[53] On July 15, 2026, the President directed USTR to impose a 25 percent tariff on goods of Brazil, with certain exemptions.[54] USTR expressly made no findings on the Supreme Federal Court's Article 19 decision or on Brazil's restrictions on transfers of personal data. ACT urges USTR to use its ongoing engagement with Brazil to address these issues and the other barriers to U.S. small business technology developers described in this section.

---

[50] Tax Foundation, Digital Services Taxes in Europe, 2026 (May 4, 2026), https://taxfoundation.org/data/all/eu/digital-services-taxes-europe/

[51] Chamber of Representatives of Belgium, Bill amending the Code of Miscellaneous Duties and Taxes to introduce a digital services tax, DOC 56 1491/001 (Mar. 30, 2026), https://www.lachambre.be/FLWB/PDF/56/1491/56K1491001.pdf

[52] ACT, Comments on the Initiation of Section 301 Investigation: Brazil's Acts, Policies, and Practices Related to Digital Trade and Electronic Payment Services, Docket No. USTR-2025-0043 (Aug. 18, 2025), https://actonline.org/post/comments-of-act-the-app-association-initiation-of-section-301-investigation-brazils-acts-policies-and-practices-related-to-digital-trade-and-electronic-payment-services-unfair-prefere/.

[53] Office of the U.S. Trade Representative, Notice of Determination and Request for Comments Concerning Action Pursuant to Section 301: Brazil's Acts, Policies, and Practices (June 4, 2026), https://public-inspection.federalregister.gov/2026-11158.pdf

[54] Memorandum on Action Under Section 301 Concerning Brazil's Acts, Policies, and Practices, 91 Fed. Reg. (July 20, 2026), https://www.govinfo.gov/content/pkg/FR-2026-07-20/html/2026-14654.htm

Issue: Brazilian General Data Protection Law

The National Congress of Brazil passed the Lei Geral de Proteção de Dados Pessoais (LGPD)[55] in July of 2018, and it was signed into law on August 14, 2018. The LGPD entered into force in September 2020, and its provisions allowing for penalties and sanctions to be imposed took effect on August 1, 2021.[56] Various provisions of the LGPD, much like the EU's General Data Protection Regulation, impose additional requirements on non-Brazilian firms (due to its extraterritorial reach) that increase the cost and risk associated with handling data pertaining to Brazilian citizens. Furthermore, Articles 33-36 do not permit cross-border data transfers based on the controller's legitimate interest. In August 2024, Brazil's National Data Protection Authority (ANPD) adopted Resolution CD/ANPD No. 19/2024, which governs international transfers and requires companies relying on contractual clauses to adopt the ANPD's standard contractual clauses without changes within 12 months.[57] In January 2026, Brazil and the European Union adopted mutual adequacy decisions, but Brazil has not recognized the United States as an adequate destination, and ACT urges USTR to advocate for the United States' recognition as an adequate destination.[58] Such provisions can be an insurmountable hurdle to our small business members seeking to enter the Brazilian market. Anything that can be done throughout the LGPD's implementation process to ease the burden for small and medium-sized companies could have tremendously positive economic implications.

More recently, Brazil's Congress introduced Bill No. 4097/2023, which seeks to impose new "digital sovereignty" measures within the LGPD. This bill would require IT companies operating in Brazil to have a significant level of Brazilian ownership and control—such as at least 25 percent of voting shares held by Brazilian nationals, incorporation under Brazilian law, or headquarters in Brazil. In May 2026, the bill was sent to the Senate's Science, Technology, Innovation, Communication and Informatics Committee for a final committee decision, where it awaits the designation of a rapporteur.[59]

Issue: Proposed Intervention into Competitive Digital Markets

ACT remains concerned with the introduction of PL 2768/2022 in the Brazilian House of Representatives, which would designate certain digital platforms as "essential access control power holders" and intervene into their operations, oblige the payment of an inspection fee amounting to 2 percent of their annual gross operating revenue, and empower Brazil's National Telecommunications Agency (ANATEL) to sanction platforms with a fine of up to 2 percent of the national revenue and suspend certain business activities. The Chamber's Economic Development

[55] Chris Brook, Breaking Down LGPD, Brazil's New Data Protection Law, DATAINSIDER, June 10, 2019, available at https://digitalguardian.com/blog/breaking-down-lgpd-brazils-new-data-protection-law#targetText=What%20is%20the%20LGPD%3F,scheduled%20date%20of%20February%202020.
[56] International Association of Privacy Professionals, In Rapid-Fire Reversal, Brazil Effectuates Privacy Law Immediately (Aug. 2020), https://iapp.org/news/a/in-rapid-fire-reversal-brazil-effectuates-privacy-law-immediately/.
[57] Autoridade Nacional de Proteção de Dados, Resolução CD/ANPD nº 19, de 23 de agosto de 2024 (Aug. 23, 2024), https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-19-de-23-de-agosto-de-2024.
[58] eucrim, EU and Brazil Mutually Recognise Data Protection Standards (2026), https://eucrim.eu/news/eu-and-brazil-mutually-recognise-data-protection-standards/
[59] Congresso Nacional, Projeto de Lei nº 4097/2023 (status as of Oct. 2026), https://www.congressonacional.leg.br/materias/materias-bicamerais/-/ver/pl-4097-2023

Committee approved a substitute text of the bill on July 1, 2026, and it now awaits an opinion in the Communications Committee.[60] ACT is also concerned about the development of a report on digital markets by Brazil's Department of Economic Studies (DEE) of the Administrative Council for Economic Defense (CADE) intended to substantiate the Brazilian government's competition-themed intervention into digital markets. Brazilian government intervention into the digital economy would jeopardize the functionality of mobile operating systems and software distribution platforms that have enabled countless American small businesses to grow.

The Brazilian government later released its Digital Platform Report. ACT has urged that Brazilian government's next steps be taken only after carefully considering the impact of proposed interventions into nascent and evolving markets that support small business growth and job creation in Brazil.[61] Any Brazilian government interventions into digital platform markets should be based on demonstrated risks to competition and consumers and avoid disrupting the competitive dynamics of the app economy. ACT notes its support for the report's recommendation that CADE, the government's primary competition agency, is best suited to lead the Brazilian government's work in overseeing digital platforms using Brazil's existing laws. As the Brazilian government continues to assess digital platform competition and next steps, ACT will work closely with local policymakers to ensure the perspective of small business technology developers is at the forefront of the decision-making process.

In September 2025, the Brazilian government introduced new digital platform legislation, Bill 4.675/2025. The bill aims to regulate large digital platforms by introducing ex ante rules similar to the European Digital Markets Act. The bill proposes creating a distinct Digital Markets Superintendency within CADE to enforce special obligations on companies deemed to have "systemic relevance" in digital markets, based on criteria like market power and data control. Key features include mandatory interoperability, prohibitions on self-preferencing, algorithmic transparency, and data portability, with sanctions of up to 20 percent of Brazilian turnover for non-compliance. These regulations will affect a select group of no more than 10 companies, targeting those already designated as "gatekeepers" under the EU's DMA framework - predominantly American technology companies. The proposal's structure will create an uneven playing field, where other foreign and domestic competitors will not need to be subject to the same rules, uncertainty or potential fines. The Chamber of Deputies approved urgency for the bill on March 18, 2026, which allows it to go directly to a floor vote, and the rapporteur's July 2026 draft keeps the designation and special obligations regime while adjusting the designation criteria and procedures.[62] As of October 2026, the bill is ready for a floor vote, and committees have approved requests for further public hearings on

[60] Congresso Nacional, Projeto de Lei nº 2768/2022 (status as of Oct. 2026), https://www.congressonacional.leg.br/materias/materias-bicamerais/-/ver/pl-2768-2022

[61] ACT, Letter to Minister of Finance Fernando Haddad re Digital Platform Legislation in Brazil (July 30, 2025), https://actonline.org/post/act-the-app-association-letter-to-minister-of-finance-fernando-haddad-re-digital-platform-legislation-in-brazil-english-and-portuguese-versions/; ACT, Comments to Public Consultation on Digital Platforms to Brazil's Ministry of Finance (Mar. 18, 2024), https://actonline.org/post/act-comments-to-public-consultation-on-digital-platforms-to-brazils-ministry-of-finance/.

[62] Teletime, PL dos mercados digitais: relator apresenta minuta (July 2, 2026), https://teletime.com.br/02/07/2026/pl-dos-mercados-digitais-relator/

its economic impact.[63] ACT has written to Brazilian lawmakers opposing the bill, and we ask USTR to continue urging Brazil not to adopt it.

Issue: OTT Regulatory Requirements

ACT is concerned with the launch of a public consultation by ANATEL proposing mandates for financial contributions by OTTs (termed "value added services") for the improvement, expansion, and maintenance of the network infrastructure and a related push to establish ANATEL as a regulator for the digital economy in Brazil. On March 27, 2026, ANATEL opened a further call for input (Tomada de Subsídios No. 1/2026) on the obligations of large network users, including digital platforms, which asks about traffic growth, content delivery networks and where their infrastructure is located, and local traffic exchange.[64] The expansion of network infrastructure support fees to OTTs would imperil countless network edge technology innovators' efforts to grow and create new jobs and contradicts well-established U.S. policy on universal service contribution base expansion.

Issue: Intellectual Property Rights (IPR) and Standards

Brazil has begun presenting IPR and competition challenges for ACT members. The country is seeing an influx of SEP disputes, in which injunctions are being rapidly awarded without serious competition consideration. This trend of injunctive relief is in part because Brazilian IP law does not require previous licensing negotiations or notice prior to seeking an injunction. While preliminary injunctions in Brazil are assessed based on the impact on the defendant's business and public interest as mandated by Article 300(3) of the Civil Procedure Code, final injunctions are issued almost automatically upon a finding of infringement. This places SEP holders in a unique position to control who can use a standard by virtue of their patent's necessity.

We expect Brazil's jurisprudence to have a significant impact on the global SEP licensing landscape. We encourage USTR to work with Brazil to improve its approach to SEPs, including by limiting injunctions on FRAND-committed SEPs to rare circumstances.

Issue: Discriminatory Localization Policies

Brazil has made changes to its tax laws with respect to information and communications technology (ICT) and digital goods in response to findings that the laws were in violation of World Trade Organization (WTO) rules, but Brazil's Basic Production Process law continues to inappropriately favor "local content" production of these categories.

Further, recent amendments to Institutional Security Group (GSI) policies require the localization of certain types of government data. The GSI, led by the military, issued a Normative Instruction outlining new rules for federal cloud service contracts, mandating that data and metadata be stored exclusively within Brazil in certain cases. These requirements disadvantage foreign digital service

[63] Congresso Nacional, Projeto de Lei nº 4675/2025 (status as of Oct. 2026), https://www.congressonacional.leg.br/materias/materias-bicamerais/-/ver/pl-4675-2025

[64] Teletime, Anatel abre tomada de subsídios para regras entre teles e big techs (Mar. 30, 2026), https://teletime.com.br/30/03/2026/anatel-abre-tomada-de-subsidios-sobre-regulamento-de-grandes-usuarios/

providers that lack local data storage capabilities, setting a concerning precedent for broader data localization mandates.

Meanwhile, the Department of Innovation within the Ministry of Development, Industry, and Trade (MDIC) is exploring legislative proposals modeled after the European Union's Data Act, aimed at regulating the "data economy." While no formal proposal has been released, discussions continue on how Brazil should implement a similar framework. There is concern that such regulations could impose discriminatory obligations on U.S. companies, particularly through targeted thresholds.

Brazil also maintains various data localization barriers, largely in response to the limited competitiveness of its domestic tech sector. It offers tax incentives for locally produced information and communication technology (ICT) goods and equipment (under the Basic Production Process – PPB, Law 8387/91, Law 8248/91, and Ordinance 87/2013) and prioritizes local ICT hardware and software providers in government procurement (per 2014 Decrees 8184, 8185, 8186, 8194, and 2013 Decree 7903). Additionally, Brazil does not recognize conformity assessments conducted outside the country for telecommunications equipment (per ANATEL's Resolution 323).

Issue: Artificial Intelligence

Brazil's Congress is rapidly advancing AI regulation that diverges sharply from the U.S.-led risk-based approach and could undermine the global competitiveness of American technology firms. Bill 2338/2023, approved by the Senate in December 2024 and pending before a Special Committee of the Chamber of Deputies,[65] has faced widespread opposition from civil society, businesses, and academia, who warn it could harm Brazil's economy, stifle innovation, and disrupt international interoperability. The committee rapporteur's report has been delayed repeatedly and may be addressed in the immediate aftermath of Brazil's October 2026 elections. The bill would impose significant restrictions on U.S. AI developers and businesses deploying AI-driven solutions, limiting their ability to export tools and services to Brazil—dealing a major setback to leading U.S. innovators competing against Chinese tech firms. Of particular concern, the bill takes a broad, indiscriminate approach to AI regulation, failing to focus on high-risk applications and instead encompassing even low-risk, routine business functions. Additionally, it lacks clear distinctions between AI system developers and deployers, creating regulatory uncertainty that could severely hinder companies of all sizes from advancing AI innovation. The Senate-approved text would also require AI developers to pay copyright holders for content used to train AI models, including content used before the law takes effect, which could block U.S. companies from conducting AI training in Brazil.[66]

Issue: Digital Services Tax

ACT is a strong supporter of the several multilateral efforts to keep digital services taxes (DSTs) out of the international taxation system. Despite these efforts, the Brazilian Congress has introduced a number of bills seeking to create a DST that would impact any U.S. company that does business in Brazil. Several such bills are currently under consideration, including Complementary Bill 157/2025,

[65] Senado Federal, Projeto de Lei nº 2338/2023 (status as of Oct. 2026), https://www25.senado.leg.br/web/atividade/materias/-/materia/157233

[66] Jornal de Brasília, Lei de IA avança no Senado com previsão de remuneração de direitos autorais (Dec. 5, 2024), https://jornaldebrasilia.com.br/noticias/brasil/lei-de-ia-avanca-no-senado-com-previsao-de-remuneracao-de-direitos-autorais/

introduced in July 2025, which would create a 7 percent "Digital Social Contribution" on advertising and data sales by companies with revenue above R$500 million,[67] and President Lula has expressed support for their goal of "charging taxes from U.S. digital service providers." If the policy envisioned by these bills—an additional tax exclusively on the revenue of multinational companies—becomes law, the burden will fall heavily on American companies and may force small businesses to withdraw from the country's marketplace.

Issue: Intermediary Liability and Online Content Rules

On June 26, 2025, Brazil's Supreme Federal Court (STF) partly struck down Article 19 of the Marco Civil da Internet, which had shielded online services from liability for third-party content unless they ignored a court order to remove it. Until Congress adopts new legislation, services can now be held liable for many types of third-party content if they fail to remove it after receiving a notice, for content involving certain serious offenses if they do not act immediately, and, without any notice, for illegal paid advertising and boosted content unless they show they acted promptly to stop its circulation.[68] Motions for clarification filed by affected companies were scheduled for review by the STF in June 2026.[69] This regime pushes app developers, marketplaces, and other online services toward over-removal and creates liability risks that fall hardest on small firms without large content moderation teams. Separately, the Digital Statute of Children and Adolescents (Law 15.211/2025, known as the "ECA Digital") took effect on March 17, 2026, with the ANPD as its enforcement authority, and applies age verification, parental supervision, and design obligations to any digital product or service likely to be accessed by minors in Brazil, wherever it is developed.[70] ACT asks USTR to urge Brazil to restore legal certainty for online intermediaries and to implement the ECA Digital through interoperable, risk-based rules developed with stakeholder input.[71]

CAMBODIA

Issue: National Internet Gateway

In February 2021, Cambodia adopted a sub-decree establishing a National Internet Gateway that would route all domestic and international internet traffic through government-appointed operators and authorize the blocking and disconnection of network connections on broad and undefined

[67] Teletime, Boulos quer taxar big techs para financiar infraestrutura e transferência de renda (July 23, 2025), https://teletime.com.br/23/07/2025/boulos-quer-taxar-big-techs-para-financiar-infraestrutura-e-transferencia-de-renda/

[68] Teletime, Art. 19: STF concilia votos e plataformas terão responsabilização parcial (June 26, 2025), https://teletime.com.br/26/06/2025/art-19-stf-concilia-votos-e-plataformas-terao-responsabilizacao-parcial/

[69] Supremo Tribunal Federal, STF vai analisar recursos contra tese fixada no julgamento do Marco Civil da Internet (June 9, 2026), https://noticias.stf.jus.br/postsnoticias/stf-vai-analisar-recursos-contra-tese-fixada-no-julgamento-do-marco-civil-da-internet/

[70] Teletime, Lei que torna ANPD agência e fixa vigência do ECA Digital é sancionada (Feb. 26, 2026), https://teletime.com.br/26/02/2026/lei-que-torna-anpd-agencia-e-fixa-vigencia-do-eca-digital-e-sancionada/

[71] ACT, Comments on the Draft Guia Orientativo "Providers of Information Technology Products or Services: Scope and General Obligations under the ECA Digital" (June 15, 2026), https://actonline.org/post/act-comments-on-the-draft-guia-orientativo-providers-of-information-technology-products-or-services-scope-and-general-obligations-under-the-eca-digital/.

grounds.[72] The government delayed implementation in February 2022 but did not withdraw the sub-decree.[73] The gateway would give the government broad power to monitor and block online services and would raise costs and security risks for U.S. small businesses that serve Cambodian users. In the U.S.-Cambodia Agreement on Reciprocal Trade signed on October 26, 2025, Cambodia committed to refrain from measures that discriminate against U.S. digital services, to ensure the free transfer of data across trusted borders, and not to impose digital services taxes or customs duties on electronic transmissions.[74] We urge USTR to ensure that Cambodia implements these commitments and repeals the National Internet Gateway sub-decree.

CANADA

Issue: Digital Service Taxes

The Canadian government's previous positioning with respect to DSTs, including its opposition to the OECD/G20 Inclusive Framework on Base Erosion and Profit Shifting's agreement extending a moratorium on imposing DSTs, was a matter of concern. ACT has consistently made clear that a Canadian DST would negatively impact Canada's and the United States' most innovative markets, including software development and IoT connected devices, in which ACT members lead.

On June 29, 2025, Canada announced it would rescind its DST before its first collection. The DST was initially adopted in June of 2024, which would impose a three percent tax on online services, primarily targeting U.S firms and retroactively costing them an estimated US$3 billion in 2025.[75] The Budget 2025 Implementation Act, No. 1, which received Royal Assent on March 26, 2026, repealed the Digital Services Tax Act retroactive to June 20, 2024, and allows the government to refund DST payments with interest.[76] ACT welcomes the repeal, which removes a significant source of uncertainty for small business innovators, and asks USTR to confirm that all amounts paid by U.S. companies in anticipation of the tax are refunded promptly and to secure a commitment through the USMCA joint review that Canada will not adopt a DST or similar measure in the future.

Issue: Data Protection and Localization Requirements

The Province of Québec's privacy legislation, Bill 64 (the Act to Modernize Legislative Provisions as Regards the Protection of Personal Information), adopted in 2021 followed by phased in enforcement, significantly restricts cross-border data transfers and introduces compliance burdens

[72] Human Rights Watch, Cambodia: Internet Censorship, Control Expanded (Feb. 18, 2021), https://www.hrw.org/news/2021/02/18/cambodia-internet-censorship-control-expanded
[73] Internet Society, Internet Impact Brief: Cambodia National Internet Gateway (Feb. 18, 2022), https://www.internetsociety.org/resources/2022/internet-impact-brief-cambodia-national-internet-gateway/
[74] Agreement Between the United States of America and the Kingdom of Cambodia on Reciprocal Trade, arts. 3.1, 3.2, 3.5 (Oct. 26, 2025), https://www.whitehouse.gov/briefings-statements/2025/10/agreement-between-the-united-states-of-america-and-the-kingdom-of-camboida-on-recipricol-trade/
[75] https://www.congress.gov/crs-product/IN12399
[76] Parliament of Canada, Bill C-15, Budget 2025 Implementation Act, No. 1 (Royal Assent Mar. 26, 2026), https://www.parl.ca/legisinfo/en/bill/45-1/c-15; Library of Parliament, Legislative Summary of Bill C-15 (2026), https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/LegislativeSummaries/451C15E

that are disproportionate for small firms.[77] The U.S. International Trade Commission identified the law as a barrier to digital trade in its Year in Trade 2021 report.[78] The law's prescriptive consent and localization requirements create operational uncertainty for U.S. technology providers and threaten the integrity of the integrated U.S.–Canada digital marketplace.

At the federal level, Bill C-27 died when Parliament was prorogued in January 2025, and on June 15, 2026, the Canadian government introduced Bill C-36, which would enact the Protecting Privacy and Consumer Data Act, replace Part 1 of the Personal Information Protection and Electronic Documents Act, and create a new Digital Safety and Data Protection Commission of Canada.[79] The bill would require organizations to complete a privacy impact assessment and adopt risk mitigation measures before transferring personal information outside Canada, treat all personal information of individuals under 18 as sensitive, and add new disclosure and explanation obligations for automated decision systems.[80] The government's renewed focus on "digital sovereignty" could introduce additional restrictions on cross-border data flows and data storage. Such provisions increase compliance costs and legal uncertainty for U.S. companies, impede innovation in emerging fields such as artificial intelligence, and risk fragmenting a market long defined by interoperability. ACT urges USTR to engage proactively with the Canadian government to advocate for a privacy framework that aligns with global standards and supports a fair and open digital marketplace. Key areas requiring clarification include transfer rules that do not single out cross-border data flows, refining consent exceptions, explicitly recognizing advertising and marketing as legitimate business activities, and confirming a 2-3-year implementation timeline.

Additionally, in August 2025, Shared Services Canada (SSC) issued a request for information to guide the development of a sovereign procurement regime for Infrastructure-as-a-Service and Platform-as-a-Service offerings.[81] This proposal would require that all government data be processed and stored within Canada and that providers—including parent companies—be free from any foreign legal obligations permitting external governmental access to data. SSC has since said the sovereign stream will be tied to the government's Buy Canadian Policy framework, open only to small and medium-sized businesses that show neither they nor their parent companies are subject to foreign orders compelling access, and launched through draft solicitations planned for 2026.[82] Invoking a "national security exception" to justify these restrictions, the proposal would effectively exclude U.S. cloud providers based on ownership rather than objective security criteria. Such an approach risks violating Canada's trade commitments and unfairly discriminates against U.S. suppliers by limiting their ability to compete in public-sector procurement. ACT urges USTR to treat Canada's proposed localization and procurement policies as discriminatory trade barriers warranting continued monitoring and engagement in the 2027 NTE.

[77] https://www.assnat.qc.ca/en/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html
[78] https://www.usitc.gov/publications/332/pub5349.pdf
[79] Parliament of Canada, Bill C-36, An Act to enact the Protecting Privacy and Consumer Data Act (first reading June 15, 2026), https://www.parl.ca/legisinfo/en/bill/45-1/c-36
[80] House of Commons of Canada, Bill C-36, First Reading (2026), https://www.parl.ca/DocumentViewer/en/45-1/bill/C-36/first-reading
[81] https://canadabuys.canada.ca/sites/default/files/webform/tender_notice/71894/rfi-dr-wave-1---vague-1---sovereign-cloud-supplier-webinar---august-22-2025_0.pdf
[82] Shared Services Canada, Request for Information, Sovereign Public Cloud Capability (CS-IAAS-2025), CanadaBuys, https://canadabuys.canada.ca/en/tender-opportunities/tender-notice/cb-416-17296820

Issue: Intellectual Property Rights Enforcement

ACT remains concerned with Canada's approach to intellectual property rights enforcement. The Canadian government's notice and notice requirement under Canada's Copyright Act is an ineffective step to ensure that internet services providers (ISPs) take reasonable steps to prevent piracy on their platforms. This process does not prevent infringers from engaging in illicit acts, such as the common IPR violations provided above that affect ACT members. Stronger enforcement mechanisms, such as a notice-and-takedown procedures provided by the U.S. Digital Millennium Copyright Act (DMCA) are more effective steps that should be encouraged to the Canadian government to protect businesses, including ACT members, that interact with their economy.

Issue: Artificial Intelligence Regulation

In June 2022, the Canadian government introduced the Artificial Intelligence and Data Act (AIDA) as part of Bill C-27, the Digital Charter Implementation Act, 2022. AIDA would have granted the government broad authority to regulate "high-impact" AI systems, but its overly vague definitions risked encompassing low-risk applications, posing significant challenges for U.S. companies and the U.S.-led risk-based approach to AI governance. The bill also included steep penalties—up to 3 percent of global revenue— and introduced an unprecedented criminal enforcement provision for non-compliance. This regulatory framework would have imposed a heavy compliance burden on leading U.S. AI researchers and developers while undermining interoperability across North America. AIDA faced significant criticism from stakeholders for its ambiguous language, lack of proper consultation, and misalignment with global AI standards, and it died with Bill C-27 when Parliament was prorogued in January 2025. Canada's national AI strategy now contemplates new legislation over the next five years, and from July to September 2026 the government consulted on AI transparency measures covering AI-generated content, disclosure of AI interactions, information about AI systems, incident tracking, and AI agents.[83] ACT responded to the consultation, urging a risk-based approach that relies on existing law, and asks USTR to encourage Canada not to revive AIDA's approach in any future AI or transparency legislation.

Issue: Lawful Access and Encryption

Bill C-22, the Lawful Access Act, 2026, passed the House of Commons on June 18, 2026, and is at second reading in the Senate.[84] Part 2 of the bill would enact the Supporting Authorized Access to Information Act, under which the government could require electronic service providers, a term that on its face includes foreign providers serving persons in Canada, to develop and maintain technical capabilities to support lawful access and to retain certain metadata for up to six months, and could impose these duties through ministerial orders whose existence and contents providers may not disclose.[85] Although the bill exempts providers from requirements that would introduce a systemic vulnerability, the breadth of the capability obligations and the secrecy of ministerial orders leave

[83] Innovation, Science and Economic Development Canada, Have Your Say: Advancing AI Transparency in Canada (July 23 to Sept. 23, 2026), https://ised-isde.canada.ca/site/ised/en/have-your-say-advancing-ai-transparency-canada

[84] Parliament of Canada, Bill C-22, Lawful Access Act, 2026 (status as of Oct. 8, 2026), https://www.parl.ca/legisinfo/en/bill/45-1/c-22

[85] House of Commons of Canada, Bill C-22, Third Reading (June 18, 2026), https://www.parl.ca/DocumentViewer/en/45-1/bill/C-22/third-reading

developers of encrypted messaging, cloud, and connected device services uncertain about whether they may be pressed to weaken the security of their products. ACT urges USTR to encourage Canada to confirm that no provider will be required to weaken encryption or build access mechanisms into its products.[86]

Issue: Online Streaming Act Contributions

Under the Online Streaming Act, the Canadian Radio-television and Telecommunications Commission (CRTC) in June 2024 required online streaming services not affiliated with a Canadian broadcaster and earning more than C$25 million in annual Canadian broadcasting revenues to contribute 5 percent of those revenues to Canadian content funds.[87] In May 2026, the CRTC raised the total Canadian programming expenditure requirement for these services to 15 percent of revenues.[88] On June 3, 2026, the government announced it would direct the CRTC to reverse that increase, remove the requirement to contribute to individual funds, and set a lower rate.[89] These obligations operate as a discriminatory levy on digital services that falls mainly on U.S. companies, which have limited access to the funds they finance. ACT asks USTR to ensure that the announced reversal is implemented in full and that the remaining discriminatory elements of the framework are removed.

Issue: Online Safety Legislation

On June 10, 2026, the Canadian government introduced Bill C-34, the Safe Social Media Act, which would enact a Digital Safety Act and create a Digital Safety Commission of Canada with the stated aim of making social media services and AI chatbots safer for children.[90] Earlier proposals in this area included 24-hour takedown duties, broad regulator powers, and penalties based on global revenue. ACT asks USTR to monitor the bill and encourage Canada to adopt proportionate, risk-based obligations that do not require scanning of encrypted communications or Canada-specific age assurance systems that are costly for small developers.

Issue: Online News Act

Canada's Online News Act, which received Royal Assent in June 2023, requires designated digital news intermediaries to bargain with and pay Canadian news businesses for news content. Since the Act took effect, one U.S. company has paid C$100 million per year, indexed to inflation, to a collective of Canadian news businesses in exchange for a five-year exemption from the Act's bargaining and arbitration provisions, while another U.S. company stopped making news available on its platforms in Canada, and in 2026 a group of broadcasters asked the CRTC to compel that

[86] ACT, Letter to the Canadian Parliament re Bill C-22, An Act Respecting Lawful Access (June 3, 2026), https://actonline.org/post/act-letter-re-bill-c-22-4-jun-2026/.
[87] CRTC, Broadcasting Regulatory Policy CRTC 2024-121 (June 4, 2024), https://crtc.gc.ca/eng/archive/2024/2024-121.htm
[88] CRTC, Broadcasting Regulatory Policy CRTC 2026-96 (May 21, 2026), https://crtc.gc.ca/eng/archive/2026/2026-96.htm
[89] Global News, Ottawa to Direct CRTC to Reverse Streaming Contribution Increase (June 3, 2026), https://globalnews.ca/news/11888757/crtc-online-streaming-act-rules-ottawa-review/
[90] Parliament of Canada, Bill C-34, Safe Social Media Act (first reading June 10, 2026), https://www.parl.ca/legisinfo/en/bill/45-1/c-34

company to bargain.[91] The Act functions as a discriminatory levy on a small number of U.S. firms and is in tension with Canada's national treatment and digital products obligations under the USMCA. We urge USTR to seek its repeal through the USMCA joint review.

CHILE

Issue: Cybersecurity Incident Reporting

Chile's Framework Law on Cybersecurity (Law No. 21.663), in force since March 2025, requires essential service providers and operators of vital importance to send an early alert to the National Cybersecurity Agency within three hours of becoming aware of a significant cybersecurity incident.[92] This deadline is far shorter than the 72-hour period common in other frameworks, and it raises compliance costs for the U.S. cloud and software providers that serve regulated Chilean customers and for the small developers that build on them. We urge USTR to encourage Chile to align its reporting timelines with international practice.

CHINA

Issue: China's Encryption Law

On May 11, 2020, China issued the Commercial Encryption Product Certification Catalogue and the Commercial Encryption Certification Measures. Manufacturers of products listed in the catalogue will not be subject to mandatory approval requirements before launching products into the market. The certification is voluntary, but its goal is to serve as an assurance to customers that the commercial encryption products conform to Chinese standards. However, China's amended Regulations on the Administration of Commercial Cryptography, which took effect on July 1, 2023, require testing and certification before certain commercial cryptography products can be sold, set out import licensing and export control lists, and require critical information infrastructure operators to pass a commercial cryptography application security assessment before operation and at least once a year after that.[93] These requirements risk making certification mandatory in practice and make it harder for ACT members to get their products to customers in China. The certifications remain valid for a five-year period but are subject to further review if the product or entity producing the product undergoes any changes.

On October 26, 2019, China enacted an Encryption Law, which took effect on January 1, 2020. The new encryption law greatly impacts the regulatory landscape for foreign-made commercial encryption products, leaving unanswered questions. For example, the import licensing and export control framework provides an exemption for "commercial encryption" used in "products for consumption by the general population." However, because the law does not sufficiently define either of these terms, businesses are left to speculate on how to apply the law. As a result, app

[91] Canadian Heritage, Question Period Note: Implementing the Online News Act (Apr. 16, 2026), https://search.open.canada.ca/qpnotes/record/pch%2CPCH-2026-QP-00002

[92] Ley No. 21.663, Ley Marco de Ciberseguridad, art. 9, https://www.bcn.cl/leychile/navegar?idNorma=1202434.

[93] State Council of the People's Republic of China, Regulations on the Administration of Commercial Cryptography (State Council Decree No. 760) (Apr. 27, 2023, effective July 1, 2023), https://www.mee.gov.cn/zcwj/gwywj/202305/t20230529_1031579.shtml.

developers experience legal uncertainty, and ACT members will suffer due to their inability to maintain customers' trust regarding the security of their information. Furthermore, the lack of clear regulations will also impede American businesses' ability to succeed in China's large consumer market.

Issue: China's Cybersecurity Law

China's Cybersecurity Law, which was amended effective January 1, 2026, to raise penalties and add provisions on artificial intelligence,[94] imposes tough regulations, introduces serious uncertainties, and unreasonably prevents market access for American companies seeking to do business in China. This law is particularly difficult for ACT's small business members seeking access to digital markets and consumers in China. The law includes onerous data localization requirements and uses overly vague language when outlining important provisions (such as when Chinese law enforcement bodies can access a business's data or servers or how frequently a business must perform demanding safety assessments). Legal certainty is vital to app developers' operations and their ability to maintain their customers' trust in the protection of their data. In addition to creating obligations that are often infeasible for our members, the Cybersecurity Law's vague language leaves businesses without clear guidelines about how the law will be applied and jeopardizes American businesses' potential to succeed in China's important market.

The law requires Critical Information Infrastructure operators to predict the potential national security risks that are associated with their products and services. It includes restrictive review requirements and will most likely cause supply disruptions. Important clarifications are needed to allow for American businesses to succeed in the Chinese market, including how to balance new requirements for data encryption to protect Chinese consumers' privacy while allowing on demand access to the Chinese government.[95] ACT continues to oppose data localization requirements and China's use of overly prescriptive and technically or economically infeasible mandates to address public safety goals.

Our comments also addressed concerns related to the vague definition of "network operator," as the "owner of the network, network managers and service providers." This definition can be interpreted to include app developers, even though most small business innovators operate on larger platforms or networks they do not manage. Including small app developers and software companies within this broad definition forces them to abide by cybersecurity responsibilities that do not apply to them. We separately contributed comments[96] on the Cyberspace Administration of China's implementation of the Cybersecurity Law's restrictive policies on data transfers outside of Chinese borders.

[94] China Daily, China approves amendment to cybersecurity law, highlighting safe AI development (Oct. 29, 2025), https://subsites.chinadaily.com.cn/npc/2025-10/29/c_1136116.htm

[95] Lorand Laskai & Adam Segal, The Encryption Debate in China: 2021 Update, CARNEGIE ENDOWMENT INT'L PEACE, Mar. 31, 2021, available at https://carnegieendowment.org/2021/03/31/encryption-debate-in-china-2021-update-pub-84218.

[96] See http://actonline.org/wp-content/uploads/ACT-Comments-re-China-Data-Transfer-Proposed-Law-051117-EN-1.pdf.

While we believe our advocacy has helped delay the implementation of some of the Cybersecurity Law's more onerous provisions and has limited its scope, our members seeking to reach new customers in China inevitably must assess the viability of entering the Chinese market.

Issue: Personal Information Protection Law

The Personal Information Protection Law (PIPL) was enacted by the Chinese National People's Congress on August 20, 2021, and took effect on November 1, 2021.[97] The law applies to all companies processing personal information of Chinese individuals inside or outside China, exposing violators to fines up to 5 percent of annual revenue from the previous year. PIPL also sets out data transfer restrictions and localization requirements for those who exceed the amount of personal information allowed by the Cyberspace Administration of China (CAC). The CAC sets the threshold amount of personal data an organization may handle without restriction and decides what companies are excepted from the law's requirements. The CAC eased some of these requirements in March 2024,[98] and the CAC and the State Administration for Market Regulation (SAMR) issued measures for certifying outbound transfers of personal information that took effect on January 1, 2026,[99] but the transfer mechanisms remain costly and uncertain for small businesses. Article 24 of PIPL also sets out restrictions on the use of automated decision-making, including systems used to deliver targeted advertisements, potentially harming the ability of American companies to derive revenue from their products through advertising. The broad extraterritorial reach of this law, and the heavy penalties associated with non-compliance, pose a significant burden to ACT members and reduce their ability to do business in China. We therefore request the inclusion of the PIPL in the NTE report.

Issue: Various Data Localization Requirements (Proposed and Final)

China implemented or proposed numerous restrictions on the flow of data across its borders. These regulations limit or prohibit the transfer of data outside of China in areas like banking and financial credit, cybersecurity, counterterrorism, commercial information systems, healthcare, and insurance. The Network Data Security Management Regulations, which took effect on January 1, 2025, add further data processing and transfer obligations and extend to some processing outside China.[100] Each represents a significant barrier to market entry and is a non-starter for small business innovators. When compared to large corporations, small businesses are often unable to overcome this barrier and will ultimately be left out of the market. Companies face large penalties for non-compliance. These events threaten to disrupt the free flow of information over the internet on a much larger scale.

---

[97] Standing Committee of the National People's Congress, Personal Information Protection Law of the People's Republic of China (Aug. 20, 2021), http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml.

[98] Cyberspace Administration of China, Provisions on Promoting and Regulating Cross-Border Data Flows (CAC Order No. 16) (Mar. 22, 2024), https://www.cac.gov.cn/2024-03/22/c_1712776611775634.htm

[99] Cyberspace Administration of China and State Administration for Market Regulation, Measures for Personal Information Export Certification (Oct. 17, 2025), https://www.cac.gov.cn/2025-10/17/c_1762449728518762.htm

[100] State Council of the People's Republic of China, Regulations on Network Data Security Management (State Council Decree No. 790) (Sept. 24, 2024), https://www.gov.cn/zhengce/content/202409/content_6977766.htm

Issue: China's Use of Antitrust Laws

ACT believes USTR should, in the context of China's WTO commitments, remain concerned with China's antitrust laws being used as a means to target foreign firms, which USTR has already documented and addressed. China's activities justified under antimonopoly laws often contradict China's commitments under the WTO, including in relation to IP licensing in violation of TRIPS Article 40 Section 8, and in violation of Article 40, which invokes other standards in TRIPS, such as due process ("making decisions on the merits," "without undue delay," "based only on evidence," "with an opportunity for review," "with the right to written notice," and "the right to be represented by independent legal counsel").[101] In addition, China's antimonopoly laws justify Chinese court practices, such as extra-territorial anti-suit injunctions, in violation of China's commitment to TRIPS Articles 1.1, 28.1, 28.2, 41.1, 44.1, 63.1, and 63.3, and a July 2025 WTO appeal arbitration award found China's anti-suit injunction policy inconsistent with the TRIPS Agreement.[102] China has since told the WTO that it withdrew the policy, but the EU stated in September 2025 that it could not conclude that China had fully implemented the award.[103] China's antitrust and competition laws continue to raise concerns regarding their deployment against foreign firms as part of broader economic statecraft. Notably, SAMR's enforcement practice increasingly employs discretionary measures which may conflict with WTO TRIPS procedural safeguards, such as due process rights, evidentiary standards, and independent legal counsel protections. Chinese courts' use of extraterritorial antisuit injunctions and other measures targeting foreign parties may also contravene China's WTO commitments. Recent high-profile antitrust investigations during 2024-2025 illustrate an intensification of scrutiny over foreign company operations in China, linked to claims of IP misuse and competition harm, although transparency remains limited. In November 2025, China committed to end its antitrust, anti-monopoly, and anti-dumping investigations targeting U.S. companies in the semiconductor supply chain,[104] and we urge USTR to confirm that China fully implements this commitment and does not open similar investigations in the future. These instances highlight the ongoing tension between China's ambitions to protect domestic industry and the trade obligations that guard fair treatment of foreign entrants.

Issue: Export Controls, the Unreliable Entity List, and Countermeasures Against U.S. Firms

China increasingly uses export controls, its Unreliable Entity List, and countermeasures under its Anti-Foreign Sanctions Law against U.S. companies as tools of trade retaliation. In February 2025, on the same day it announced retaliatory tariffs, China added U.S. companies to its Unreliable Entity

[101] Mark Cohen, "RCEP And Phase 1: Strange Bedfellows in IP," China IPR, December 3, 2020, https://chinaipr.com/2020/12/03/rcep-and-phase-1-strange-bedfellows-in-ip/; World Trade Organization, "Agreement on Trade-related Aspects of Intellectual Property Rights," https://www.wto.org/english/docs_e/legal_e/27-trips.pdf.

[102] European Commission, WTO appeal arbitrator finds China wrong to restrict intellectual property rights in dispute brought by EU (July 22, 2025), https://policy.trade.ec.europa.eu/news/wto-appeal-arbitrator-finds-china-wrong-restrict-intellectual-property-rights-dispute-brought-eu-2025-07-22_en

[103] Delegation of the European Union to the WTO, Regular Meeting of the Dispute Settlement Body, 26 September 2025 (Sept. 26, 2025), https://www.eeas.europa.eu/delegations/world-trade-organization-wto/regular-meeting-dispute-settlement-body-26-september-2025_en

[104] The White House, Fact Sheet: President Donald J. Trump Strikes Deal on Economic and Trade Relations with China (Nov. 1, 2025), https://www.whitehouse.gov/fact-sheets/2025/11/fact-sheet-president-donald-j-trump-strikes-deal-on-economic-and-trade-relations-with-china/

List and opened an antitrust investigation into a U.S. technology company,[105] and in March 2025 the State Council issued regulations implementing the Anti-Foreign Sanctions Law that allow authorities to seize or freeze assets, including intellectual property, and to restrict transactions, investment, and the provision of data and personal information.[106] China committed in November 2025 to suspend the expanded export controls it announced in October 2025 and to remove certain U.S. companies from its Unreliable Entity List,[107] but these tools remain available and create unpredictable risk for U.S. small businesses that license technology into China, partner with Chinese firms, or source components from China. We urge USTR to monitor China's implementation of these commitments and to address the use of these tools against U.S. firms in the 2027 NTE report.

Issue: Harmful Digital Platform Regulation

China's new digital platform policies impose stringent requirements on digital platforms, substantially increasing compliance burdens and operational risks. Notably, frequent reporting obligations, the risk of heavy fines, and potential business suspensions create significant regulatory barriers for cross-border e-commerce and digital services, particularly for ACT members, hindering digital trade and complicating market entry and operation. The Network Data Security Management Regulations, effective January 1, 2025, add to these burdens by requiring app distribution platforms to check apps for data security compliance and by imposing additional obligations on large platforms.[108]

Issue: Intellectual Property in China

Theft and infringement of IP has grown exponentially in recent years and often originates in China. China's harmful practices put our members' businesses and the jobs they create at serious risk – a single occurrence can represent an "end-of-life" scenario. Both criminals and government-backed hackers based in China are a demonstrated and well-known risk to our members in the digital economy, and the Center for Strategic and International Studies has described China's behavior as "long-running state espionage programs targeting Western firms and research centers" that has carried over into cyberspace.[109] Numerous USTR National Trade Estimate (NTE) reports have detailed how actors affiliated with the Chinese Government and the Chinese military have infiltrated the computer systems of U.S. companies, stealing terabytes of data, including the companies' proprietary information and IP, for the purpose of providing commercial advantages to Chinese

[105] PBS NewsHour, China announces retaliatory tariffs on U.S. imports, antitrust investigation into Google (Feb. 4, 2025), https://www.pbs.org/newshour/world/china-announces-retaliatory-tariffs-on-u-s-imports-antitrust-investigation-into-google

[106] China Daily, Countermeasures against foreign sanctions empowered (Mar. 25, 2025), https://govt.chinadaily.com.cn/s/202503/25/WS67e24650498eec7e1f732acb/countermeasures-against-foreign-sanctions-empowered.html

[107] The White House, Fact Sheet: President Donald J. Trump Strikes Deal on Economic and Trade Relations with China (Nov. 1, 2025), https://www.whitehouse.gov/fact-sheets/2025/11/fact-sheet-president-donald-j-trump-strikes-deal-on-economic-and-trade-relations-with-china/

[108] State Council of the People's Republic of China, Regulations on Network Data Security Management (State Council Decree No. 790) (Sept. 24, 2024), arts. 40-46, https://www.gov.cn/zhengce/content/202409/content_6977766.htm

[109] Jim Lewis, "Learning the Superior Techniques of the Barbarians," Center for International and Strategic Studies.

enterprises. China appropriately remains on USTR's Priority Watch List of countries committing the most extensive IP rights infringements.[110] We support investigations into unfair cloud computing-related and other digital trade barriers, where China has intentionally disenfranchised U.S. firms.[111]

First, we fully support strong and enforceable IP rights for U.S. companies and condemn government policies that seek to diminish those rights to hinder market entry. To the extent these policies are used by the Chinese government, we urge USTR to investigate and document them to determine its next steps. One of the most problematic Chinese policies is the application of the controversial "essential facilities" doctrine to IP in the State Administration for Industry and Commerce's (SAIC)[112] Rules on Prohibition of Abusing Intellectual Property Rights to Eliminate or Restrict Competition (IP Abuse Rules), which took effect on August 1, 2015, and were later incorporated wholesale into China's State Administration for Market Regulation Provisions Prohibiting the Abuse of IPR to Eliminate or Restrict Competition, which were most recently updated in 2023.[113] These rules prohibit the preclusion or restriction of competition without justifiable reasons by refusing to license others to use, under reasonable terms, its intellectual property which is an essential facility in production and operation.

ACT does not support the notion that competitors should have access to regular patents simply because they cannot compete without such access, even in the rare cases where there is little damage to the IP holder, or consumer interests are allegedly harmed by lack of competition. Application of this provision would seriously undermine the fundamental right to exclude others from using one's intellectual property, and thus, impact incentives to innovate in the long term. Under this provision, U.S. innovators, particularly those with operations in China, are vulnerable given the significant discretion vested in SAMR to balance the necessary factors to determine the issuance of a compulsory license.

ACT notes the critical differences between regular patents and standard-essential patents (SEPs), which must be considered separately. FRAND commitments prevent the owners of SEPs, the patents needed to implement a standard, from exploiting market power that results from the broad adoption of a standard.

Today, SAMR appropriately recognizes that it may be an abuse of dominance for SEP holders to eliminate or restrict competition, "such as by refusing to license, tying or imposing other unreasonable trading terms, in violation of fair, reasonable, and non-discriminatory principle." ACT, therefore, does not believe that inclusion of the SAMR's rules addressing SEPs constitutes a WTO violation (in contrast to the SAMR's rules discussed above that require a patent holder to give competitors access to the former's "essential" patents).

In contrast to its policies on patents generally, SAMR's treatment of FRAND-committed SEPs is consistent with an established consensus on the meaning and effect of FRAND commitments. We

[110] https://ustr.gov/sites/default/files/IssueAreas/IP/2022%20Special%20301%20Report.pdf
[111] Stephen Ezell, "Hearing on U.S.-China Innovation, Technology, and Intellectual Property Concern," (April 14, 2022), 15, https://www2.itif.org/2022-us-china-innovation-tech-ip.pdf.
[112] SAIC has since been merged into the State Administration for Market Regulation.
[113] https://www.samr.gov.cn/zw/zfxxgk/fdzdgknr/fgs/art/2023/art_e155397fbe5c4c05ad3c1838c1322ad2.html.

strongly urge USTR to ensure that it does not conflate general patent licensing issues with the unique set of issues—and global competition law consensus—specific to standard-essential patents.

COLOMBIA

Issue: Digital Services Tax

Colombia has introduced a 3 percent tax on digital services provided by foreign companies starting January 2024 under its Significant Economic Presence framework. In September 2025, the government proposed raising this rate to 5% through a tax reform bill, which Congress archived in December 2025.[114] The outgoing administration proposed the same increase again in July 2026 in Bill 004 of 2026, which the incoming government has rejected but which remains pending in committee.[115] This policy imposes additional tax burdens on U.S. digital service providers, undermining the United States-Colombia Trade Promotion Agreement (USCTPA) by treating them unfavorably. Given Colombia's fiscal pressures, a new tax reform is likely, and ACT urges USTR to press Colombia not to raise the rate or adopt other tax measures targeting digital services.

Issue: Intellectual Property Rights

We note that Colombia's patent system is similar to that of Germany and Brazil in that the system bifurcates infringement and validity proceedings, so that an injunction may be awarded even if the validity of the patent has not been examined in complete misalignment with the U.S. approach under eBay, denying adequate protection to U.S. small businesses that rely on a fair and transparent SEP licensing ecosystem to engage in standards-driven markets. Unless addressed by the United States, we expect that Colombia will continue to be a venue for SEP licensing abuse and have a significant impact on the global SEP licensing landscape and American small businesses in particular.

Issue: Over-The-Top Regulation

Colombia's Communications Regulatory Commission (CRC) and Ministry of Information and Communications Technologies (MinTIC) launched a consultation in 2024 aimed to gather input on OTT digital services, which has fed into the prospect of introducing specific regulations or fees on OTT platforms. ACT has engaged with CRC and MinTIC, most recently through comments filed in June 2026 on the CRC's consultations concerning OTT services, unsolicited traffic, and network fees,[116] raising concerns that such policy changes would put trade barriers into place, stifling

[114] Cámara de Representantes de Colombia, Proyecto de Ley 283/2025C, Ley de Financiamiento (archived), https://www.camara.gov.co/ley-de-financiamiento

[115] Cámara de Representantes de Colombia, Proyecto de Ley 004/2026C, Por medio de la cual se adopta una reforma tributaria y se dictan otras disposiciones (filed July 20, 2026), https://www.camara.gov.co/reforma-tributaria-; La República, Ministro entrante, Miguel Gómez, aseguró que tributaria de Petro debe archivarse (July 24, 2026), https://www.larepublica.co/economia/ministro-entrante-miguel-gomez-aseguro-que-tributaria-de-petro-debe-archivarse-4442888.

[116] ACT, Comments on the Study "Monetization in the Content Industry, Traffic and Unsolicited Content" (Study Code 11000-41-3-1) and the Accompanying Technical Consultation (June 16, 2026), https://actonline.org/post/comments-of-the-association-for-competitive-technology-act-on-the-study-monetization-in-the-content-industry-traffic-and-unsolicited-content-study-code-11000-41-3-1-and-the-acco/; ACT, Comments to the CRC Regarding the Study on the Role of OTT Services in Colombia – 2024 (Jan.

innovation and limiting competition in Colombia's digital ecosystem, most acutely harming small companies.

EUROPEAN UNION

Issue: Digital Platform Regulation

ACT has concern with numerous steps taken by the EU themed in advancing European sovereignty, which often are positioned to exclude American companies from entering and competing in the EU, despite the EU's commitment in the August 2025 EU-U.S. Joint Statement to address unjustified digital trade barriers.[117]

As a prime example, the European Commission's (EC) imposition of regulations on digital platforms, via the Digital Markets Act (DMA)[118] continues to present a significant protectionist barrier to trade. The DMA, without justification, intervenes in the operations of competitive and well-functioning digital markets that enable countless small businesses to grow and create jobs. By creating new obligations for "gatekeeping" platforms, the DMA has had, and will have, far-reaching consequences for the companies that operate on them, including ACT members. As recent reports have demonstrated,[119] implementing this novel piece of regulation thoughtfully will be more critical than ever to ensure it does not only level the playing field between the largest players but also truly benefits all businesses, including small app developers. If not implemented with small enterprises in mind, some of the obligations for gatekeepers will lock small app developers with fewer resources out of the market. Further, the DMA's broad-stroke obligations for online platforms have unintentionally opened the gate to malicious actors and put end-users' data and safety at risk. App developers rely on the safe environment platforms provide to keep bad actors out of the app ecosystem, gain consumers' trust, and innovate. The DMA must be implemented to enable all SMEs to innovate, grow, and thrive in a fair, competitive, and safe app ecosystem, and ACT looks forward to collaborating with policymakers to ensure small and medium-sized businesses continue to succeed. The DMA has already been appropriately acknowledged by USTR as a barrier to digital trade and should remain designated as such in future NTEs. As we have discussed in a recently released paper, the impact of the DMA has been harmful and discriminatory in its first year of operation.[120] ACT agrees that the DMA functions as an ex ante competition regulation that is in effect targeting U.S. entities (e.g., notably identifying six U.S. companies as gatekeepers that must adhere to restrictions on data usage, obligations for data portability and access, and requirements for interoperability). Currently, the EC is imposing substantial fines on these companies in

31, 2025), https://actonline.org/post/comments-of-act-the-app-association-to-crc-regarding-study-on-the-role-of-over-the-top-ott-services-in-colombia-2024/.

[117] The White House, Joint Statement on a United States-European Union Framework on an Agreement on Reciprocal, Fair, and Balanced Trade (Aug. 21, 2025), https://www.whitehouse.gov/briefings-statements/2025/08/joint-statement-on-a-united-states-european-union-framework-on-an-agreement-on-reciprocal-fair-and-balanced-trade/

[118] European Commission, Online Platforms, available at https://ec.europa.eu/digital-single-market/en/policies/online-platforms.

[119] https://www.politico.eu/article/iphone-apple-eu-ios-dma-big-tech-anti-competition-pornhub-users-app/.

[120] https://actonline.org/wp-content/uploads/DMA-One-Year-Later.pdf.

enforcement, including €500 million on Apple and €200 million on Meta in April 2025[121] and €890 million on Google in July 2026,[122] with the harm to our community only beginning to be understood. The EC's April 2026 review of the DMA concluded that the regulation remains fit for purpose,[123] a conclusion that does not reflect the experience of small developers, and the EC is now extending the DMA's reach to additional services, reaching a preliminary position in June 2026 that Amazon's and Microsoft's cloud computing services should be designated[124] and issuing guidance in July 2026 on AI interoperability on Android.[125] The potential designation of cloud providers as gatekeepers under the DMA is especially concerning, as the cloud services market is a particularly poor fit for the law's objective of weakening the ability of platforms that stand between businesses and customers to limit passage through that "gate." Cloud services do not stand between customers and businesses; rather, they provide services like hosting or analytics to businesses that are otherwise fully accessible to customers. In addition, to the extent gatekeeper designation might be intended to allow regulators to push for greater data interoperability between clouds, the EU Data Act already addresses switching and interoperability between cloud services, rendering DMA designation redundant.

Further, the EC has already carried forward numerous regulations, directives, consultations, and proposals that raise significant concerns for ACT, including attempts to regulate the free flow of information online through measures such as the EU's Digital Services Act, which centers around tackling illegal hate speech with the goal, moving forward, of removing illegal content from the internet.

Issue: Privacy Regulation

Various provisions of the GDPR impose additional requirements on non-European firms (due to its extraterritorial reach) that increase the cost and risk associated with handling data pertaining to EU citizens. For example, Article 27 of the law requires firms to physically place a representative in the EU.[126] Such provisions can be an insurmountable hurdle to our small business members seeking to enter the EU market. Anything that can be done throughout the GDPR implementation process,

[121] European Commission, Commission finds Apple and Meta in breach of the Digital Markets Act (Apr. 23, 2025), https://digital-markets-act.ec.europa.eu/commission-finds-apple-and-meta-breach-digital-markets-act-2025-04-23_en

[122] European Commission, Commission fines Google €890 million for breaches of the Digital Markets Act (July 23, 2026), https://digital-markets-act.ec.europa.eu/commission-fines-google-eur890-million-breaches-digital-markets-act-2026-07-23_en

[123] European Commission, Review highlights Digital Markets Act remains fit for purpose and has positive impact (Apr. 28, 2026), https://digital-markets-act.ec.europa.eu/review-highlights-digital-markets-act-remains-fit-purpose-and-has-positive-impact-2026-04-28_en; ACT, Feedback to the European Commission Regarding the Review of the Digital Markets Act (Sept. 23, 2025), https://actonline.org/post/feedback-of-act-the-app-association-to-the-european-commission-regarding-the-review-of-the-digital-markets-act/

[124] European Commission, Commission reaches preliminary position that Amazon's and Microsoft's market leading cloud services should be designated under the DMA (June 25, 2026), https://digital-markets-act.ec.europa.eu/commission-reaches-preliminary-position-amazons-and-microsofts-market-leading-cloud-services-should-2026-06-25_en

[125] European Commission, Commission provides guidance to Google for AI interoperability on Android and sharing of Google Search data under the Digital Markets Act (July 16, 2026), https://digital-markets-act.ec.europa.eu/commission-provides-guidance-google-ai-interoperability-android-and-sharing-google-search-data-under-2026-07-16_en

[126] See https://www.privacy-regulation.eu/en/27.htm.

including through the Digital Omnibus the European Commission proposed in November 2025,[127] to ease the burden for small and medium-sized companies could have tremendously positive economic implications.

Issue: Digital Service Taxes

Numerous EU Member States without a DST in place are looking to revive discussions on a Directive for a common system of digital services tax on revenues generated from certain digital services and potentially a corporate tax on a "significant digital presence." ACT strongly encourages the USTR to oppose discriminatory DSTs.

Issue: Network Usage Fees

Since 2022, the European Commission has pursued ways to impose network usage fees on large digital service providers, primarily U.S. technology and content companies, requiring them to subsidize European telecom operators' infrastructure, and its February 2024 White Paper on the future of Europe's digital infrastructure floated extending EU telecom regulations to CSPs, an arbitration mechanism for interconnection fees, and "universal service obligations" requiring digital companies to co-finance telecom infrastructure. Despite the EU's commitment in the August 2025 EU-U.S. Joint Statement not to adopt or maintain network usage fees,[128] the Commission is considering indirect approaches through the Digital Networks Act (DNA), proposed in January 2026, which would replace the European Electronic Communications Code (EECC) and create a voluntary ecosystem cooperation mechanism on IP interconnection and traffic efficiency.[129] ACT urges USTR to ensure this mechanism remains voluntary and does not become a route to impose new costs throughout the internet infrastructure and network edge layers, harming small developers.[130] Italy's AGCOM has already set a precedent by ruling CDNs fall under EECC dispute mechanisms, allowing Italian telcos to press payment claims, a move that could spread across Europe if unchecked.[131] These developments threaten to impose hidden costs on small U.S. digital firms.

Issue: Standards Regulation

In a development that could significantly influence the direction of data and AI regulations, the European Commission has initiated a project to localize standards-setting within the Union for essential sectors of the economy. The EC has stated that this effort aims to prevent the "undue

[127] European Commission, Digital Omnibus Regulation Proposal (Nov. 19, 2025), https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal

[128] The White House, Joint Statement on a United States-European Union Framework on an Agreement on Reciprocal, Fair, and Balanced Trade (Aug. 21, 2025), https://www.whitehouse.gov/briefings-statements/2025/08/joint-statement-on-a-united-states-european-union-framework-on-an-agreement-on-reciprocal-fair-and-balanced-trade/

[129] European Commission, Digital Networks Act (proposal adopted Jan. 21, 2026), https://digital-strategy.ec.europa.eu/en/policies/digital-networks-act

[130] ACT, Feedback to the European Commission Regarding the Consultation on the Digital Networks Act (June 15, 2026), https://actonline.org/post/feedback-of-association-for-competitive-technology-to-the-european-commission-regarding-the-consultation-on-the-digital-networks-act/.

[131] ACT, Feedback to the Autorità per le Garanzie nelle Comunicazioni Regarding Delibera 55/25/CONS (Apr. 14, 2025), https://actonline.org/post/feedback-of-act-the-app-association-to-the-autorita-per-le-garanzie-nelle-comunicazioni-regarding-its-delibera-55-25-cons/.

influence of actors from outside the EU and EEA" in establishing standards for crucial areas. As a result, this initiative could limit ACT members' capacity to contribute to the standards that will be vital for upcoming regulations.

Issue: EU Space Act Proposal

The EU Space Act proposal, introduced in June 2025 and still under consideration in the European Parliament,[132] introduces uncertain and potentially novel technical requirements on service providers that diverge from international norms, particularly in areas like orbital congestion and collision avoidance. Further, under the Space Act, EU operators must rely on the EU Space Surveillance and Tracking system, while non-EU operators, including U.S. companies, face operational challenges due to exclusion from this system and must meet alternative standards not aligned with best practices. The law also discriminates in registration processes by imposing undefined timelines on non-EU operators and features governance concerns given potential conflicts of interest. Enforced from 2030, with a tight compliance window for next-generation constellations, the Act grants the Commission inspection rights over non-EU facilities, raising issues around confidentiality and conflicts with U.S. regulations. Overall, the EUSA imposes disproportionate burdens on non-EU operators, effectively limiting their competitiveness in the European space market, reducing competition in connectivity markets, with harms flowing down to small businesses that rely on a competitive market for internet connectivity.

Issue: Cloud Security Regulation

Since 2020, the EU Agency for Cybersecurity (ENISA) has been developing the European Cybersecurity Certification Scheme for Cloud Services (EUCS). In June 2022, ENISA revised the draft framework to introduce four new criteria— including immunity from foreign law—for cloud service providers (CSPs) to qualify for the highest cybersecurity certification level. If implemented, this requirement would restrict eligibility to companies with their head office and global headquarters in an EU Member State, effectively barring U.S. CSPs from servicing the public sector and regulated industries in the EU and limiting competition and choice for small businesses. The European Commission stated in June 2026 that work on the stalled EUCS will resume,[133] while its January 2026 proposal to revise the EU Cybersecurity Act (CSA) targets risks in the EU's ICT supply chain from third-country suppliers,[134] and its June 2026 proposal for a Cloud and AI Development Act (CADA) would create four cloud and AI sovereignty assurance levels for public sector use, the higher of which require providers to demonstrate independence from third countries or to be owned and controlled from the EU.[135] These proposals would reintroduce through legislation the discriminatory criteria that stalled the EUCS, and ACT urges USTR to press the EU to base any cloud requirements on technical and operational security controls rather than ownership or nationality.

---

[132] European Parliament, Legislative Observatory, Procedure 2025/0335(COD), Safety, resilience and sustainability of space activities in the Union, https://oeil.europarl.europa.eu/oeil/en/procedure-file?reference=2025%2F0335%28COD%29

[133] European Commission, Proposal for a Regulation on the Cloud and AI Development Act, Explanatory Memorandum, COM(2026) 502 final, at 4 (June 3, 2026), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52026PC0502.

[134] European Commission, Cybersecurity Act (revision proposed Jan. 2026), https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

[135] European Commission, Cloud and AI Development Act (proposed June 3, 2026), https://digital-strategy.ec.europa.eu/en/policies/cloud-and-ai-development-act

Issue: Public Procurement

In September 2026, the European Commission proposed a Public Procurement Act, COM(2026) 590, that would introduce European preference criteria into public procurement across the EU.[136] While the Commission describes the proposal as consistent with the EU's international commitments, preference criteria of this kind give contracting authorities new grounds to exclude U.S. bidders, including the small technology firms that sell software and services to public buyers directly or as part of larger offerings. ACT urges USTR to press the EU to ensure that the final text fully respects its obligations under the WTO Government Procurement Agreement and does not become a vehicle for excluding U.S. suppliers.

Issue: Artificial Intelligence Regulation

The EU's enactment of sweeping regulations on the use of artificial intelligence (AI)[137] raises concerns for ACT about regulation pre-empting new and innovative uses of AI and related IPR issues. On August 1, 2024, the EU AI Act went into force, which include both positive and uncertain approaches to regulating AI. While we appreciate the EU's use of a risk-based approach and its June 2026 decision to delay high-risk obligations to December 2027 and August 2028,[138] we are most concerned with the cost of complying with minimum requirements for transparency and safety standards for small and medium-sized businesses and startups.

Additionally, the AI Act will mandate that providers of general-purpose AI models disclose a "sufficiently detailed" summary of their model training data. The European Commission published a template for these disclosures in July 2025.[139] To the extent the template requires detailed disclosure of training data, it could compromise the intellectual property and trade secrets of model developers. Furthermore, Recital 106 of the AI Act states that "any provider placing a general-purpose AI model on the Union market must comply with [the Regulation's copyright obligations], regardless of the jurisdiction in which the copyright-relevant acts related to the training of those general-purpose AI models occur." If the AI Act imposes more rigorous requirements or compliance standards, it could further complicate matters for small developers.

We also note that European standardization organizations CEN and CENELEC have established a dedicated technical committee (JTC 21) to create harmonized standards that will facilitate the implementation of the AI Act. This includes developing a framework for AI trustworthiness, as well as standards for AI risk management and quality assurance. It remains uncertain whether these

[136] European Commission, Proposal for a regulation on public contracts and concessions (Public Procurement Act), COM(2026) 590 (Sept. 9, 2026), https://single-market-economy.ec.europa.eu/publications/proposal-regulation-public-contracts-and-concessions_en

[137] Digital Single Market: Artificial Intelligence, European Commission, last updated September 27, 2021. https://ec.europa.eu/digital-single-market/en/artificial-intelligence.

[138] Council of the EU, Artificial intelligence: Council gives final green light to simplify and streamline rules (June 29, 2026), https://www.consilium.europa.eu/en/press/press-releases/2026/06/29/artificial-intelligence-council-gives-final-green-light-to-simplify-and-streamline-rules/

[139] European Commission, Explanatory Notice and Template for the Public Summary of Training Content for General-Purpose AI Models (July 24, 2025), https://digital-strategy.ec.europa.eu/en/library/explanatory-notice-and-template-public-summary-training-content-general-purpose-ai-models

standards will align with existing ISO standards, such as ISO 42001. If the standards diverge, the ACT community would face immense burdens in adjusting to EU-specific requirements.

The Commission published its proposal for CADA on June 3, 2026, as part of the Tech Sovereignty Package.[140] Its sovereignty framework uses four "Union assurance levels." Every cloud service bought by a public body must meet at least Level 1, the lowest tier, and member states and EU bodies use risk assessments to decide which public-sector activities require Level 2, 3, or 4. The lower levels center on baseline requirements, including EU establishment, data localization within the EU, and transparency on subcontracting and data flows. The higher levels move to safeguards against third-country access and, at Levels 3 and 4, a bar on third-country control, supply-chain transparency, personnel clearance, and independent audit. CADA would also require public authorities to weigh "Union added value" as a non-price procurement criterion. ACT warns that CADA conditions access to Europe's public-sector market on where a provider stores data, where it is headquartered, and who owns it, rather than on objective security and performance criteria.[141] Even at Level 1, mandatory EU data localization would force small U.S. software providers to build or contract for EU-resident infrastructure before they can compete for public contracts, a cost large firms can absorb but small businesses often cannot. At Levels 3 and 4, which the Commission's own impact assessment treats as closed to non-European providers,[142] excluding trusted U.S. providers based on ownership and corporate structure narrows the range of tools available to European public bodies and to the small businesses that serve them. Europe's digital economy, including its own startups, thrives when compute capacity can scale quickly and demand for cloud and AI services is met by the most capable providers.

Issue: Intellectual Property and Standards

The established Unified Patent Court (UPC) has posed significant concerns for American companies that operate within the EU economy. The UPC enables holders of IP issued in one of the 18 Member States that joined the court to seek an injunction that would be applied across all 18 jurisdictions. The court has become an attractive venue for SEP holders who use the court to leverage their dominant market position against potential licensees.[143] We suspect that the UPC will continue to be a venue ripe for abuse of SEP and other IP rights against American companies.

We note that the European Commission's formal withdrawal of the EU proposed regulation on standard-essential patents (SEPs) in October 2025,[144] which the European Parliament has

[140] European Commission, Proposal for a Regulation on the Cloud and AI Development Act, COM(2026) 502 final, arts. 29–30 & annex II (June 3, 2026), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52026PC0502.
[141] ACT, Feedback to the European Commission Regarding its Cloud and AI Development Act (June 3, 2025), https://actonline.org/post/feedback-of-act-the-app-association-to-the-european-commission-regarding-its-cloud-and-ai-development-act/.
[142] European Commission, Impact Assessment Report Accompanying the Proposal for a Cloud and AI Development Act, SWD(2026) 502 final (June 3, 2026), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52026SC0502.
[143] ACT, Letter to the European Commission's Directorate-General for Trade on the Judicial Landscape for Standard-Essential Patent Licensing in Europe (June 29, 2026), https://actonline.org/post/association-of-competitive-technologys-letter-to-dg-trade-on-sep-licensing-in-europe-judicial-landscape/.
[144] European Parliament, Legislative Observatory, Procedure 2023/0133(COD), Standard essential patents, https://oeil.europarl.europa.eu/oeil/en/procedure-file?reference=2023%2F0133%28COD%29

challenged before the CJEU,[145] will continue to enable bad actors to abuse the SEP licensing and standards ecosystem. A lack of soft intervention in the EU SEP landscape will impact all American businesses that build on top of technical standards and sell their products and devices in the EU. We urge the USTR to support the EU in moving forward with a regulation on SEPs as an effective solution to judicial practices that are inconsistent with established policy goals.[146]

Each of these concerns is either affecting or proposing policy changes for nascent economic segments and services that are solutions in search of a problem and stand to enable discrimination against small digital economy innovators to compete in the EU.

FRANCE

Issue: Digital Services Tax (DST)

On March 6, 2019, the government of France released a proposal for a 3 percent levy on revenues that certain companies generate from providing certain digital services to, or aimed at, French users. USTR has since undertaken a Section 301 investigation, releasing its report in December 2019.[147] In September 2025, the French Constitutional Council upheld the 3 percent DST as constitutional.[148]

In October 2025, the French National Assembly's finance committee voted in favor of a fivefold tax increase from 3 percent to 15 percent, specifically on U.S. tech companies.[149] Although the rate remained at 3 percent in the 2026 budget the government ultimately adopted,[150] the finance committee voted again in October 2026 to raise the rate to 15 percent and the global revenue threshold to €2 billion in the 2027 budget.[151] France's DST is contrary to the long-standing agreement by World Trade Organization (WTO) members not to apply customs duties to cross-border electronic transmissions and prejudices ongoing discussions at the WTO and the Organization for Economic Cooperation and Development (OECD). This action will harm U.S. goods and services exporters of all sizes in nearly every sector and threaten American jobs, creating a damaging precedent for a fragmented digital economy that will suppress American small business innovation and job growth.

---

[145] Case C-727/25, European Parliament v European Commission, action brought on 14 November 2025, OJ C/2026/89, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C_202600089

[146] ACT, Letter to the European Council on the European Commission's Intention to Withdraw the Standard Essential Patents Regulation (Feb. 20, 2025), https://actonline.org/post/letter-from-act-the-app-association-to-the-european-council-on-the-european-commissions-intention-to-withdraw-the-standard-essential-patents-regulation/.

[147] https://ustr.gov/sites/default/files/Report_On_France%27s_Digital_Services_Tax.pdf.

[148] Tax Foundation, Digital Services Taxes in Europe, 2026 (May 4, 2026) (France's DST upheld as constitutional on September 12, 2025), https://taxfoundation.org/data/all/eu/digital-services-taxes-europe/.

[149] https://waysandmeans.house.gov/2025/10/27/ways-and-means-committee-republican-leaders-slam-french-proposal-to-impose-higher-discriminatory-digital-services-tax-on-u-s-innovators/#:~:text=WASHINGTON%2C%20D.C.%20%E2%80%93%20As%20lawmakers%20in,against%20DSTs%20around%20the%20world.

[150] Journal du Geek, La taxe GAFAM pourrait passer de 3 % à 15 % (Oct. 12, 2026), https://www.journaldugeek.com/2026/10/12/la-taxe-gafam-pourrait-passer-de-3-a-15-4-milliards-pour-renflouer-la-dette-de-la-france/

[151] Univers Freebox, Les députés veulent taxer Microsoft, Facebook, Apple et compagnie à 15% (Oct. 13, 2026), https://www.universfreebox.com/?p=598327

We recognize that some countries have committed to withdrawing DSTs once the Organization for Economic Cooperation and Development (OECD) agreement is realized. However, until they are rescinded, we urge for the inclusion of digital service taxes in the NTE.

Issue: Prohibitions on the Use of Strong Encryption

ACT is deeply concerned with efforts in France to weaken encryption under the pretext of combating narcotrafficking. In March 2025, the French National Assembly removed from the narcotrafficking bill ("Loi visant à sortir la France du piège du narcotrafic") a provision that would have required messaging services to give authorities access to encrypted communications,[152] but similar proposals are likely to return in other legislation. As we explain above, ACT members depend on the use of strong encryption techniques to keep users safe from harms like identity theft. French government efforts to require that backdoors be built into encryption keys for the purpose of government access jeopardize the safety and security of data, as well as the trust of end users, by creating known vulnerabilities that unauthorized parties can exploit. We urge USTR to monitor any renewed attempt in France to mandate such access.

Issue: Sovereign Cloud Requirements in Public Procurement

France's 2024 law on securing and regulating the digital space (the SREN law) requires State administrations and certain public bodies to host sensitive data with cloud providers that are protected against extraterritorial laws, and Decree No. 2026-272 of April 14, 2026 made this obligation enforceable, with compliance shown through the SecNumCloud qualification issued by France's cybersecurity agency.[153] Because SecNumCloud limits non-European ownership of qualified providers, these rules effectively exclude U.S. cloud providers from a growing share of French public procurement, and a pending bill would extend similar obligations to large local governments. These requirements also limit the choices of the small software developers that build public sector solutions on U.S. cloud services. We urge USTR to press France to base its cloud security requirements on technical and operational controls rather than the nationality of a provider's owners.

GERMANY

Issue: Data Sharing Mandates

The German Competition Act has been amended to incorporate extensive restrictions that disproportionately affect U.S. companies, including the mandatory sharing of proprietary data with competitors. This has already led to legal actions and findings aimed at U.S. firms under Section 19a, most recently binding commitments in August 2026 that require Apple to change the consent

[152] Electronic Frontier Foundation, Win for Encryption: France Rejects Backdoor Mandate (Mar. 21, 2025), https://www.eff.org/deeplinks/2025/03/win-encryption-france-rejects-backdoor-mandate

[153] Banque des Territoires (Localtis), SecNumCloud : six GIP assujettis, les données sensibles enfin définies (Apr. 16, 2026), https://www.banquedesterritoires.fr/secnumcloud-6-gip-assujettis-les-donnees-sensibles-enfin-definies

prompts of its App Tracking Transparency framework,[154] a privacy feature on which app developers and their users rely.

Issue: Unbalanced German Patent Law as a Trade Barrier

Germany continues to develop damaging patent policy and enforcement frameworks. Under Germany's current legal framework, courts issue injunctions against those accused of patent infringement without fully determining if infringement has occurred. The courts also do not consider whether the remedy they order is proportionate to the impact on the public interest. Fortunately, the German government took an important step towards creating a more competitive and innovation-enabling environment in Germany by modernizing its Patent Act.

The modernized Patent Act provides for a change to §139, which regulates injunctive relief for the patent holder in cases of patent infringement. The new revision now allows for the limitation of injunctions for proportionality reasons. It remains to be seen over the next several years which cases will trigger these restrictions of injunctive relief and how the modernized Patent Act will impact the way courts grant injunctions in patent litigation.

Because an injunction can be devastating for small and medium-sized businesses whose business models and growth often depend entirely on one product line or offering, it's so important that courts confirm an injunction is in the public interest. For this reason, considering the proportionality of a remedy before granting an injunction is essential to ensure continued small business competitiveness and a level playing field for all actors. We believe this modernized Patent Act addresses some of the current power imbalances in German patent law and aligns Germany meaningfully with many other leading markets, but we encourage USTR to monitor this development in the 2027 NTE report.

In practice, German courts have historically been a favorable venue for patent holders to enforce their patents. Courts in Germany have been known to award injunctive relief to patent holders based on the court's determination of infringement before the validity of the patent has properly been assessed by the German Federal Patent Court. Germany's practice to award injunctions so readily has created international conflicts where their decisions extend to patents issues in another jurisdiction.

In the following years, German courts have continued their practice of awarding injunctions to SEP holders against licensees without first considering the validity of the patents, and on the basis that the licensee did not sufficiently express its willingness to take a license from the SEP holder.[155] The burden that German courts have imposed on licensees to show their "willingness" to accept a SEP holder's offered license on seemingly FRAND terms distorts an important holding from *Huawei*

[154] Bundeskartellamt, Apple changes its rules for personalised advertising in apps (Aug. 17, 2026), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2026/08_17_2026_Apple_ATTF.html

[155] See Nokia v Daimler, District Court (Landgericht) of Mannheim, judgment dated 18 August 2020, Case-No. 2 O 34/19; see Sisvel v Haier, Federal Court of Justice, judgment dated 5 May 2020, Case No. KZR 36/17; ACT, Letter to the European Commission's Directorate-General for Trade on the Judicial Landscape for Standard-Essential Patent Licensing in Europe (June 29, 2026), https://actonline.org/post/association-of-competitive-technologys-letter-to-dg-trade-on-sep-licensing-in-europe-judicial-landscape/.

Technologies Co. v. ZTE Deutschland GmbH. German courts have also begun issuing anti-interim-license injunctions, as the Munich Regional Court did in September 2025.[156]

Germany's approach to SEP injunctions has caused immense disruptions to supply chains across several industries and has resulted in various companies ceasing operation in the country because of the inability to reliably use standards (due to an imbalanced approach to SEP injunctions), fraying the international norm for limited injunctions on FRAND-committed SEPs and undermining international standards.

Issue: Proposed Digital Levy

Germany's federal government has considered a 10 percent levy on the digital advertising revenues of large online platforms.[157] Such a levy would fall mainly on U.S. companies and, like other DSTs, would raise costs for the small businesses that rely on these platforms to reach customers. ACT urges USTR to oppose any German digital levy and to address it in the 2027 NTE report.

Issue: Media Investment Obligations

In May 2026, Germany's federal cabinet adopted a draft Media Services Investment Obligation Act that would require international streaming services and German video-on-demand services to invest at least 8% of their net annual revenue in European audiovisual works, most of it in German-language and new productions, possibly from January 1, 2027.[158] To count toward the obligation, an investment could give the platform exclusive exploitation rights for only three to seven years before the rights revert to the producer. These limits on the ownership and use of IP fall mainly on U.S. services and raise concerns under Germany's national treatment obligations under the TRIPS Agreement. We ask USTR to oppose the measure and to include it in the 2027 NTE report.

HUNGARY

Issue: Data Localization Requirement

In Hungary, data management for state and local government bodies providing essential services was regulated by Act No. 50 of 2013 on the Electronic Information Security of State and Local Government Bodies, which mandated that data handled by these bodies be processed and stored within Hungarian territory, unless the supervisory authority permitted processing in another European Economic Area country. Its successor, Act LXIX of 2024 on the cybersecurity of Hungary, continues to allow covered public bodies to use non-private cloud services or process data abroad only on the basis of a data classification and where no other law prohibits or restricts it.[159]

---

[156] JUVE Patent, Legal News Ticker, Regional Court Munich I – Anti-Interim License Injunction (AILI) (Dec. 18, 2025), https://www.juve-patent.com/ticker/legal-news-ticker-in-cooperation-with-grur/#regional-court-munich-i-anti-interim-license-injunction-aili

[157] Tax Foundation, Digital Services Taxes in Europe, 2026 (May 4, 2026), https://taxfoundation.org/data/all/eu/digital-services-taxes-europe/

[158] Screen Global Production, Streaming execs and producers debate likely German investment obligation (July 3, 2026), https://www.screenglobalproduction.com/news/2026/07/03/streaming-execs-producers-debate-german-investment-obligations

[159] Act LXIX of 2024 on the cybersecurity of Hungary, Section 9(4), https://njt.hu/jogszabaly/en/2024-69-00-00

Additionally, any organization not registered in Hungary but dealing with such data is required to appoint a local representative in Hungary, ensuring compliance and local oversight.

INDIA

Issue: Various Proposed and Final Restrictive Data Localization Laws

India has both proposed and implemented policies that restrict the flow of data across its borders and create significant issues for small business innovators seeking to expand into the Indian market, including:

- India's National Data Sharing and Accessibility Policy which requires that all data collected using public funds to be stored within the borders of India.[160]

- The 2015 National Telecom M2M ("machine to machine") Roadmap,[161] which has not been implemented, states that all M2M gateways and application servers serving customers in India need to be located within India.

- India's 2018 Draft Cloud Computing Policy would require data generated within India to be stored within the confines of the country, and in 2026 the government was reported to be considering a requirement that companies in critical sectors such as energy, telecommunications, and financial services run their core digital infrastructure only on sovereign cloud systems built in India.[162] In September 2026, the Ministry of Electronics and Information Technology was also reported to have drafted a sovereign cloud framework for government data that would assess where providers' servers are located, who controls them, and how much of their technology and supply chain stays under Indian control.[163] As a result of these proposals, cloud companies will either be forced out of the India market or be required to build local data centers to comply with India's policy. Therefore, this policy will deter or create a barrier to entry in the Indian marketplace for small and large companies alike.

- In December 2023, India enacted the Telecommunications Act, 2023, which replaced the outdated Indian Telegraph Act and Wireless Telegraphy Act,[164] and the Department of Telecommunications (DoT) continues to issue rules under the new law that could control the use of M2M communications and the communications between IoT devices. These rules

[160] Government of India Ministry of Science & Technology, India's National Data Sharing and Accessibility Policy, (2012), available at https://dst.gov.in/national-data-sharing-and-accessibility-policy-0.
[161] Government of India Ministry of Communications & Information Technology Department of Telecommunications, National Telecom M2M Roadmap, available at http://www.gsma.com/connectedliving/wp-content/uploads/2015/05/150513-DoT-National-Telecom-M2M-Roadmap.pdf.
[162] Shrishti Bisht, Centre Mulls Sovereign Cloud Mandate For Critical Sectors, INC42 (Apr. 28, 2026), https://inc42.com/buzz/centre-mulls-sovereign-cloud-mandate-for-critical-sectors/.
[163] StratNews Global, Sovereign Cloud Plan for India's Government Data (Sept. 14, 2026), https://stratnewsglobal.com/general/sovereign-cloud/.
[164] Inc42, Telecom Bill 2023 Excludes OTT, Confirms Ashwini Vaishnaw (Dec. 23, 2023), https://inc42.com/buzz/telecom-bill-2023-excludes-ott-confirms-ashwini-vaishnaw.

have the potential to significantly affect American IoT device and application makers, as the Indian government looks to increase domestic production of telecommunications devices and related services.

Issue: Intellectual Property Rights Enforcement

India represents an immense opportunity for American small business tech and software development companies. India's technology industry is becoming a global leader, employing over 5.4 million workers with revenues of an estimated $245 billion in fiscal year 2023.[165] However, ACT members continue to experience a wide range of IPR infringement and lack of legal redress, despite ongoing (incomplete) efforts across Indian ministries and courts that appear to lend themselves to a more consistent and reliable IPR regime in the country. Ongoing problems in this key market include but are not limited to:

- A lack of copyright protections and enforcement;
- A failure to provide consistent protection for trade secrets across India; and
- Data storage and processing localization requirements imposed on small businesses that can require unfettered access to data (including IP), a non-starter for ACT members.

Certain steps indicate the Indian government's willingness to adequately protect IPR. For example, the Indian government undertook efforts to further its commitment to formally establish a copyright royalty board and appoint a functional Intellectual Property Appellate Board. Under the Finance Act of 2017, the informal Copyright Board merged with the Intellectual Property Appellate Board. As a result, applications for copyrights increased by 78 percent from 2016-2017, compared to 2015-2016.[166] In 2021, the Tribunals Reforms Act abolished the Intellectual Property Appellate Board and transferred its functions to the High Courts and commercial courts.[167] As of May 20, 2016, the Indian government established additional commercial courts, advancing the 2015 Commercial Courts Act,[168] which ACT perceives as further evidence of India's commitment to enhance its IPR procedures. Furthermore, India acceded to the WIPO Internet Treaties in July 2018 (namely the WIPO Copyright Treaty and WIPO Performances and Phonograms Treaty). The Indian government also appears committed to the IPR Task Force announced by the Maharashtra government. As of January 24, 2018, Cell for IPR Promotion and Management (CIPAM) and Federation of Indian Chambers of Commerce & Industry (FICCI) have made an IPR Enforcement Toolkit for Police, and there have been 26 programs dedicated to training police officers on Intellectual Property Rights Enforcement. Despite this positive movement, ACT members experience weak and ineffective enforcement in India.

Moreover, numerous hurdles to market access, either in place today or proposed, restrict market access for ACT members that rely on IPR, including but not limited to data localization requirements

[165] See https://nasscom.in/sites/default/files/sr-2023-press-release.pdf.
[166] See https://spicyip.com/wp-content/uploads/2018/01/IPR-Regime-In-India-Government-Initiatives.pdf.
[167] PRS Legislative Research, The Tribunals Reforms Bill, 2021 (Aug. 2021), https://prsindia.org/billtrack/the-tribunals-reforms-bill-2021.
[168] See https://timesofindia.indiatimes.com/city/delhi/Commercial-courts-begin-functioning-in-Delhi-Mumbai/articleshow/52488068.cms.

and in-country cybersecurity testing mandates, such as the cross-border transfer and localization powers under India's Digital Personal Data Protection Act, 2023 and its implementing rules discussed below.

ACT members continue to experience IP infringement originating from India, and face challenges in enforcement through the Indian system. India has not yet fully implemented its obligations under the WIPO Copyright Treaty and WIPO Performances and Phonograms Treaty; furthermore, Indian patent law is inconsistent with the TRIPS Agreement. Another troubling development is the Indian government's continuing effort to decriminalize provisions in its IP laws,[169] including through the Jan Vishwas (Amendment of Provisions) Act, 2023, which replaced certain criminal penalties in the Patents Act with monetary penalties.[170] Extending this approach to the Copyright Act would threaten copyright protections that aim to protect small businesses and innovators alike.

India has become a new venue for SEP abuse, impeding small and medium-sized businesses and startups from bringing deep-tech solutions to critical global markets. In 2023, the Delhi High Court held that SEP holders are not prohibited from seeking an injunction from the court at an interim or final stage.[171] Since then, the Delhi High Court has ordered implementers to post pro tem security early in a case under a lowered prima facie standard, including in *Dolby v. Lava*, where the deposit was based on the rates the SEP holder itself had offered.[172]

Small inventors, including ACT members, rely on the FRAND construct to develop cutting-edge technology around the globe, which is defeated by the ability for some SEP holders to hold international technical standards hostage. We address this issue in detail in our piece, "A Call to Action: Guiding a Fair Standard-Essential Patent Licensing Process for a Thriving Indian Economy,"[173] a comprehensive paper recommending a pro-competitive standards and SEP framework for India that will protect and augment its Indian innovation as well as India's global leadership.

Issue: Digital Platform Regulation

The Indian government (most recently the Ministry of Corporate Affairs (MCA)[174]) continues to propose competition-themed interventions into nascent and highly competitive digital markets, raising significant concerns for ACT members that pro-competitive dynamics in the Indian market will be distorted to benefit a few large developers. While the Indian government has since withdrawn the draft digital competition law in its current form, MCA has commissioned a market study on the thresholds and core digital services a fresh version of the legislation would cover, which the Management Development Institute (MDI) Gurugram began in 2026 with a final report expected in

[169] Surojit Gupta, Govt Moves to Decriminalise Minor Offences to Woo Investors, June 12, 2020, https://timesofindia.indiatimes.com/india/govt-moves-to-decriminalise-minor-offences-to-woo-investors/articleshow/76331374.cms.
[170] PRS Legislative Research, The Jan Vishwas (Amendment of Provisions) Bill, 2022 (passed Aug. 2023), https://prsindia.org/billtrack/the-jan-vishwas-amendment-of-provisions-bill-2022.
[171] Intex Technologies (India) Ltd. V. Telefonaktiebolaget L M Ericsson [2023 SCC OnLine Del 1845].
[172] Dolby International AB & Anr. v. Lava International Ltd., CS(COMM) 350/2024 (Del. HC July 10, 2025), https://indiankanoon.org/doc/148335635/.
[173] See https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4536835.
[174] https://www.mca.gov.in/bin/dms/getdocument?mds=gzGtvSkE3zIVhAuBe2pbow%253D%253D&type=open.

October 2026.[175] ACT participated in the study's stakeholder consultation.[176] In August 2026, the Parliamentary Standing Committee on Finance urged the government to finalize the bill and extend it to virtual assistants and cloud services.[177] We urge USTR to track digital platform regulation in India, to press India to honor its February 2026 commitment to address discriminatory or burdensome barriers to digital trade,[178] and to include it in the 2027 NTE report.

Separately, the Competition (Amendment) Act, 2023 and the CCI's 2024 penalty guidelines allow the CCI to calculate penalties on an enterprise's global turnover rather than on turnover linked to India or to the conduct at issue, an approach now under challenge in the Delhi High Court.[179] Penalties untethered from Indian commerce raise the stakes of the CCI's ongoing investigations of U.S. platforms, including its app store investigation, and discourage U.S. companies from launching new products and services in India, which in turn limits the distribution and security tools that small developers rely on to reach Indian consumers. We ask USTR to urge India to tie competition penalties to turnover from the relevant Indian market.

Issue: Proposed Regulation of Over-The-Top Services

India continues to explore proposed regulation of OTTs (e.g., through TRAI consultations and rules issued under its Telecommunications Act, 2023), including through licensing and extending universal service contribution mandates to OTTs. ACT strongly objects to these proposals and continues to engage with India to avoid OTTs being treated the same as telecommunications services, save for OTT communications services that have the primary purpose of providing real-time person-to-person telecommunication voice services using the network infrastructure (e.g., utilizing a telephone number) of a TSP. Although the Telecommunications Act, 2023 does not cover OTT services,[180] the Department of Telecommunications amended its telecom cybersecurity rules in 2025 to reach apps that identify users by mobile number and, in November 2025, directed messaging apps to keep each account continuously linked to the SIM card in the user's device,[181] with the compliance deadline now extended to December 31, 2026.[182] Consistent with the above, these

[175] MediaNama, RTI: Government Studying Which Tech Companies and Services Should Fall Under Digital Competition Bill (Oct. 13, 2026), https://www.medianama.com/2026/10/223-rti-mca-digital-competition-bill-india-market-study/.
[176] ACT, Letter to Indian Parliament Standing Committee on Finance re Digital Competition Bill Considerations (Aug. 9, 2026), https://actonline.org/post/act-letter-to-indian-parliament-standing-committee-on-finance-re-digital-competition-bill-considerations/.
[177] MediaNama, Lowdown: Parliamentary Committee on Finance Calls for Digital Competition Bill, E-Commerce Code of Conduct (Aug. 17, 2026), https://www.medianama.com/2026/08/223-committee-finance-digital-competition-bill/.
[178] The White House, United States-India Joint Statement (Feb. 6, 2026), https://www.whitehouse.gov/briefings-statements/2026/02/united-states-india-joint-statement.
[179] MediaNama, Apple Challenges CCI's Global Turnover Penalty Framework in Delhi High Court (Nov. 26, 2025), https://www.medianama.com/2025/11/223-apple-cci-global-turnover-penalty-framework-delhi-high-court/.
[180] Inc42, Telecom Bill 2023 Excludes OTT, Confirms Ashwini Vaishnaw (Dec. 23, 2023), https://inc42.com/buzz/telecom-bill-2023-excludes-ott-confirms-ashwini-vaishnaw.
[181] All India Radio News, DoT Mandates SIM Binding for Messaging Apps to Curb Digital Fraud (Dec. 1, 2025), https://www.newsonair.gov.in/dot-mandates-sim-binding-for-messaging-apps-to-curb-digital-fraud.
[182] PTI, DoT Extends SIM-Binding Deadline for Messaging Apps to Dec 31, OUTLOOK BUSINESS (Apr. 2, 2026), https://www.outlookbusiness.com/economy-and-policy/dot-extends-sim-binding-deadline-for-messaging-apps-to-dec-31.

developments are of high concern to our community and we urge for their consideration in the 2027 NTE report.

Issue: Continuing Threats and Uncertainty Regarding the Ability to Use Strong Encryption

Currently, India's 2021 IT Rules require large messaging services to enable identification of the first originator of information, a traceability mandate that cannot be met without weakening end-to-end encryption, which WhatsApp challenged in the Delhi High Court in 2021,[183] and the Supreme Court transferred all challenges to the IT Rules to that court in 2024.[184] CERT-In directions issued in 2022 also require VPN, cloud, and data center service providers to keep subscriber records for five years and require covered entities to keep system logs within India for 180 days.[185] Laws like this provide fewer touchpoints for our members' apps to reach consumers. The Indian government abandoned its proposed National Encryption Policy after widespread pushback and recognition that encryption is a key building block for trust in digital infrastructure. Nevertheless, the government is considering diluting end-to-end encryption in a variety of use cases.[186] This is an ongoing issue of serious concern to small business innovators; therefore, we recommend it be considered in the 2027 NTE report to ensure continued prioritization for the U.S. government and other stakeholders.

Issue: Sweeping Privacy Regulation in India

India's Digital Personal Data Protection Act, 2023 (DPDP Act) and the Digital Personal Data Protection Rules, 2025, notified in November 2025, set rules for how personal data should be processed and stored as well as list the rights of people regarding their personal information, with most obligations phased in over 18 months.[187] As the law has evolved, ACT believes that its provisions have improved, though implementation of the law will be crucial in shaping ACT members' ability to operate and grow in this vital market. The DPDP Act gives India's central government the power to exempt any agency from its requirements on grounds related to national security, national sovereignty, and public order, and to restrict transfers of personal data to countries it designates.[188] The Rules also let the government require significant data fiduciaries to keep categories of personal data identified by a government committee within India, without clear criteria, and in early 2026 the Ministry of Electronics and Information Technology (MeitY) considered

[183] Bar & Bench, WhatsApp Moves Delhi High Court Against IT Intermediary Rules 2021 Mandating It to Trace First Originator of Information (May 26, 2021), https://barandbench.com/news/litigation/whatsapp-moves-delhi-high-court-against-it-intermediary-rules-2021-trace-originator-information.
[184] Bar & Bench, Supreme Court Transfers IT Rules Petitions to Delhi High Court (Mar. 22, 2024), https://www.barandbench.com/news/supreme-court-transfers-it-rules-petitions-to-delhi-high-court.
[185] Indian Computer Emergency Response Team, Directions Under Sub-section (6) of Section 70B of the Information Technology Act, 2000 (Apr. 28, 2022), https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf.
[186] Trisha Ray, The Encryption Debate in India: 2021 Update, Carnegie Endowment Int'l Peace, Mar. 31, 2021, available at https://carnegieendowment.org/2021/03/31/encryption-debate-in-india-2021-update-pub-84215.
[187] Press Information Bureau, Digital Personal Data Protection Rules, 2025 (Nov. 2025), https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc20251117695301.pdf.
[188] The Digital Personal Data Protection Act, 2023 (No. 22 of 2023), https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf.

bringing these transfer rules into force immediately.[189] These provisions could create technical issues that raise small businesses' compliance costs, and ACT requests U.S. government support to ensure that India's law and its implementation do not serve as trade barriers.

Issue: Content Takedown and AI Labelling Mandates

In February 2026, India amended its IT Rules to require platforms to label synthetically generated content with visible disclosures and, where technically feasible, embedded provenance metadata, to require large social media services to collect user declarations on whether uploads are AI-generated and verify them, and to cut the deadline for removing content after a government notice from 36 hours to three hours.[190] These one-size-fits-all mandates apply regardless of the risk a given use presents, and a three-hour removal window leaves no practical room for review, which pushes services toward over-removal of lawful content. Small U.S. developers that offer AI features or host user content face compliance costs that larger domestic competitors can absorb more easily. We urge USTR to press India to take a risk-based approach that relies on existing law and to restore workable takedown timelines.

Issue: Digital Services Tax

USTR found India's DST discriminatory under Section 301,[191] and India abolished the 2 percent equalization levy on e-commerce supplies from August 1, 2024 and the 6 percent equalization levy on online advertising services from April 1, 2025.[192] We welcome the removal of these levies, which were inconsistent with international tax principles, restricted U.S. commerce, and created a damaging precedent for a fragmented digital economy that would suppress American small business innovation and job growth.

We urge USTR to secure a commitment in the U.S.-India Bilateral Trade Agreement that India will not reimpose a digital services tax or a similar levy, and to include any such measure in the 2027 NTE report.

INDONESIA

Issue: Data Localization Requirements

Indonesia's Ministry of Communications and Information Technology (MCIT), now the Ministry of Communication and Digital Affairs (Komdigi), has enacted regulations that require electronic system

[189] Anwesha Sen, MeitY Considers Reducing DPDPA Compliance Timelines, TAKSHASHILA INSTITUTION (Jan. 26, 2026), https://takshashila.org.in/content/blogs/20260126-meity-considers-reducing-dpdpa-compliance-timelines.html.

[190] Outlook Business, Social Media Platforms Get 3 Hours to Remove Unlawful, AI Content Under New IT Rules (Feb. 10, 2026), https://www.outlookbusiness.com/news/it-rules-amendment-2026-3-hour-takedown-rule-synthetic-content-defined-new-compliance-norms.

[191] https://ustr.gov/sites/default/files/enforcement/301Investigations/Report%20on%20India%E2%80%99s%20Digital%20Services%20Tax.pdf.

[192] YourStory, Equalisation Levy on Online Advertisements to Be Abolished From April 1 (Mar. 2025), https://yourstory.com/2025/03/equalisation-levy-online-advertisements-abolished-google-meta-x-ads.

providers for public services to locate a data center and disaster recovery center within Indonesia.[193] In October 2019, Indonesia passed Regulation No. 71 of 2019 which revoked Regulation No. 82 of 2012. It also relaxed the data localization rules for private electronic system operators, while operators in the public scope must still keep their systems and data in Indonesia. The 2019 regulation requires private Electronic System Operators (ESOs) to register with MCIT prior to their electronic systems being made accessible to users while existing ESOs must register with MCIT within a period of one year. The 2019 Indonesian regulation permits private ESOs to locate electronic systems and data outside of the territory of Indonesia so long as "the location does not diminish the effectiveness of the supervision conducted by a relevant state ministry or institution and law enforcement agencies; and access to the electronic system and electronic data must be provided for the purpose of supervision and law enforcement, in accordance with law." The 2019 regulation incorporates the "right to be forgotten" and requires ESOs to delete electronic information that is within their control and is no longer relevant. Komdigi has also been preparing a revision of Regulation No. 71 of 2019 that would add data classification rules and address government access to electronic systems and data,[194] and we urge USTR to ensure that any revision does not extend localization requirements or authorize broad government access to data without due process.

Issue: Intellectual Property Rights Enforcement

While the Indonesian government has taken steps to improve IPR enforcement, Indonesia continues to present challenges with respect to IPR protections and enforcement mechanisms that translate into a barrier to entry for U.S. small business innovators in the Indonesian market. For example, its revision of Indonesian trademark law in November 2016 demonstrates a positive step forward to advance the rights of trademark holders through shorter examination times and better criteria for protected marks. In addition, Indonesia joined the Madrid Protocol in January 2018.

However, there are still ongoing concerns about whether the recent provisions will be adequately enforced and there has been minimal progress in integrating USTR's suggested reforms in its Special 301 reviews. For example, Indonesia has apparently not yet created a specialized IPR unit within its National Police to enforce against Indonesian criminal syndicates that create counterfeit and pirated marks and works. Indonesia's Patent Law also continues to raise concern. Although a 2020 amendment allowed importation to satisfy the patent working requirement,[195] the 2024 amendments require every patent holder to file an annual statement on whether the invention is worked in Indonesia, and non-working can expose a patent to compulsory licensing or invalidation.[196] In the U.S.-Indonesia Agreement on Reciprocal Trade (ART) signed on February 19, 2026, Indonesia committed to eliminate the local manufacturing and use requirements in its Patent

[193] See Mary R. Silaban, Unleashing Indonesia's Digital Innovation, American Chamber of Commerce in Indonesia (June 10, 2014), available at http://www.amcham.or.id/fe/4614-unleashing-indonesia-s-digital-innovation.

[194] Ministry of Communication and Digital Affairs, Laporan Hasil Evaluasi Peraturan Perundang-Undangan: Peraturan Pemerintah Nomor 71 Tahun 2019 [Evaluation Report on Government Regulation No. 71 of 2019] (2025), https://jdih.komdigi.go.id/dokumen-pembentukan-puu/unduh/87.

[195] Swiss Federal Institute of Intellectual Property, Indonesia Removes Local Manufacturing Requirement from Its Patent Law (Dec. 11, 2020), https://www.ige.ch/en/services/newsroom/news/news-details/indonesia-removes-local-manufacturing-requirement-from-its-patent-law

[196] Asia IP, Indonesia's New Annual SOW Requirement: Compliance Risks and Legal Implications for Patent Holders (Jan. 1, 2026), https://asiaiplaw.com/section/ip-analysts/indonesias-new-annual-sow-requirement-compliance-risks-and-legal-implications-for-patent-holders

Law,[197] and we urge USTR to ensure this commitment is implemented. Certainty in enforcement is lacking and continues to present challenges.

Issue: Indonesian Tariff Codes for "Intangible Goods" (Software and Other Digital Products)

In February 2018, the Indonesian government issued Ministry of Finance Regulation No. 17/PMK.010/2018 on the Second Amendment of Regulation No. 6/PMK.010/2017 on Stipulation of Goods Classification System and Import Duty on Imported Goods (Regulation 17), which went into effect as of March 1, 2018. Regulation 17 provides Chapter 99 as a new addition to the Indonesian tariff system, covering intangible goods ("Software and Other Digital Goods"). While the import duty is currently at 0 percent, ACT remains very concerned at the unprecedented addition of digital goods to a tariff system and fears the precedent Indonesia may create.

We note that Ministry of Finance Regulation No. 190/PMK.04/2022 came into effect on January 13, 2023, introducing a new import declaration procedure for intangible goods. This regulation effectively establishes a customs administrative framework that allows Indonesia to begin collecting duties on intangible goods if it decides to raise the applicable duty rate from zero percent. This change could lead to significant compliance costs and administrative burdens for small businesses operating in Indonesia. Customs authorities have yet to determine the complete implementation of Regulation 190 and the application process for reporting customs data, with additional technical provisions still under development, despite the regulation currently being in effect.

We recognize Indonesia's commitment under the ART to eliminate its existing HTS tariff lines on intangible products, to suspend the requirement to file import declarations for electronic transmissions, and to support a permanent WTO moratorium on customs duties on electronic transmissions.[198] Indonesia has not yet ratified the ART,[199] and we urge USTR to ensure these commitments are followed through on.

Issue: Taxation of Digital Services

On July 1, 2020, the Indonesian government began requiring foreign digital services providers to collect value-added tax (VAT) on digital goods and services sold to Indonesian consumers. Foreign operators are required to remit the collected taxes to the Indonesian government. Indonesia raised its general VAT rate to 12 percent in January 2025 but kept the effective rate on digital subscriptions

[197] Agreement Between the United States of America and the Republic of Indonesia on Reciprocal Trade, Annex III, art. 2.26(f) (Feb. 19, 2026), https://ustr.gov/sites/default/files/files/Press/Releases/2026/02.19.26%20US-IDN%20ART%20Full%20Agreement%20-%20US%20Final%20for%20Website%20sanitized.pdf

[198] Agreement Between the United States of America and the Republic of Indonesia on Reciprocal Trade, art. 3.5 and Annex III, art. 3.1 (Feb. 19, 2026), https://ustr.gov/sites/default/files/files/Press/Releases/2026/02.19.26%20US-IDN%20ART%20Full%20Agreement%20-%20US%20Final%20for%20Website%20sanitized.pdf

[199] Iman Pambagyo, Arianto Patunru & Deasy Pane, The US-Indonesia Agreement on Reciprocal Trade: Three Views on its Economic and Strategic Impacts, ISEAS Perspective 2026/54 (July 27, 2026), https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2026-54-the-us-indonesia-agreement-on-reciprocal-trade-three-views-on-its-economic-and-strategic-impacts-by-iman-pambagyo-arianto-patunru-and-deasy-pane/

at 11 percent.[200] Of greater concern, Law No. 2 of 2020 authorizes an electronic transaction tax on foreign digital service providers and allows the tax authority to treat foreign providers with a "significant economic presence" as permanent establishments, which would function as a digital services tax applied extraterritorially to American service providers.[201] In the ART, Indonesia committed not to impose digital services taxes, or similar taxes, that discriminate against U.S. companies.[202] Until the electronic transaction tax authority is repealed, we urge for U.S. government opposition to it.

Issue: Harmful Digital Platform Regulation

Indonesia's Ministry of Communication and Digital Affairs (Komdigi) continues to develop digital platform regulatory proposals, on which ACT continues to engage. These proposals build on Ministerial Regulation No. 5 of 2020, which requires private electronic system operators to register, to remove prohibited content within 24 hours of a request or within four hours in urgent cases, and to give authorities access to their systems and data, with penalties up to blocking of the service.[203] ACT is concerned that Indonesia may enact EU DMA-like requirements that are barriers to digital trade.

Issue: Cross-Border Data Transfer Restrictions Under the Personal Data Protection Law

On July 16, 2026, Indonesia issued Government Regulation No. 33 of 2026 to implement its 2022 Personal Data Protection Law, and the regulation takes effect in January 2027.[204] The regulation reaches processing outside Indonesia that has legal effects in Indonesia or affects Indonesian citizens abroad. It permits transfers only to countries that a new supervisory authority finds to have equivalent protection, under safeguards such as standard contractual clauses that the authority has yet to issue, or with consent limited to non-repetitive transfers of a limited number of data subjects. The supervisory authority has not yet been established,[205] which leaves U.S. small businesses facing new obligations without the transfer tools needed to meet them. In the ART, Indonesia committed to recognize the United States as providing adequate data protection under Indonesian law.[206] We urge

[200] Bisnis Indonesia, Bukan Barang Pokok, Langganan Netflix Cs Kena PPN 12%? Ini Kata Kemenkeu (Jan. 1, 2025), https://teknologi.bisnis.com/read/20250101/84/1828115/bukan-barang-pokok-langganan-netflix-cs-kena-ppn-12-ini-kata-kemenkeu

[201] Arjuna Dibe, Tackling the Challenges of Digital Tax and BEPS in Indonesia, THE JAKARTA POST (July 29, 2020), https://www.thejakartapost.com/academia/2020/07/29/tackling-the-challenges-of-digital-tax-and-beps-in-indonesia.html

[202] Agreement Between the United States of America and the Republic of Indonesia on Reciprocal Trade, art. 3.1 (Feb. 19, 2026), https://ustr.gov/sites/default/files/files/Press/Releases/2026/02.19.26%20US-IDN%20ART%20Full%20Agreement%20-%20US%20Final%20for%20Website%20sanitized.pdf

[203] Human Rights Watch, Indonesia: Suspend, Revise New Internet Regulation (May 21, 2021), https://www.hrw.org/news/2021/05/21/indonesia-suspend-revise-new-internet-regulation

[204] PPC Land, Data Controllers Face 2% Revenue Fines Under Indonesia's New Data Rules (2026), https://ppc.land/data-controllers-face-2-revenue-fines-under-indonesias-new-data-rules/

[205] Antara, Indonesia to Set Up Independent Personal Data Protection Agency (July 22, 2026), https://en.antaranews.com/news/423673/indonesia-to-set-up-independent-personal-data-protection-agency

[206] Agreement Between the United States of America and the Republic of Indonesia on Reciprocal Trade, art. 3.2(b) and Annex III, art. 3.2 (Feb. 19, 2026), https://ustr.gov/sites/default/files/files/Press/Releases/2026/02.19.26%20US-IDN%20ART%20Full%20Agreement%20-%20US%20Final%20for%20Website%20sanitized.pdf

USTR to press Indonesia to implement that recognition before the regulation takes effect and to accept internationally recognized transfer mechanisms such as the Global Cross-Border Privacy Rules system.

Issue: Mandatory Payments for News Content

In February 2024, Indonesia issued Presidential Regulation No. 32 of 2024 on publisher rights, which requires digital platforms to support quality journalism, including through paid licensing, profit sharing, or other cooperation with news publishers.[207] A pending amendment to the Copyright Law would go further, with an Article 30 that would require digital platforms to pay producers of journalistic works whenever they profit directly or indirectly from that content, including through aggregation, curation, or advertising.[208] These measures fall mainly on U.S. platforms and are inconsistent with Indonesia's commitments in the ART. We urge USTR to press Indonesia to withdraw the payment mandate from the Copyright Law amendment and to ensure the publisher rights regulation is not enforced against U.S. companies.

ITALY

Issue: Digital Services Taxation

Italy currently imposes a 3% DST, and its 2025 Budget Law removed the €5.5 million threshold for Italian digital services revenue, extending the tax to more companies.[209] For reasons discussed above, ACT is significantly concerned with the imposition of DSTs in this key market, and calls for USTR support in opposing it.

JAPAN

Issue: Digital Platform Regulation

Japan has enacted a new law, the Act on Promotion of Competition Related to Specified Software Used on Smartphones (known as the SSCPA or the Mobile Software Competition Act), which took full effect on December 18, 2025.[210] The SSCPA takes a more measured approach than the EU's DMA, with a narrower scope and provisos that allow designated providers to take necessary measures to ensure cybersecurity, protect user information and youth, and prevent crime.[211] However, the SSCPA could still unduly restrict the ability of platforms to curate apps and content,

[207] Cabinet Secretariat of the Republic of Indonesia, Gov't Issues Regulation on Publisher Rights (Feb. 2024), https://setkab.go.id/en/govt-issues-regulation-on-publisher-rights/
[208] The Jakarta Post, Copyright and journalism (July 2, 2026), https://www.thejakartapost.com/opinion/2026/07/02/copyright-and-journalism
[209] Digital Policy Alert, Budget law amending digital services tax enters into force (Law No. 207 of 2024), https://digitalpolicyalert.org/event/26431-budget-law-amending-digital-services-tax-enters-into-force-law-no-207-of-2024
[210] Japan Fair Trade Commission, Subordinate Legislations and Guidelines under the Mobile Software Competition Act (July 29, 2025), https://www.jftc.go.jp/en/pressreleases/yearly-2025/July/250729.html
[211] Japan Fair Trade Commission, Summary of Subordinate Legislations and Guidelines under the Mobile Software Competition Act (tentative translation) (July 29, 2025), https://www.jftc.go.jp/file/250729/MSCA_Subordinate_Legislations_and_Guidelines_tentative_translation_summary.pdf

including with respect to enforcing IPR, as the law contains no exception for compliance for appropriate protection of IPR. The Japan Fair Trade Commission sought comment on the scoping of this law, which ACT provided written comments on.[212] ACT has engaged extensively with relevant Japanese government actors for years, including the Ministry of Internal Affairs and Communications, the Headquarters for Digital Market Competition, and the Japan Fair Trade Commission to emphasize the need for protecting IPR on platforms, and has also raised concerns with the law's conflicts with obligations in both Article 16 of the General Agreement on Trade in Services and other trade agreement obligations.[213] Because the SSCPA stands to inhibit some core platform functions, including those that will protect IPR in the digital economy, we urge USTR to track this development and recommend that it be reflected in the 2027 NTE report as, unless altered, a means of denying adequate and effective protection of IPR (as the SSCPA contains no exception to compliance for protecting IPR), as well as a denial of fair and equitable market access to U.S. small businesses who rely on IPR protections.

Although more measured than the EU's DMA, Japan's regulatory approach still risks undermining the very foundations of the mobile ecosystem—security, privacy, and consumer trust—that app developers rely upon and users expect. By restricting core marketplace management functions, such as app review and consumer-protection screening, the SSCPA weakens the value of curated online marketplaces (COMs) for small and medium-sized firms while specifically targeting U.S. companies that provide these COMs. These changes distort competition between app stores and developers by limiting discoverability and driving up overhead for small businesses. Moreover, by prohibiting key features of the current marketplace framework, the SSCPA shifts costs downward, forcing smaller firms to absorb the compliance costs.

Issue: Artificial Intelligence Regulation

ACT notes that the Japan Fair Trade Commission (JFTC) has examined the competitiveness of generative AI markets, most recently in its April 2026 Report Regarding Generative AI Version 2.0,[214] raising the potential of Japanese government intervention into these nascent and rapidly evolving segments of the economy. We have discouraged such interventions and urged Japan to study the impacts of the hasty intervention made into AI markets by the EU before moving forward.[215] Japan's Act on Promotion of Research, Development and Utilization of AI-Related Technologies, which took full effect on September 1, 2025, focuses on promoting AI rather than imposing new regulatory

[212] See https://actonline.org/wp-content/uploads/App-Assn-Comment-re-JFTC-SSCPA-Scaling-RFI-EN.pdf.
[213] ACT, Comments to JFTC Regarding MSCA Enforcement and Compliance Statements (Mar. 25, 2026), https://actonline.org/post/act-comments-to-jftc-regarding-msca-enforcement-and-compliance-statements/.
[214] Japan Fair Trade Commission, Report Regarding Generative AI Version 2.0 (Apr. 16, 2026), https://www.jftc.go.jp/en/pressreleases/yearly-2026/April/260416.html
[215] ACT, Comments Regarding the Japan Fair Trade Commission's Request for Information and Comments Concerning Generative AI and Competition (Nov. 22, 2024), https://actonline.org/post/re-act-the-app-association-comments-regarding-the-japan-fair-trade-commissions-request-for-information-and-comments-concerning-generative-ai-and-competition/; ACT, Comments Regarding Japan's Basic Plan for Artificial Intelligence (Dec. 9, 2025), https://actonline.org/post/comments-of-act-the-app-association-regarding-japans-basic-plan-for-artificial-intelligence-english-and-japanese-versions/.

obligations,[216] and we urge USTR to encourage Japan to keep this approach and to oppose new Japanese government regulation of AI markets at this time.

Issue: User Information External Transmission Rules

Japan's Ministry of Internal Affairs and Communications (MIC) is considering further measures to secure compliance with the external transmission rules for user information under the Telecommunications Business Act. A draft second report of MIC's User Information Working Group, released for comment in August 2026, proposes periodic compliance surveys, published requests to non-compliant operators, and a handbook of recommended practices that goes beyond legal requirements, and it raises the possibility of browser-level opt-out rules over the medium to long term.[217] ACT submitted comments on the draft in September 2026. Many U.S. small business app developers and website operators rely on third-party analytics and advertising tools, and new expectations that blur the line between legal obligations and voluntary practices would raise their compliance costs in Japan. We urge USTR to monitor this process so that any new measures remain proportionate, clearly separate legal requirements from best practices, and align with international approaches.

KENYA

Issue: Data Localization

The Data Protection (General) Regulations of 2021 mandate the localization of a broad set of data, including data processed for civil registration and legal identity management systems, elections, public finance administration, protected computer systems, early childhood and basic education, and primary or secondary health care.[218] The Regulations require that data falling under these categories be processed through a server and data center located in Kenya, or that at least one serving copy of the data be stored in a data center located in-country.

In addition, Kenya's 2025 Cloud Policy, which took effect in May 2025, requires sensitive categories of public sector data to be hosted in Kenya through government or accredited cloud service providers.[219] In August 2026, the government began implementing the Policy through guidelines under which providers must seek accreditation from a Cloud Adoption Committee that has not yet been established.[220] While framed as a measure to strengthen national infrastructure, the

[216] Cabinet Office of Japan, Act on Promotion of Research, Development and Utilization of AI-Related Technologies (AI Act) (accessed Oct. 19, 2026), https://www8.cao.go.jp/cstp/ai/ai_act/ai_act.html
[217] Ministry of Internal Affairs and Communications, Request for Comments on the User Information Working Group Draft Second Report (Measures for Compliance with the External Transmission Rules for User Information) (Aug. 19, 2026), https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000293.html
[218] Data Protection (General) Regulations, 2021, Legal Notice No. 263, reg. 26 (Dec. 31, 2021), https://www.odpc.go.ke/wp-content/uploads/2024/03/THE-DATA-PROTECTION-GENERAL-REGULATIONS-2021-1.pdf
[219] Digital Policy Alert, Kenya Cloud Policy 2025 Entered into Force, Including Authorisation of Cloud Computing Services (May 2, 2025), https://digitalpolicyalert.org/event/29666-kenya-cloud-policy-2025-entered-into-force-including-authorisation-of-cloud-computing-services
[220] Vincent Owino, Search for Firm to Host Sensitive State Data on Cloud Begins, Business Daily Africa (Aug. 6, 2026), https://www.businessdailyafrica.com/bd/corporate/technology/search-for-firm-to-host-sensitive-state-data-on-cloud-begins-5549208

preference for local storage and local providers risks excluding or disadvantaging foreign suppliers, creating discriminatory barriers to market access that conflict with Kenya's trade commitments and undermine the competitiveness of U.S. cloud and digital service providers.[221]

Issue: Intellectual Property Rights Protection

Kenya has taken steps to strengthen its IP enforcement by updating its copyright and anti-counterfeit legislation, including amendments to the Copyright Act that introduced take-down procedures and protections for internet service providers, and the government is now pursuing a bill to consolidate its IP agencies into a single authority. ACT sees these as positive steps to deter IP infringement in Kenya.[222]

Issue: Digital Platform Competition

In May 2024, the Competition Authority of Kenya (CAK) issued a draft Competition (Amendment) Bill for public comment, in which ACT participated,[223] that would create a framework similar to the EU DMA, discussed above, in an attempt to address concerns with large tech platforms. A revised version, the Competition (Amendment) Bill, 2026, is now before the National Assembly and would introduce a "strategic market position" standard and a "superior bargaining position" standard that does not depend on market power, backed by turnover-based fines and criminal liability.[224] ACT submitted comments on the Bill to the National Assembly in June 2026, and the National Assembly's Departmental Committee on Finance and National Planning reported on the Bill in August 2026.[225] As with DMA, we believe such a move would create barriers to participation in the Kenyan digital economy and stifle innovation and growth, and we urge USTR to raise the Bill in its ongoing trade discussions with Kenya.

Issue: Digital Economy Taxation

In December 2024, Kenya replaced its 1.5 percent digital services tax with a Significant Economic Presence Tax on non-resident providers of services through a digital marketplace, which taxes a deemed profit of 10 percent of gross turnover at 30 percent, for an effective rate of 3 percent of gross

[221] ACT, Comments on the Draft Final National Data Governance Policy (June 5, 2026), https://actonline.org/post/comments-of-the-association-for-competitive-technology-on-the-draft-final-national-data-governance-policy/.
[222] U.S. Department of State, 2026 Investment Climate Statement: Kenya (Sept. 2026), https://www.state.gov/wp-content/uploads/2026/09/701264_2026-Kenya-Investment-Climate-Statement.pdf.
[223] ACT, Comments to the Competition Authority of Kenya on its Draft 2024 Competition Bill (June 11, 2024), https://actonline.org/post/act-the-app-association-comments-to-the-competition-authority-of-kenya-on-its-draft-2024-competition-bill/.
[224] Competition (Amendment) Bill, 2026 (National Assembly Bill No. 4 of 2026), Kenya Gazette Supplement (Feb. 19, 2026), https://new.mzalendo.com/legislative-trends/bills/na/432/
[225] Letter from ACT to the Clerk of the National Assembly of Kenya re Competition (Amendment) Bill, 2026 (June 12, 2026), https://actonline.org/wp-content/uploads/ACT-Letter-re-Kenya-Competition-Bill-2026-12-June-2026-w-appendix.pdf; National Assembly of Kenya, Report on the Consideration of the Competition (Amendment) Bill (National Assembly Bill No. 4 of 2026) (Aug. 12, 2026), https://libraryir.parliament.go.ke/items/3b27a06e-06e8-49cb-ae49-e2055c8d7d57/full

turnover.[226] The Finance Act, 2025 then widened the tax to cover income from services provided through the internet or any electronic network and removed the KES 5 million turnover threshold, so the tax now applies to non-resident providers regardless of size.[227] Because the tax falls only on non-resident providers and is levied on gross turnover rather than actual profit, it discriminates against U.S. small business technology developers, many of whom earn modest revenue in Kenya and now face registration and monthly filing obligations from their first sale. We urge USTR to include this tax in the 2027 NTE report and to seek its removal in the ongoing U.S.-Kenya reciprocal trade negotiations, which cover digital trade.[228]

MALAYSIA

Issue: Network Operation Fees

The Malaysian government intends to implement a Universal Service Provision (USP) Fund contribution for Cloud Service Providers (CSPs). This new requirement, slated to take effect in 2026, marks a significant departure from its previous policy and would affect the competitiveness of cloud services in Malaysia, impacting their availability and cost to small businesses. In the U.S.-Malaysia Agreement on Reciprocal Trade (ART) signed on October 26, 2025, Malaysia committed not to require U.S. social media platforms and cloud service providers to pay into its domestic fund.[229] The ART has not yet entered into force,[230] and we urge USTR to ensure that Malaysia implements this commitment and does not apply the USP contribution to U.S. providers.

Issue: Intellectual Property Rights Enforcement

Concerns persist regarding intellectual property matters, including the prevalence of pirated copyright and counterfeit trademark products, as well as the absence of suitable U.S.-style safe harbors to facilitate the efficient removal of infringing or problematic content.

Issue: Digital Platform Regulation

The Malaysia Competition Commission (MyCC) is actively engaged in advancing new regulation of digital platforms under the Competition Act 2010. Conducted from mid-2024 to late 2025, the review focuses on five strategic sectors: mobile operating and payment systems, e-commerce

[226] U.S. Department of State, 2026 Investment Climate Statement: Kenya (Sept. 2026), https://www.state.gov/wp-content/uploads/2026/09/701264_2026-Kenya-Investment-Climate-Statement.pdf; Kenya Nets Sh2.3 Billion from International Digital Service Providers, Eastleigh Voice (Sept. 27, 2025), https://eastleighvoice.co.ke/digital%20economy/217251/kenya-nets-sh2-3-billion-from-international-digital-service-providers

[227] PwC, Worldwide Tax Summaries, Kenya: Corporate - Taxes on Corporate Income (2026), https://taxsummaries.pwc.com/kenya/corporate/taxes-on-corporate-income

[228] Kenya, US Hold First Round of Talks on Reciprocal Trade Framework, The Star (Feb. 27, 2026), https://www.the-star.co.ke/business/2026-02-27-kenya-us-hold-first-round-of-talks-on-reciprocal-trade-framework

[229] The White House, Joint Statement on United States-Malaysia Agreement on Reciprocal Trade (Oct. 26, 2025), https://www.whitehouse.gov/briefings-statements/2025/10/joint-statement-on-united-states-malaysia-agreement-on-reciprocal-trade/

[230] Ministry of Investment, Trade and Industry, Agreement on Reciprocal Trade between Malaysia and the United States (last updated May 22, 2026), https://www.miti.gov.my/index.php/pages/view/ART

marketplaces, digital advertising services, online travel agencies, and data privacy as a cross-cutting issue. MyCC published the report of its review on February 10, 2026,[231] proposing 12 targeted and six general recommendations, including new subsector guidelines for mobile operating and payment systems and an expansion of payment system regulation to cover integrated app store payments.[232] ACT has advocated on the review extensively,[233] emphasizing the impact on the small business technology innovator community. We continue to work with MyCC and the Malaysian government to avoid the adoption of harmful ex ante EU DMA-like requirements being imposed on the ecosystem.

Issue: Artificial Intelligence Regulation

Malaysia's National AI Office (NAIO) has introduced a Sovereign AI Strategy featuring a tiered governance approach with strict requirements around compute infrastructure, data residency, and operational workflows, especially for sensitive government workloads. The strategy includes plans for government-owned cloud and compute capabilities for the highest tier (L3) workloads and introduces sovereignty certification requirements, even when collaborating with global companies. The new mandates raise concerns about possible market entry barriers and favoritism toward domestic firms. The strict rules for managing sensitive government data, along with enhanced certification and audit standards, would increase compliance burdens and operational costs for small U.S. companies in Malaysia. The government is also implementing a National Sovereign AI Cloud intended to keep sensitive government information beyond the reach of foreign laws,[234] and the tender to build it was open only to companies incorporated and licensed in Malaysia.[235] The Ministry of Digital also expects to table an AI Governance Bill in Parliament by the first quarter of 2027.[236] ACT has urged Malaysia to keep any AI legislation risk-based and grounded in existing law, and we ask USTR to ensure that sovereign cloud and AI measures do not exclude U.S. providers on the basis of nationality.

---

[231] Malaysia Competition Commission, Market Review on the Digital Economy Ecosystem under the Competition Act 2010 (Feb. 10, 2026), https://www.mycc.gov.my/market-review

[232] Malaysia Competition Commission, Public Summary, Market Review on the Digital Economy Ecosystem under the Competition Act 2010 (2026), https://www.mycc.gov.my/sites/default/files/pdf/newsroom/Public%20Summary%20-%20Market%20Review%20on%20the%20Digital%20Economy%20Ecosystem%20under%20the%20Competition%20Act%202010.pdf

[233] ACT, Comments to the Malaysia Competition Commission re Public Consultation for Interim Report, Market Review of the Digital Economy Ecosystem Under the Competition Act 2010 (Mar. 31, 2025), https://actonline.org/post/comments-of-act-the-app-association-to-the-malaysia-competition-commission-mycc-re-public-consultation-for-interim-report-market-review-of-the-digital-economy-ecosystem-under-the-competition-act-2/; ACT, Comments to the Malaysia Competition Commission for Market Review on the Digital Economy Ecosystem Under the Competition Act 2010 (Sept. 14, 2025), https://actonline.org/post/act-the-app-association-comments-to-the-malaysia-competition-commission-for-market-review-on-the-digital-economy-ecosystem-under-the-competition-act-2010/.

[234] Bernama, Sovereign AI Cloud Crucial to Protecting Country's Digital Sovereignty - Fahmi (Oct. 14, 2026), https://www.bernama.com/en/general/news.php?id=2620518

[235] Malaysian Communications and Multimedia Commission, Pre-Qualification Document for Tender for the Design, Development and Operation of a National Sovereign AI Cloud Infrastructure, Tender Ref. MCMC/NSAICO(01)/CLOUD/TC/05/2026(05) (May 2026), https://www.mcmc.gov.my/skmmgovmy/files/7d/7d797d5c-d610-4733-acc6-c6dd67a532a2.pdf.

[236] Bernama, AI Governance Bill Expected to Be Tabled in Parliament by Q1 2027 at the Latest - Gobind (Sept. 10, 2026), https://www.bernama.com/en/general/news.php?id=2605398

Issue: Encryption and Cybercrime Legislation

Malaysia's Cybercrimes Bill 2026, which the National Cyber Security Agency (NACSA) will implement, raises concerns for developers that rely on strong commercial encryption to protect their users. In August 2026, ACT wrote to NACSA urging that implementation of the bill not require developers to weaken encryption or build exceptional access mechanisms, and that any obligations be proportionate for micro, small, and medium-sized enterprises.[237] Measures that weaken encryption would expose U.S. small businesses and their customers to greater security risks and would sit uneasily with Malaysia's ART commitment to cooperate with the United States on cybersecurity and to promote international standards.[238] We urge USTR to engage Malaysia to ensure that its cybercrime framework preserves strong encryption.

MEXICO

Issue: Intellectual Property Rights Enforcement

Intellectual property laws in Mexico have made significant improvements but lag behind the rest of the world on protection and enforcement. Mexico's accession to the U.S.–Mexico–Canada Agreement (USMCA) and the WIPO Internet Treaties (WIPO Copyright Treaty [WCT] and the WIPO Performances and Phonograms Treaty [WPPT]) has strengthened both their Federal Copyright Law and Federal Criminal Code. This significant progress was met with constitutional challenges that we were encouraged were rejected by the Mexican Supreme Court. While these reforms were upheld as constitutional, we now urge USTR to encourage the Government of Mexico to fully implement them without further delay by issuing the corresponding implementing regulations by the Minister of Culture and the Copyright Office. If these laws are overturned, Mexico will be a jurisdiction for significant IP abuse. ACT therefore encourages USTR to consider this issue in the 2027 NTE report.

Issue: Regulatory Independence in Telecommunications and Digital Services

Mexico's 2025 Law on Telecommunications and Broadcasting replaced the autonomous Federal Telecommunications Institute (IFT) with a Telecommunications Regulatory Commission (CRT) that sits within the executive branch's Agency for Digital Transformation and Telecommunications (ATDT), and the Senate ratified the CRT's commissioners in October 2025.[239] During the legislative process, a draft provision would have allowed the ATDT to block digital platforms without a court order, and experts warned that this power and the loss of an independent regulator could conflict with Mexico's USMCA commitments on digital trade and telecommunications.[240] Placing telecommunications and digital oversight in an agency the executive controls reduces regulatory predictability for U.S. technology companies of all sizes. ACT asks USTR to use the USMCA joint

[237] Association for Competitive Technology, Letter to the National Cyber Security Agency on Implementation of the Cybercrimes Bill 2026 (Aug. 31, 2026), https://actonline.org/post/association-for-competitive-technology-to-nacsa-re-malaysia-cybercrimes-bill-2026-implementation/

[238] Agreement Between the United States of America and Malaysia on Reciprocal Trade, art. 3.2(c) (Oct. 26, 2025), https://ustr.gov/sites/default/files/files/agreements/ARTs/MALAYSIA%20ART.pdf

[239] Expansión, Senado ratifica a la CRT, que sustituye al IFT (Oct. 14, 2025), https://expansion.mx/tecnologia/2025/10/14/senado-ratifica-crt-sustituye-ift-quien-dirige

[240] El Financiero, Incumple reforma en telecomunicaciones los acuerdos del T-MEC (Apr. 28, 2025), https://www.elfinanciero.com.mx/empresas/2025/04/28/incumple-reforma-en-telecomunicaciones-los-acuerdos-del-t-mec/

review to secure Mexico's commitment to independent, transparent regulators and to non-discriminatory treatment of digital services.

NEPAL

Issue: Digital Services Tax

Since July 2022, Nepal has applied a 2 percent digital services tax to listed digital services that non-resident companies provide to consumers in Nepal.[241] The tax applies only to non-resident suppliers, is inconsistent with international tax principles, and adds a separate registration, payment, and reporting burden that falls hardest on small U.S. developers selling apps and digital services into Nepal. We urge USTR to press Nepal to repeal the tax and to include it in the 2027 NTE report.

Issue: Social Media Registration and Platform Blocking

On September 4, 2025, Nepal ordered the blocking of 26 social media and messaging platforms that had not registered with the Ministry of Communication and Information Technology, and it lifted the order days later after deadly protests.[242] Local registration requirements enforced through the sudden blocking of entire services create serious uncertainty for U.S. small business technology developers that offer communications features. We urge USTR to press Nepal to avoid registration mandates that serve as a precondition for market access and to rule out blocking entire services as an enforcement tool.

NEW ZEALAND

Issue: Digital News Bargaining

New Zealand's Fair Digital News Bargaining Bill, introduced in August 2023, would require large digital platforms to bargain with New Zealand news publishers over the use of news content.[243] The bill has not been enacted, but Australia's August 2026 enactment of a charge on platforms that do not reach agreements with publishers may prompt New Zealand to revive or expand it. ACT is concerned that mandatory bargaining frameworks of this kind fall primarily on U.S. companies, and we ask USTR to monitor the bill and urge New Zealand not to adopt a mandatory bargaining scheme or charge.

Issue: Digital Services Taxation

[241] Inland Revenue Department of Nepal, Digital Service Tax (directives and procedures) (accessed Oct. 19, 2026), https://ird.gov.np/category/digitalservicetax/.
[242] JURIST, Nepal blocks 26 social media platforms in historic crackdown (Sept. 2025), https://www.jurist.org/news/2025/09/nepal-blocks-26-social-media-platforms-in-historic-crackdown/; Gulf News, Social media ban triggers deadly street protests in Nepal (Sept. 2025), https://gulfnews.com/world/asia/social-media-ban-triggers-deadly-street-protests-in-nepal-1.500261179.
[243] Manatū Taonga Ministry for Culture and Heritage, Fair Digital News Bargaining Bill, https://www.mch.govt.nz/fair-digital-news-bargaining-bill

ACT welcomes the New Zealand government's May 2025 decision to discharge its Digital Services Tax Bill from the legislative program.[244] We ask USTR to encourage New Zealand to maintain this position and to refrain from adopting any unilateral digital services tax.

NIGERIA

Issue: Data Localization & Nigerian Workforce Requirements

The Nigerian government enacted "Guidelines for Nigerian Content Development in Information and Communications Technology,"[245] which raise a myriad of concerns for our members. The Nigerian government imposes data localization requirements on multinational companies. For instance, section 10.3 of the Nigerian government's guidelines mandates multinational companies to not only store their data in Nigeria but also requires such companies to incorporate 50 percent of local products when manufacturing ICT devices in the region. Additionally, it requires companies to hire local engineers when manufacturing such products. More recently, the National Information Technology Development Agency (NITDA) issued a National Cloud Computing Guideline in August 2026, alongside the government's new National Digital Cloud Policy, that sorts government and regulated data into four levels and requires the most sensitive "classified" tier to be hosted only in Nigeria, with the rules taking effect on January 1, 2027,[246] and its Director General stated in September 2026 that defense information, financial transaction records, health care information, and citizens' personal data should remain within Nigeria's borders.[247] We urge USTR to press Nigeria to narrow its cloud and sovereign data policies so that they do not operate as broad localization mandates.

Issue: Cross-Border Data Transfers

Nigeria's Data Protection Act of 2023 and the Nigeria Data Protection Commission's (NDPC) 2025 General Application and Implementation Directive (GAID) add conditions that burden cross-border data flows. The GAID calls for consent before personal data is transferred to a country without an NDPC adequacy decision, treats cross-border transfers as a trigger for a data protection impact assessment filed with the NDPC, and lists the risk of transfers outside Nigeria as a factor in designating data controllers of major importance.[248] The NDPC has also enforced these rules against U.S. firms, issuing a $32.8 million remedial fee against Meta in February 2025 that cited, among other things, unauthorized transfers of Nigerians' data abroad, before the matter was settled in November

[244] Hon Simon Watts, Discharge of Digital Services Tax Bill (May 20, 2025), https://www.beehive.govt.nz/release/discharge-digital-services-tax-bill

[245] NITDA, Guidelines for Nigerian Content Development in Information and Communications Technology (2017).

[246] NITDA, National Cloud Computing Guideline 2026 (Aug. 4, 2026), https://nitda.gov.ng/wp-content/uploads/2026/08/NCCG-Final-signed.pdf; Federal Ministry of Communications, Innovation and Digital Economy, Federal Government Unveils National Digital Cloud Policy to Drive Investment, Digital Sovereignty and Government Transformation (Aug. 17, 2026), https://fmcide.gov.ng/?p=4175.

[247] NITDA, GITEX 2026: Nigeria's Digital Future Depends on Local Infrastructure, Skills, Innovation - NITDA DG (Sept. 15, 2026), https://nitda.gov.ng/gitex-2026-nigerias-digital-future-depends-on-local-infrastructure-skills-innovation-nitda-dg/9807/

[248] NDPC, Nigeria Data Protection Act 2023 General Application and Implementation Directive (GAID) 2025, arts. 8(3)(b), 18(1)(e), 28(3)(o) (2025), https://ndpc.gov.ng/wp-content/uploads/2025/07/NDP-ACT-GAID-2025-MARCH-20TH.pdf

2025.[249] These requirements raise compliance costs for U.S. small business technology developers that rely on cloud services located outside Nigeria. We urge USTR to press Nigeria to recognize a full range of transfer mechanisms and to avoid using transfer rules to localize data.

Issue: Digital Economy Taxation

Since 2020, Nigeria has been assessing taxes on non-resident companies based on their commerce over the internet/on digital platforms. The Nigeria Tax Act, 2025, signed in June 2025, carries this significant economic presence rule forward, treating a non-resident digital business as taxable in Nigeria if it earns at least NGN 25 million from Nigeria in a year, uses a .ng domain, or prices its products in naira, and setting a minimum tax of 4 percent of its Nigerian-source income where no withholding tax applies.[250] We have significant concerns with this tax, which discriminates against non-resident providers and undermines the OECD's work toward a consensus solution for digital economy taxation. We urge USTR to include this development in the 2027 NTE report and to work with the Nigerian government to mitigate its damage and influence in the region.

Issue: Platform Local Incorporation and Content Takedown Requirements

NITDA's Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries, issued in 2022, requires platforms with more than one million registered users in Nigeria to incorporate in Nigeria, maintain a physical address in the country, and appoint a liaison officer to the government. All platforms must also acknowledge and remove content reported as unlawful by an authorized government agency within 48 hours.[251] NITDA continues to monitor and report on platform compliance with the Code.[252] Local incorporation mandates and short government-directed takedown deadlines raise costs and legal risk for the U.S. platforms that distribute the apps and services of U.S. small business technology developers. We urge USTR to press Nigeria to withdraw the local incorporation requirement and to align takedown obligations with due process and international norms.

Issue: Discriminatory Competition and Consumer Protection Enforcement

In 2024, the Federal Competition and Consumer Protection Commission (FCCPC) fined Meta and WhatsApp $220 million over their privacy and data practices, and in 2025 the Competition and

[249] $32.8 Million Fine Dispute: Meta Settles with Nigerian Govt Out of Court, Premium Times (Nov. 3, 2025), https://www.premiumtimesng.com/news/headlines/832580-32-8-million-fine-dispute-meta-settles-with-nigerian-govt-out-of-court.html

[250] Tinubu Signs Nigeria's Tax Reform Bills into Law, Premium Times (June 26, 2025), https://www.premiumtimesng.com/news/top-news/803455-tinubu-signs-nigerias-tax-reform-bills-into-law.html; PwC, Worldwide Tax Summaries, Nigeria: Corporate - Taxes on Corporate Income (May 29, 2026), https://taxsummaries.pwc.com/nigeria/corporate/taxes-on-corporate-income

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

[252] NITDA, Compliance with Laws and Misinformation Management: An Analysis of Compliance with Laws and Misinformation Management by Social Media Platforms in Nigeria (Dec. 2024), https://nitda.gov.ng/wp-content/uploads/2024/12/NITDA24-COP-REPORT-JNT-compressed.pdf

Consumer Protection Tribunal largely upheld that decision, which Meta has appealed.[253] In July 2026, the President directed the FCCPC to investigate Meta, Google, X, and certain generative AI platforms following a petition by Nigerian media organizations, including whether news content was used to train AI models without authorization and whether media organizations were denied a fair opportunity to negotiate compensation, and the FCCPC pointed to South Africa's news media remedies as a reference.[254] ACT is concerned that this inquiry could lead to compelled payments for news content and restrictions on AI development that single out U.S. firms. We urge USTR to monitor the investigation closely and to press Nigeria to ensure that any enforcement is evidence-based, nondiscriminatory, and consistent with due process.

Issue: Intellectual Property Rights Protection

While Nigeria has taken steps towards improving its IP protections,[255] Nigerian enforcement agencies lack the resources needed to effectively enforce IP rights.

PAKISTAN

Issue: Data Localization

ACT notes that Pakistan has released a new draft of the "Personal Data Protection Bill," which remains pending.[256] This updated version maintains the ban on the cross-border transfer of a vaguely defined category of "critical" personal data. The draft bill also proposes the establishment of a National Commission for Personal Data Protection, which would have broad authority to create new regulatory frameworks and access data.

Additionally, in 2022, Pakistan introduced a Cloud First Policy that imposes data localization requirements on various broad categories of data, including "restricted," "sensitive," and "secret."[257] In June 2026, the Ministry of Information Technology and Telecommunication also released a draft Data Governance Policy that would require federal public bodies, and the contractors and service providers that handle government data for them, to host, store, and process all personal data and all restricted and confidential government data within Pakistan, and would treat remote access from

[253] Nigeria Rebuffs Meta's Threat to Quit Country over Data Privacy Fines, Premium Times (May 4, 2025), https://www.premiumtimesng.com/news/headlines/792079-nigeria-rebuffs-metas-threat-to-quit-country-over-data-privacy-fines.html

[254] Tinubu Directs FCCPC to Investigate Meta, Google, X, AI Platforms over Media Complaints, Premium Times (July 6, 2026), https://www.premiumtimesng.com/business/business-news/893409-tinubu-directs-fccpc-to-investigate-meta-google-x-ai-platforms-over-media-complaints.html

[255] See USTR, 2019 National Trade Estimate Report on Foreign Trade Barriers (2019) ("In 2017, Nigeria submitted its instruments of accession and ratification of four World Intellectual Property Organization (WIPO) treaties: the WIPO Copyright Treaty, the WIPO Performances and Phonograms Treaty, the Marrakesh Treaty, and the Beijing Treaty").

[256] Ministry of Information Technology and Telecommunication, Personal Data Protection Bill May 2023 (Draft), https://moitt.gov.pk/SiteImage/Legislations/Final%20Draft%20Personal%20Data%20Protection%20Bill%20May%202023%20(1).pdf.

[257] Ministry of Information Technology and Telecommunication, Pakistan Cloud First Policy (Feb. 2022), https://moitt.gov.pk/SiteImage/Policies/Pakistan%20Cloud%20First%20Policy-Final-25-02-2022%20(1).pdf.

abroad as a cross-border transfer that needs approval from the Pakistan Digital Authority.[258] In the financial sector, the State Bank of Pakistan (SBP) prohibits financial institutions from storing and processing core workloads on offshore cloud services. These data localization requirements do not effectively enhance data protection while making it more difficult to enter the market and raising costs for ACT members.

Issue: Social Media Regulation and Content Blocking

In January 2025, Pakistan amended its Prevention of Electronic Crimes Act to create a Social Media Protection and Regulatory Authority with power to require social media platforms to enlist with it, to order the removal or blocking of content on broad grounds that include content against the "ideology of Pakistan" and information it considers false, and to block a platform partially or fully until it complies, and the amendments also made spreading false information a crime punishable by up to three years in prison.[259] Because the law defines a social media platform to include any service that lets users create accounts or share content, it reaches app developers well beyond large social networks. These requirements raise compliance costs and legal risk for U.S. small business technology developers that offer messaging or user-generated content features in Pakistan. We urge USTR to press Pakistan to narrow these powers and to provide clear procedures and independent review before any blocking order.

Issue: Taxes on Foreign Digital Vendors

Pakistan's budget for fiscal year 2025-26 introduced a 5 percent tax on foreign vendors that sell goods and services to Pakistani customers through digital means.[260] The Federal Board of Revenue exempted goods and services supplied from outside Pakistan from the tax in July 2025, retroactive to its July 1 start date, but left the underlying law in place.[261] A tax that applies only to non-resident suppliers discriminates against U.S. digital exporters, adds a separate registration and payment burden that falls hardest on small developers, and is inconsistent with international tax principles. We urge USTR to press Pakistan to repeal the tax formally and to confirm that it will not apply to U.S. suppliers, and to include it in the 2027 NTE report.

PAPUA NEW GUINEA

Issue: Data Localization and Sovereign Hosting

In August 2026, Papua New Guinea's Department of Information and Communications Technology (DICT) consulted on a draft Data Governance and Data Protection Bill 2026, which addresses cross-

[258] Ministry of Information Technology and Telecommunication, Data Governance Policy 2026 (Draft, June 26, 2026), https://moitt.gov.pk/SiteImage/Policies/Data%20Governance%20Policy%20June%202026.pdf.
[259] Prevention of Electronic Crimes (Amendment) Act, 2025 (Act No. II of 2025), Gazette of Pakistan (Jan. 29, 2025), https://www.na.gov.pk/uploads/documents/679b243193585_457.pdf.
[260] Business Recorder, Rs17.6trn FY26 Budget Unveiled Under the Shadows of IMF Conditions, US Tariff Tensions and War Threat (June 10, 2025), https://www.brecorder.com/news/40367135/rs176trn-fy26-budget-unveiled-under-the-shadows-of-imf-conditions-us-tariff-tensions-and-war-threat.
[261] The Express Tribune, Pakistan Removes Hurdle in Trade Deal with US (July 30, 2025), https://tribune.com.pk/story/2558726/pakistan-removes-hurdle-in-trade-deal-with-us; Arab News Pakistan, Pakistan Withdraws Digital Tax on Foreign Online Purchases (July 31, 2025), https://www.arabnews.pk/pakistan/pakistan-withdraws-digital-tax-on-foreign-online-purchases-2610121.

border transfers and sovereign hosting and sought views on approved sovereign environments and localization requirements.[262] DICT's draft National Sovereign Artificial Intelligence and Digital Transformation Strategy would keep critical government systems, sensitive citizen data, and nationally significant data in trusted sovereign environments or equivalent arrangements, and calls for a National AI Act that would include registration of high-risk systems.[263] ACT filed comments on both in September 2026. Broad sovereign hosting or localization mandates would raise costs for U.S. small businesses offering cloud-based services in Papua New Guinea and limit access to secure international services. We ask USTR to encourage Papua New Guinea to rely on interoperable transfer mechanisms rather than localization and to keep any AI framework risk-based and grounded in existing law.

PERU

Issue: Proposed OTT Regulation

Peru's Organismo Supervisor de la Inversion Privada en Telecomunicaciones (OSIPTEL) has initiated a consultation on the potential implications of the framework for regulating over-the-top (OTT) services and applications, posing the potential of network fees and other onerous requirements on innovative OTT services that ACT members offer. Consistent with our views above, ACT has significant concerns with the potential of such a regime being imposed in Peru, and we have provided our detailed views to OSIPTEL. We are continuing to engage with the Peruvian government and believe this development should be included in the 2027 NTE report.

PHILIPPINES

Issue: Data Localization Mandate

In July 2026, President Marcos issued Executive Order No. 119, which establishes a data residency framework requiring Top Secret and Secret government data to be stored in the Philippines and allowing Confidential data to be stored offshore only with the express prior approval of a new Joint Oversight Committee for Data Classification, whose implementing guidelines will determine how strictly these rules apply in practice.[264] Legislative moves parallel this trend, including a last-minute addition to the Konektadong Pinoy Act (formerly the Open Access in Data Transmission Act), which took effect in September 2025 and directs the Department of Information and Communications Technology (DICT) to craft policies to safeguard local data, although the law also gives primacy to

[262] Department of Information and Communications Technology, Data Governance and Data Protection Bill 2026, Consultation Notice (Aug. 2026), https://www.ict.gov.pg/Draft%20Bill/Data_Governance_and_Data_Protection_Bill_2026_Consultation_Notice.pdf

[263] Department of Information and Communications Technology, National Sovereign Artificial Intelligence and Digital Transformation Strategy (draft v15, 2026), https://www.ict.gov.pg/wp-content/uploads/2026/03/National-Sovereign-AI-Strategy-v15.pdf

[264] Executive Order No. 119, s. 2026, Updating the Government Data Classification, Establishing a Data Residency Framework, and for Other Purposes, https://www.lawphil.net/executive/execord/eo2026/eo_119_2026.html; PTV News, PBBM Modernizes Outdated Gov't Data Classification Framework (July 16, 2026), https://ptvnews.ph/pbbm-modernizes-outdated-govt-data-classification-framework/.

cross-border data flows.[265] ACT remains concerned with continued developments in this space, and urges USTR's attention to them in the 2027 NTE report.

POLAND

Issue: Intellectual Property Rights Enforcement

Poland's treatment of enforcement against online piracy is concerning to ACT members, particularly due to the nation continuing not to implement significant provisions of EU directives, including Article 8(3) of the EU Copyright Directive (2001/29/EC) requiring Member States to ensure injunctive relief is available "against intermediaries whose services are used by a third party to infringe a copyright or related right."

Issue: Digital Services Taxation

In 2026, Poland's Ministry of Digital Affairs proposed a DST of up to 3 percent that would apply to companies with global digital services revenue above €1 billion and Polish revenue above PLN 25 million,[266] and the Ministry of Finance has since taken up work on the proposal.[267] These thresholds would place the burden mainly on U.S. companies. For reasons discussed above, ACT is significantly concerned with the imposition of DSTs in this key market and calls for USTR support in opposing it.

REPUBLIC OF KOREA

Issue: Discriminatory Digital Platform Regulation Policies

ACT remains deeply concerned about the Republic of Korea's escalating use of competition policy and proposed ex-ante regulation to target U.S. digital firms and distort healthy competition in the online platform economy, despite bipartisan opposition from U.S. policymakers including explicit warnings from President Trump.

Both the Korean National Assembly and the Korea Fair Trade Commission (KFTC) continue to pursue government interventions into the operation of U.S.-based digital platforms that, among other consequences, would undermine small businesses' access to competitive and secure app ecosystems. Specifically, the Korean National Assembly continues to pursue sweeping regulatory initiatives modeled on the EU's DMA, including the proposed Online Platform Monopoly Act (OPMA), the Fairness in Online Platform Brokerage Transactions Act ("Fairness Act"), and several bills focused on the food delivery sector.[268] These bills would "pre-designate" major U.S. platforms (e.g., Google, Apple, Meta, Coupang) through arbitrary market thresholds, compelling disclosure of proprietary algorithms and even source code, while exempting powerful domestic conglomerates

[265] Republic Act No. 12234, Konektadong Pinoy Act (Aug. 24, 2025), https://batasnatin.com/laws/ra-12234
[266] Bloomberg Tax, Polish Ministry Asks Government to Take Up Digital Services Tax (Jan. 29, 2026), https://news.bloombergtax.com/daily-tax-report/polish-ministry-asks-government-to-take-up-digital-services-tax
[267] bne IntelliNews, Poland to advance 3% digital tax despite US criticism (May 14, 2026), https://www.intellinews.com/poland-to-advance-3-digital-tax-despite-us-criticism-442818/
[268] https://www.techpolicy.press/digital-regulation-is-no-longer-just-domestic-policy-as-korea-and-us-clash-over-new-law/

and, in practice, favoring Chinese platforms. Coupled with the KFTC's "Platform Bureau,"[269] these efforts mark a sharp departure from Korea's evidence-based competition tradition and threaten to chill innovation, raise compliance costs for small developers, and reduce consumer choice. Alarmingly, many of these proposals focus on specific sectors and set arbitrary revenue and user-base thresholds to target successful U.S. companies while exempting most Korean conglomerates and sparing Chinese tech giants operating in the Korean market from comparable scrutiny.

The "Fairness Act," in particular, problematically singles out online platform intermediaries for supposedly exercising a superior bargaining position over business users and using this position to implement unfair trade practices.[270] By narrowing the scope to this single sector, it is tailor-made to disproportionately cover a substantial number of innovative U.S. companies, including Google, Apple, Coupang, Meta, Netflix, Uber, and potentially others, while ignoring other sectors where Korean conglomerates have a well-documented dominant position in the Korean economy.[271]

Though the legislation in theory captures a greater number of companies than the OPMA due to lower proposed financial thresholds, it would still, in practice, give Chinese competitors a free pass since the companies in scope (e.g., Temu, Shein, Alibaba) have a history of deceptive practices, including misrepresenting business data and corporate revenues. Alibaba also has "self-regulatory" arrangements with the KFTC, which raises legitimate questions about whether they would be targeted to the same degree as the many American firms in scope.

We continue to be concerned about proposed regulations that target foreign-headquartered companies, rely on price controls and fee caps, and undermine free-market competition. This type of market intervention will force platforms to scale back popular consumer benefits, which would ultimately harm the small businesses they seek to protect.[272]

Beyond specific legislation like the Fairness Act and OPMA, KFTC Chair Ju Byung-ki has continued to push for online platform legislation and rejected valid concerns that the pending bills target U.S. companies.[273] In the November 2025 U.S.-Korea Joint Fact Sheet, Korea committed to ensure that U.S. companies are not discriminated against and do not face unnecessary barriers in laws and policies concerning digital services, including network usage fees and online platform regulations.[274] As such, ACT urges the U.S. government to hold Korea to this commitment, to ensure that Korea's competition and digital-platform policies are applied transparently and without discrimination, and

---

[269] https://n.news.naver.com/mnews/article/214/0001428922?sid=154

[270] ACT, Letter to USTR and Commerce Urging Action on Korea's Digital Platform Regulation (Mar. 13, 2026), https://actonline.org/post/act-the-app-association-letter-to-ustr-and-commerce-urging-action-on-koreas-digital-platform-regulation/.

[271] https://www.nytimes.com/2023/12/18/business/chaebol-south-korea.html

[272] Ko Dong-hwan, *Delivery Fee Cap Risks Shifting Costs to Riders, Consumers*, Korea Times (Oct. 13, 2026), https://www.koreatimes.co.kr/business/companies/20261013/delivery-fee-cap-risks-shifting-costs-to-riders-consumers; *배달 수수료 관련 여야 법안 3건 계류… 중개·결제수수료·광고비 15% 상한* [Three Bills on Delivery Fees Pending, Capping Brokerage, Payment, and Advertising Fees at 15%], CEO Score Daily (Oct. 14, 2026), https://ceoscoredaily.com/page/view/2026101416510899041.

[273] Korea Herald, FTC chief rejects US concerns over online platform bill (Jan. 9, 2026), https://www.koreaherald.com/article/10652330

[274] The White House, Joint Fact Sheet on President Donald J. Trump's Meeting with President Lee Jae-myung (Nov. 13, 2025), https://www.whitehouse.gov/fact-sheets/2025/11/joint-fact-sheet-on-president-donald-j-trumps-meeting-with-president-lee-jae-myung/

to prioritize updates to Chapter 16 of KORUS or equivalent USMCA-style provisions to prohibit regulatory practices that unfairly target U.S. firms and stifle the global digital economy.

Issue: Competition Law Enforcement

The Korea Fair Trade Commission (KFTC) under Chairman Ju has increasingly relied on aggressive and unpredictable enforcement tools, such as dawn raids, threats of criminal prosecution for practices considered lawful elsewhere, and record-setting penalties, creating significant uncertainty for U.S. small technology firms. These measures, often lacking transparent due process or clear evidentiary bases, have produced unjustified investigations and constrained legitimate business operations.

Recent KFTC actions against U.S. firms over platform integration, network usage fees, and subscription-cancellation features exemplify a troubling trend toward enforcement that disadvantages foreign innovators while granting broad leeway to domestic and Chinese competitors. Such actions not only burden U.S. market entrants with disproportionate compliance costs but also risk contravening Korea's obligations under the KORUS FTA.

Notably, a study by the Competere Foundation (October 2026) finds that Korea's regulatory and antitrust policies targeting U.S. companies could cost the United States and Korea more than $1 trillion in combined economic losses over the next decade—up to $646 billion in the U.S. alone.275 These findings underscore how Korea's KFTC and digital trade bills undermine U.S. innovation, exports, and small-business access to Asia, running directly counter to President Trump's agenda to eliminate non-tariff barriers, expand digital exports, and secure reciprocal market access for U.S. firms. ACT's 2026 APAC Competition report also finds Korea as one of highest risk in terms of discriminatory digital platform regulations in the region. Addressing these policies would strengthen U.S.–Korea supply-chain resilience and advance the administration's Indo-Pacific trade objectives.

U.S. industry concerns about KFTC's targeting of American companies have been heightened by the appointment of Ju Byung-ki as KFTC Chairman in September 2025, who has expressed views critical of U.S. trade policy and rejected U.S. government criticism of KFTC actions.[276] We urge USTR to monitor closely whether such views inform KFTC investigations and enforcement against U.S. companies.

ACT therefore encourages USTR to launch a review of KFTC enforcement under President Lee and Chairman Ju to identify discriminatory or politically motivated patterns. Moreover, USTR can leverage Section 301 and KORUS trade mechanisms to ensure that Korea's competition policy does not become an instrument of anti-U.S. economic nationalism.

Issue: Intellectual Property Rights Enforcement

Korea continues to propose ill-advised regulations for digital platforms that would unduly restrict the ability of platforms to curate apps and content, including with respect to enforcing IPR. Most recently, the ROK's legislature is considering amendments to its Monopoly Regulation and Fair Trade Act (MRFTA) which would inhibit the protection of IPR on platforms subject to Korean law. ACT has

[275] https://competerefoundation.org/wp-content/uploads/2026/10/Korea-Digital-Report-Oct2026-Final.pdf
[276] https://n.news.naver.com/mnews/article/047/0002484791?sid=101

engaged extensively with the ROK to emphasize the need for protecting IPR on platforms, and has also raised concerns with the law's conflicts with obligations in both Article 16 of the General Agreement on Trade in Services and the U.S.-Korea Free Trade Agreement in chapters addressing investment and electronic commerce.[277] Because ROK proposals for platform regulation would inhibit some core platform functions, including those that will protect IPR in the digital economy, we urge USTR to track this development, recommending that it be reflected in the 2027 NTE report as, unless altered, a means of denying adequate and effective protection of IPR, as well as a denial of fair and equitable market access to U.S. small businesses who rely on IPR protections.

Issue: Network Usage Fees

Korea's "sending party network pays" approach, together with pending amendments to the Telecommunications Business Act that would require large content providers to pay Korean internet service providers for network usage, imposes costs on U.S. content and application providers that, according to USTR, no other country imposes.[278] These fees raise the cost of delivering apps and services to Korean users, and those costs ultimately reach the small developers that depend on these services to distribute their products. Korea committed in the November 2025 Joint Fact Sheet that U.S. companies would not face unnecessary barriers in laws and policies concerning digital services, including network usage fees.[279] ACT has opposed similar network fee proposals in other jurisdictions and at the ITU. We urge USTR to press Korea to abandon network usage fee mandates and to reflect this barrier in the 2027 NTE report.

Issue: Proposed Digital Services Tax

In 2026, a bill was introduced in the National Assembly (Bill No. 2219551) that would amend the Adjustment of International Taxes Act to impose a digital services tax. Like DSTs elsewhere, the proposal would likely fall mainly on U.S. companies and would raise costs across the digital ecosystem that U.S. small business technology developers rely on to reach Korean customers. In August 2026, ACT wrote to the National Assembly opposing the bill.[280] The bill would also run counter to Korea's commitment in the November 2025 Joint Fact Sheet that U.S. companies will not be discriminated against in laws and policies concerning digital services.[281] We urge USTR to oppose the bill and to include it in the 2027 NTE report.

---

[277] See https://actonline.org/2025/01/24/act-the-app-associations-letter-to-the-republic-of-koreas-government-regarding-online-platform-regulation-legislation/.

[278] Korea Herald, US calls Korea's network fee policy 'outlier,' raises trade concerns (Apr. 28, 2026), https://www.koreaherald.com/article/10727598

[279] The White House, Joint Fact Sheet on President Donald J. Trump's Meeting with President Lee Jae-myung (Nov. 13, 2025), https://www.whitehouse.gov/fact-sheets/2025/11/joint-fact-sheet-on-president-donald-j-trumps-meeting-with-president-lee-jae-myung/

[280] Association for Competitive Technology, Letter to the National Assembly of the Republic of Korea regarding Bill No. 2219551 amending the Adjustment of International Taxes Act (Aug. 2026), https://actonline.org/post/acts-letter-to-the-national-assembly-of-the-republic-of-korea-in-opposition-to-the-proposed-amendment-to-the-adjustment-of-interational-taxes-act-imposing-a-digital-services-tax-on-foreign-digital-p/.

[281] The White House, Joint Fact Sheet on President Donald J. Trump's Meeting with President Lee Jae-myung (Nov. 13, 2025), https://www.whitehouse.gov/fact-sheets/2025/11/joint-fact-sheet-on-president-donald-j-trumps-meeting-with-president-lee-jae-myung/

Issue: Restrictions on Exporting Location Data

Korea has long restricted the export of high-precision map data, which has prevented U.S. suppliers from offering fully functioning online maps, navigation, and related location-based services that U.S. app developers build upon. In February 2026, a Korean interagency body conditionally approved the export of 1:5,000 scale map data to a U.S. provider, but the conditions require raw data to be processed on domestic servers run by a local partner, Korean coordinates to be removed or restricted on global services, and sensitive facilities to be obscured in imagery,[282] and the export had still not proceeded two months later.[283] Korea committed in the November 2025 Joint Fact Sheet to facilitate cross-border transfers of data, including location data.[284] We urge USTR to press Korea to apply any conditions in a transparent, timely, and non-discriminatory manner and to make the same access available to other U.S. providers.

Issue: App Store Payment Mandates

Korea's 2021 amendments to the Telecommunications Business Act prohibit app marketplaces from requiring the use of their own payment systems, and in 2023 the Korea Communications Commission proposed fines of 68 billion won against two U.S. app store operators, although the penalties had not been imposed as of early 2026.[285] These mandates weaken the integrated payment, security, and fraud-protection functions that small developers rely on when they distribute apps through curated online marketplaces, and they fall mainly on U.S. companies. In May 2026, a further bill to amend the Telecommunications Business Act was introduced that would add interoperability requirements for app stores.[286] We urge USTR to monitor enforcement of these rules and to oppose their expansion, including through the pending interoperability bill.

Issue: Public Sector Cloud Security Certification

Korea's Cloud Security Assurance Program (CSAP) has required cloud systems and operating personnel serving public institutions to be located in Korea, which has limited U.S. providers to the lowest certification tier and kept them out of most of Korea's public sector cloud market. In September 2026, Korea's National Intelligence Service announced that CSAP will be replaced by the National Network Security Framework (N2SF) from the second half of 2027, under which the Sensitive and Open tiers would allow overseas operations, although the Sensitive tier would still require physically separated, public-sector-only servers and storage for public data, the Classified tier would be limited to clouds operated inside agencies' own facilities, and implementation details

[282] Korea Herald, Korea clears exporting map data for Google, ends 19-year dispute (Feb. 27, 2026), https://www.koreaherald.com/article/10684189

[283] Korea Herald, Google map export stalls 2 months after Korea's conditional approval (Apr. 19, 2026), https://www.koreaherald.com/article/10720446

[284] The White House, Joint Fact Sheet on President Donald J. Trump's Meeting with President Lee Jae-myung (Nov. 13, 2025), https://www.whitehouse.gov/fact-sheets/2025/11/joint-fact-sheet-on-president-donald-j-trumps-meeting-with-president-lee-jae-myung/

[285] Korea Herald, US Section 301 probe puts Korea's digital rules in spotlight (Feb. 23, 2026), https://www.koreaherald.com/article/10680439

[286] Digital Policy Alert, Bill amending Telecommunications Business Act including interoperability requirement was introduced to National Assembly (May 21, 2026), https://digitalpolicyalert.org/event/40080-bill-amending-telecommunications-business-act-including-interoperability-requirement-was-introduced-to-national-assembly

have not been released.[287] We urge USTR to engage Korea so that N2SF is implemented in a way that gives U.S. cloud providers, and the small developers that build on them, non-discriminatory access to public sector work at every tier, including by accepting logical separation for the Sensitive tier, consistent with Korea's obligations under KORUS and the WTO Government Procurement Agreement.

Issue: AI Basic Act

Korea's Framework Act on the Development of Artificial Intelligence and Establishment of a Foundation for Trust (the AI Basic Act) took effect on January 22, 2026. It imposes obligations on providers of high-impact and generative AI, including notice and labeling requirements for AI-generated outputs and a requirement that foreign companies above certain thresholds designate a domestic representative, while implementing guidance remains limited.[288] Broad labeling and reporting obligations, applied without enough regard to the risk of a given use, raise compliance costs for U.S. AI developers and the small businesses that build on their models. We urge USTR to encourage Korea to implement the Act through risk-based guidance that relies on existing law and to avoid requirements to disclose sensitive information about AI models.

Issue: Content Rules for Online Platforms

In July 2026, Korea began enforcing amendments to its Information and Communications Network Act on false and manipulated information that allow courts to award punitive damages of up to five times the proven loss and require social media platforms with more than one million daily users to adopt systems for reporting such content.[289] Because platforms must judge what qualifies, these rules push services toward over-removal of lawful content and add legal risk for U.S. platforms and the developers that distribute through them. We ask USTR to monitor how the amendments are applied to U.S. services.

RUSSIA

Issue: Data Localization Law

Federal Law No. 242-FZ, signed by President Vladimir Putin in July of 2014, requires companies that store and process the personal data of Russian citizens to maintain servers on Russian soil and to

[287] Digital Today, Public cloud security certification overhaul seen opening door to global firms (Sept. 2026), https://www.digitaltoday.co.kr/en/view/104892/public-cloud-security-certification-overhaul-seen-opening-door-to-global-firms; Digital Daily, 국정원, 클라우드 보안인증 전면 개편…국내 CSP "해외 사업자만 유리해진다" 반발 [NIS Overhauls Cloud Security Certification] (Sept. 7, 2026), https://www.ddaily.co.kr/page/view/2026090715373498360; Byline Network, 공공 부문 민간 클라우드 등급 개편·검증 일원화…N2SF 적용도 확산 [Public-Sector Private Cloud Grades Revised and Verification Unified] (Sept. 18, 2026), https://byline.network/2026/09/18-635/

[288] International Trade Administration, South Korea AI Basic Act (Market Intelligence), https://www.trade.gov/market-intelligence/south-korea-ai-basic-act

[289] JURIST, South Korea enforces amended law on false and manipulated information (July 2026), https://www.jurist.org/news/2026/07/south-korea-enforces-amended-law-on-false-and-manipulated-information/

notify the federal media regulator, Roskomnadzor, of all server locations.[290] It empowers Roskomnadzor to block websites and to maintain a registry of data violators. Additionally, in August 2015, Russia passed a non-binding clarification suggesting that localization might apply to websites that include a built-in Russian-language options, transact in Russian rubles, or use a Russian top-level domain such as ".ru."[291] In July 2016, a package of amendments was released imposing extensive data storage requirements on telecommunications providers and companies classified as internet telecommunications services.[292] Per these changes, telecom operators will have to store metadata for three years and internet telecoms for one year, while both will have to retain the content for up to six months. Companies had until July 1, 2018, to begin implementing these requirements. Moreover, if the stored messages and files are encrypted, companies are required to provide Russian state security services with decryption keys upon request. In August 2016, Russia's Federal Security Service (FSB) announced that it has the capability to obtain information necessary for decoding the electronic messaging received, "sent, delivered, and (or) processed by users of the internet."[293] Further, on November 30, 2024, President Putin signed amendments to the Russian Code on Administrative Offences (Federal Law No. 420-FZ) that sharply increase fines for those violating Russian data protection laws, including turnover-based fines for repeat personal data leaks, effective May 30, 2025.[294] Raising the penalties for not abiding by this regulation creates additional barriers to digital trade and market entry.

Issue: Prohibitions on the Use of Strong Encryption

Under Russia's current System of Operative-Investigative Measures (SORM), Russian internet service providers (ISPs) must install a special device on their servers to allow the FSB to track all credit card transactions, e-mail messages, and web use. In 2014, SORM usage was extended to monitoring of social networks, chats, and forums, requiring their operators to install SORM probes in their networks. Advances of the SORM force online communications providers to provide the authorities with a means to decrypt users' messages, a technically infeasible result when end-to-end encryption methods are used. This law presents serious issues for small business innovators seeking to enter the Russian marketplace.

Russia also requires companies to provide the FSB with encryption keys for applications. Telegram, a popular messaging app, was fined 800,000 rubles for not providing FSB with one of these encryption keys.[295]

---

[290] Russian Federation, Federal Law No. 242-FZ, (July 21, 2014), available at https://pd.rkn.gov.ru/authority/p146/p191/.

[291] Russian Federation's Ministry of Communications and Mass Media, Clarifying Federal Law No. 242-FZ, (Aug. 3, 2015), available at http://www.bna.com/russia-clarifies-looming-n17179934521/.

[292] Russian Federation, "Yarovaya Package" Federal Laws No. 374-FZ and 375-FZ (July 6, 2016).

[293] Federal Security Service of the Russian Federation, Encryption Keys, (August 1, 2016), available at http://www.fsb.ru/fsb/science/single.htm!id=10437866@fsbResearchart.html.

[294] Digital Policy Alert, Federal Law No. 420-FZ on Amendments to the Code of the Russian Federation on Administrative Offences enters into force (May 30, 2025), https://digitalpolicyalert.org/event/29632-federal-law-on-amendments-to-the-code-of-the-russian-federation-on-administrative-offences-enters-into-force.

[295] "Russia Fines Telegram App Over Encryption-Key Demand", RadioFreeEurope RadioLiberty (October 16, 2017), available at https://www.rferl.org/a/russia-fines-telegram-app-encryption-key/28797424.html?mkt_tok=eyJpIjoiTW1OaU5EUTBPVFZtTVdObCIsInQiOiIwbVRcL1RkdDJjeXlsMFB6RkFQWStxMjBIaGV3cHFQRDZQK3BkRE1pVnE0TEtlQlZUVnFOeisyVkp6S3FlSUJpUnJZT1EzT211d1FiYWIwRis4MHhxVWZPREdGV2xPUlo2cklseE4xOEp3Mkx3aG1rc3FOTUs1RXFtWnRISDNXUHAifQ%3D%3D.

Issue: Various Virtual Private Network Restrictions

On November 1, 2017, Russia enacted regulations that prohibit consumers' ability to use VPNs to access websites as an anonymous browser. The Russian government cites this regulation as an effort to keep people from accessing dangerous and illegal content. This regulation says that any internet providers that allow these to exist, or function without being blocked, will lose their market access. Since September 1, 2025, Russia has also banned the advertising of VPNs that bypass Roskomnadzor's blocks, with fines of up to 500,000 rubles for organizations, and it now fines users who knowingly search for and access material designated as extremist.[296] This is an obvious trade barrier and real threat to the free market.

Additionally, there are now regulations regarding the anonymity of citizens while using chat apps such as WhatsApp or Facebook Messenger. Regulations that went into effect on January 1, 2018, require these apps to provide the users' phone numbers to the government to limit or prohibit access to those attempting to spread illegal content. Therefore, there is no ability to remain anonymous when using these applications. Although this is done under the veil of safety for citizens, it restricts the free flow of information and provides an extremely tough trade barrier to infiltrate.

Issue: Restrictions on Foreign Messaging Apps and Mandated Pre-Installation of State-Backed Apps

Since September 1, 2025, Russian law has required phones sold in Russia to come pre-installed with Max, a state-backed messenger developed by VK, and with RuStore, Russia's domestic app marketplace.[297] Since August 2025, Roskomnadzor has blocked voice calls on WhatsApp and Telegram, and in February 2026 it began slowing Telegram nationwide.[298] In February 2026, WhatsApp said Russia had attempted to fully block the service, with Russian authorities citing the refusal of foreign messaging services to store Russian users' data in Russia.[299] These measures steer users toward state-backed platforms and deny U.S. app developers a fair opportunity to reach Russian users through the app stores and messaging services of their choice. We ask USTR to address these measures in the 2027 NTE report.

SAUDI ARABIA

Issue: Cross-Border Data Transfer Restrictions

Saudi Arabia's Personal Data Protection Law (PDPL) and the Saudi Data and Artificial Intelligence Authority's (SDAIA) Regulation on Personal Data Transfer Outside the Kingdom permit transfers

[296] Meduza, No more phone sharing, VPN ads, or 'foreign agent' teachers (Sept. 1, 2025), https://meduza.io/en/feature/2025/09/01/no-more-phone-sharing-vpn-ads-or-foreign-agent-teachers
[297] Meduza, No more phone sharing, VPN ads, or 'foreign agent' teachers (Sept. 1, 2025), https://meduza.io/en/feature/2025/09/01/no-more-phone-sharing-vpn-ads-or-foreign-agent-teachers
[298] Meduza, Russia's federal censorship agency reportedly begins slowing Telegram nationwide (Feb. 10, 2026), https://meduza.io/en/news/2026/02/10/russia-s-federal-censorship-agency-reportedly-begins-slowing-telegram-nationwide
[299] BBC News, Russia moves to block WhatsApp in messaging app crackdown (Feb. 12, 2026), republished by The Star, https://www.the-star.co.ke/news/world/2026-02-12-russia-moves-to-block-whatsapp-in-messaging-app-crackdown

based on adequacy decisions or on safeguards such as standard contractual clauses (SCCs), binding common rules and accreditation certificates.[300] However, the SDAIA SCCs cannot be changed beyond filling in blank fields, and they require the data importer outside the Kingdom to submit to the jurisdiction of Saudi courts and to comply with and enforce binding decisions made under Saudi regulations.[301] The regulation also requires a risk assessment before any transfer that relies on these safeguards and before any continuous or large-scale transfer of sensitive data. These requirements extend Saudi jurisdiction to U.S. companies that receive data from Saudi customers or affiliates and add compliance costs that fall hardest on small businesses. We urge USTR to engage Saudi Arabia to remove the jurisdictional requirements in its SCCs and to adopt interoperable transfer tools, such as recognition of the Global Cross-Border Privacy Rules (CBPR) system.

SOUTH AFRICA

Issue: Data Localization

South Africa's National Policy on Data and Cloud, released in May 2024 by the Department of Communications and Digital Technologies (DCDT), includes provisions for data sovereignty. The policy specifies that "[g]overnment data that incorporates content pertaining to the protection and preservation of national security and sovereignty of the Republic shall be stored only in digital infrastructure located within the borders of South Africa."[302] However, the extent of the data covered under this provision is still uncertain, presenting challenges to ACT members.

Issue: Digital Platform Regulation

In 2021, the Competition Commission of South Africa (CCSA) launched an online intermediation platforms market inquiry.[303] ACT has provided detailed views on digital platforms and competition, as well as reactions and feedback on CCSA's specific proposals.[304] The inquiry's July 2023 final report directed Apple and Google to stop preventing app developers from steering consumers to pay outside the app store, to curate South African apps, and to provide advertising credits for South African developers, and stated that implementing the measures adopted in Europe under the DMA would be treated as compliance.[305] ACT has significant concerns with the South African government's interjecting itself into the digital economy, jeopardizing the functionality of mobile

[300] Saudi Data and Artificial Intelligence Authority, Regulation on Personal Data Transfer Outside the Kingdom, https://dgp.sdaia.gov.sa/wps/portal/pdp/knowledgecenter/details/RegulationonPersonalDataTransferOutsidetheKingdom

[301] Saudi Data and Artificial Intelligence Authority, Standard Contractual Clauses for Personal Data Transfer, https://dgp.sdaia.gov.sa/wps/portal/pdp/knowledgecenter/details/StandardContractualClauses

[302] Department of Communications and Digital Technologies, National Policy on Data and Cloud, Government Gazette No. 50741, Notice 2533 of 2024, § 15.4.2 (May 31, 2024), https://www.gov.za/sites/default/files/gcis_document/202406/50741gen2533.pdf.

[303] https://www.compcom.co.za/online-intermediation-platforms-market-inquiry/.

[304] E.g., https://www.compcom.co.za/wp-content/uploads/2021/07/App-Association-Comments-on-OIPMI-Statement-of-Issues-18-Jun-2021.pdf.

[305] CCSA, Online Intermediation Platforms Market Inquiry, Summary of Findings and Remedial Actions (July 2023), https://www.compcom.co.za/wp-content/uploads/2023/07/CC_OIPMI-Summary-of-Findings-and-Remedial-action.pdf

operating systems and software distribution platforms that have enabled countless American small businesses to grow. We therefore request that the CCSA's inquiry into online intermediation platforms, and the risks it poses to American small business innovators that rely on software distribution platforms, be captured in the 2027 NTE report, and that the U.S. government work with South Africa to mitigate the risks such an intervention would pose while supporting U.S. small business digital economy trade and leadership.

Separately, in November 2025 the CCSA released the final report of its Media and Digital Platforms Market Inquiry, which sets out remedial actions for Google, Meta, Microsoft, OpenAI, TikTok, and X, including a Google funding package for South African news media of up to ZAR 687.5 million over five years, backed by annual compliance reporting and possible referral to the Competition Tribunal.[306] Payments for news content and AI-related obligations arrived at through a market inquiry, rather than a finding of anticompetitive conduct, single out U.S. platforms, and Nigeria's competition authority has already cited these remedies as a reference for its own investigation. We urge USTR to capture these remedies in the 2027 NTE report and to discourage their replication elsewhere in the region.

Issue: OTT Regulation

In July 2025, the DCDT published a Draft White Paper on Audio and Audiovisual Media Services and Online Safety that would impose registration or notification obligations on online audiovisual services, contemplates South African content obligations for online content services, and proposes online safety duties for video-sharing platforms.[307] In September 2026, the Independent Communications Authority of South Africa (ICASA) published notices of its intention to conduct a market inquiry into the impact of OTT services on licensees and the regulatory framework, to which ACT responded, and then withdrew those notices on September 30, 2026.[308] Extending legacy broadcasting and telecommunications licensing, content quotas, levies, or network cost contribution obligations to OTT services would raise costs for U.S. small business technology developers whose apps depend on open internet access. We urge USTR to monitor the White Paper process and any reissued ICASA inquiry and to press South Africa to avoid such measures.

Issue: IP Rights Protection

IP laws in South Africa do not adequately address protection and enforcement of inventive and creative works in the digital age. Due to insufficient IP protections, inventive technologies and creative works are easily accessed and impact overall innovation and creation in Sub-Saharan Africa. ACT shares concerns with proposed changes to South Africa's copyright framework in the Copyright Amendment Bill. In June 2026, the Constitutional Court found several of the Bill's

[306] CCSA, Media and Digital Platforms Market Inquiry, Final Report, Annexure 8 (Remedial Actions) (Nov. 2025), https://www.compcom.co.za/wp-content/uploads/2025/11/CC_MDPMI-Final-Report_Non-Confidential_Annexure8_Remedial-Actions.pdf; CCSA, Media Statement, MDPMI Releases Final Report (Nov. 13, 2025), https://www.compcom.co.za/wp-content/uploads/2025/11/MDPMI-Releases-Final-Report-13-November-2025-2.pdf

[307] DCDT, Draft White Paper on Audio and Audiovisual Media Services and Online Safety, General Notice 3369, Government Gazette No. 52972 (July 11, 2025), https://www.gov.za/sites/default/files/gcis_document/202507/52972gen3369.pdf

[308] ICASA, General Notice Withdrawing Notices 4129 and 4148 on the OTT Market Inquiry, Government Gazette No. 55476 (Sept. 30, 2026), https://www.icasa.org.za/uploads/files/55476-30-9-ICASA-OTT-MARKET-INQUIRY.pdf

educational exceptions unconstitutional while upholding the other referred provisions, and the Bill now returns to Parliament.[309]

We further urge USTR to consider the Competition Commission of South Africa's (CCSA) market inquiry into online intermediation platforms as a potential means of denying adequate and effective protection of IPR, as well as a denial of fair and equitable market access to U.S. small businesses who rely on IPR protections. CCSA mandates for digital platform operations must preserve the ability for those platforms to provide IPR-related curations that countless developers operating in South Africa rely on.

SPAIN

Issue: Digital Services Taxation

Spain currently imposes a 3 percent DST.[310] For reasons discussed above, ACT is significantly concerned with the imposition of DSTs in this key market and calls for USTR support in opposing it.

SRI LANKA

Issue: Online Safety Act

Sri Lanka's Online Safety Act, No. 9 of 2024 created an Online Safety Commission that can direct internet intermediaries to remove or disable access to content it finds to be a prohibited statement within 24 hours, seek orders requiring them to disclose the identity of users, and declare online locations subject to further restrictions, with fines of up to 10 million rupees and possible imprisonment for non-compliance.[311] Intermediaries lose liability protection for third-party content if they do not comply with the Act or the Commission's codes of practice. These broad and vaguely defined powers create legal risk for U.S. small business technology developers that host user content or offer messaging services, and they discourage investment in Sri Lanka's digital economy. We urge USTR to press Sri Lanka to amend the Act to narrow the Commission's powers, provide for independent review, and remove criminal penalties for intermediaries.

TANZANIA

Issue: Digital Services Tax

Tanzania imposes a digital service tax on payments by individuals for electronic services supplied by non-resident providers, with no registration threshold, and non-resident providers must also charge 18 percent VAT without the ability to claim input tax credits.[312] The Finance Act, 2026 raised the

[309] Ex parte President of the Republic of South Africa: In re Constitutionality of the Copyright Amendment Bill and the Performers' Protection Amendment Bill (CCT 306/24) [2026] ZACC 26 (June 26, 2026), https://www.saflii.org/za/cases/ZACC/2026/26.html
[310] Tax Foundation, Digital Services Taxes in Europe, 2026 (May 4, 2026), https://taxfoundation.org/data/all/eu/digital-services-taxes-europe/
[311] Online Safety Act, No. 9 of 2024 (Sri Lanka, certified Feb. 1, 2024), https://www.parliament.lk/uploads/acts/gbills/english/6311.pdf.
[312] Tanzania Revenue Authority, Digital Service Tax, https://www.tra.go.tz/page/digital-service-tax

digital service tax rate from 2 percent to 3 percent of gross payments.[313] Because the tax applies only to non-resident providers and has no threshold, it falls on U.S. small business technology developers from their first sale in Tanzania. We urge USTR to include this tax in the 2027 NTE report and to press Tanzania to repeal it.

THAILAND

Issue: Digital Platform Regulation

Thailand's Electronic Transactions Development Agency (ETDA) has initiated a policy development process for digital platform regulation.[314] ACT has engaged with ETDA and others in the Thai government to emphasize the need for protecting IPR on platforms.[315] Although the government paused its draft Platform Economy Act in 2025, it has since resumed work on a Digital Platform Economy Act, which the Minister of Digital Economy and Society ordered revised in August 2026,[316] and further efforts to regulate digital platforms in Thailand are underway, including ETDA's implementation of the digital platform services law and the development of new "guidance" by ETDA.[317] In March 2026, the Trade Competition Commission of Thailand (TCCT) also published a notification on competition conduct in multi-sided e-commerce platforms,[318] and a TCCT subcommittee is now developing guidelines on trade conduct in digital platform businesses, on which ACT submitted comments in August 2026.[319] Because regulatory interventions into digital platforms markets stand to inhibit some core platform functions, including those that will protect IPR in the digital economy, we urge USTR to oppose onerous platform regulation in Thailand.

TÜRKIYE

Issue: Digital Service Taxes

[313] PwC, Worldwide Tax Summaries, Tanzania: Corporate - Significant Developments (2026), https://taxsummaries.pwc.com/tanzania/corporate/significant-developments

[314] See https://www.trade.gov/market-intelligence/thailand-information-technology-digital-platforms.

[315] See https://actonline.org/wp-content/uploads/2026/06/ACT-Positions-on-Digital-Platforms-and-Competition-for-Thailand-EDTA-EN.pdf.

[316] The Nation, Digital Minister Slows Platform Bill and Rethinks Fees Charged to Businesses (Aug. 14, 2026), https://www.nationthailand.com/news/policy/40069775; Thailand Development Research Institute, Advancing Platform Governance in Thailand (Feb. 13, 2026), https://tdri.or.th/en/2026/02/advancing-platform-governance-in-thailand/.

[317] Electronic Transactions Development Agency, Digital Platform Services, https://www.etda.or.th/th/regulator/Digitalplatform/index.aspx

[318] Trade Competition Commission of Thailand, Notification on Multi-Sided Platform Businesses (Royal Gazette, Mar. 24, 2026), https://tcct.or.th/assets/portals/1/files/Multi_sided_Platform.pdf

[319] Trade Competition Commission of Thailand, Meeting of the Subcommittee on Guidelines for Regulating and Deterring Trade Conduct in the Digital Platform Business No. 2/2569 (Sept. 17, 2026), https://www.tcct.or.th/view/1/activity/seminar/3034/TH-TH; ACT, Comments to the Office of the Trade Competition Commission of Thailand Regarding the Public Consultation on the Development of Regulatory Guidelines for Digital Platform Businesses (Aug. 31, 2026), https://actonline.org/post/comments-of-the-association-for-competitive-technology-to-the-office-of-the-trade-competition-commission-of-thailand-regarding-the-public-consultation-on-the-development-of-regulatory-guidelines-for-d/

Türkiye has implemented a DST, originally set at 7.5 percent and reduced to 5 percent from January 1, 2026, with a further cut to 2.5 percent scheduled for January 1, 2027,[320] which applies to companies that have worldwide revenues of €750 million and local revenues of 20 million Turkish Lira. USTR determined in 2021 that Türkiye's DST was actionable under Section 301 and continues to monitor it.[321] For reasons discussed above, ACT is significantly concerned with the imposition of DSTs in this key market and calls for USTR support in opposing it.

Issue: Digital Platform Regulation

A draft amendment to the Law on the Protection of Competition, No. 4054, in Türkiye would add a new online platforms regulatory framework that aligns with concepts outlined in the EU's DMA, although the amendment has not been enacted to date.[322] The draft, however, would impose additional requirements for designated companies intended to enable the interoperability of core platforms services and/or ancillary services, but stands to inhibit the ability of curated online marketplaces to enforce IPRs, which, as explained above, is a vital function small businesses in the digital economy rely upon. Because regulatory interventions into digital platforms markets by Türkiye stand to inhibit some core platform functions, including those that will protect IPR in the digital economy, we urge USTR to assist in opposing digital platform regulation in Türkiye.

Issue: Data Localization

Türkiye's E-Payment Law requires the processing of e-payments occur within Türkiye.[323] In mid-2016, Türkiye's Banking Regulation and Supervision Agency (BDDK) initiated a policy that mandates companies locate their ICT systems in the country.[324] For instance, PayPal was forced to halt their operations after the Turkish government revoked their license, an action PayPal said would affect "tens of thousands of businesses and hundreds of thousands of consumers."[325] While Türkiye amended its Personal Data Protection Law No. 6698 in 2024 to allow cross-border transfers of personal data based on standard contracts, binding corporate rules and other safeguards,[326] these sector-specific data localization requirements have largely chilled our members' plans to enter this important market should their app include e-payment capabilities.

---

[320] Digital Policy Alert, Presidential Decree No. 10767 re Determining Digital Services Tax Rate (Dec. 25, 2025), https://digitalpolicyalert.org/change/17590-presidential-decree-no-10767-re-determining-digital-services-tax-rate

[321] Office of the U.S. Trade Representative, Section 301 Investigations, Digital Services Taxes, https://ustr.gov/issue-areas/enforcement/section-301-investigations/section-301-digital-services-taxes

[322] Turkish Competition Authority, Act No. 4054 on the Protection of Competition (as amended through Act No. 7549, 2025), https://www.rekabet.gov.tr/en/Sayfa/Legislation/act-no-4054

[323] U.S. Dep't of State Bureau of Economic and Business Affairs, 2016 Investment Climate Statement – Turkey (July 5, 2016), available at http://www.state.gov/e/eb/rls/othr/ics/2016/eur/254425.htm.

[324] Turkey's Banking Regulation and Supervising Industry (BDDK), Law on Payment and Security Settlement Systems, Payment Services and Electronic Money Institutions numbered 6493, Official Gazette numbered 28690, (published June 27, 2013), available at https://www.bddk.org.tr/websitesi/english/Legislation/129166493kanun_ing.pdf.

[325] Lunden, Ingrid, "PayPal to halt operations in Turkey after losing license, impacts 'hundreds of thousands'" Tech Crunch, (May 31, 2016), available at https://techcrunch.com/2016/05/31/paypal-to-halt-operations-in-turkey-after-losing-license-impacts-hundreds-of-thousands/.

[326] Personal Data Protection Authority (KVKK), Yurt Dışına Aktarım (Cross-Border Transfer), https://www.kvkk.gov.tr/Icerik/2053/Yurtdisina-Aktarim

Issue: Social Media Law

Türkiye amended the Regulation of Internet Broadcasts and Prevention of Crimes Committed through Such Broadcasts (Law No. 5651), with these amendments coming into force October 1, 2020. These amendments are collectively known as the Social Media Law, and affect all businesses considered social network providers.[327] The law's broad definition of social network providers – which includes any business allowing users to create, view, or share text or media for social interaction – may include many ACT members not traditionally considered social network providers, placing a heavy burden on the business and discouraging expansion into the Turkish market.

UGANDA

Issue: Digital Services Tax

Uganda imposes a 5 percent digital services tax on income that non-resident providers earn from digital services supplied in Uganda, collected through returns filed with the Uganda Revenue Authority, in addition to VAT on electronic services supplied by non-residents.[328] Because the tax applies only to non-resident providers and is levied on gross income, it discriminates against U.S. small business technology developers serving Ugandan customers. We urge USTR to include this tax in the 2027 NTE report and to press Uganda to repeal it.

UNITED ARAB EMIRATES

Issue: Data Localization

The UAE requires CSPs serving the public sector and specific regulated industries to be exclusively governed by UAE law, exempt from foreign jurisdiction and laws, and to physically localize data centers along with engineering, security, maintenance, and support operations and personnel. For reasons discussed above, ACT is concerned with such requirements and requests USTR support in opposing them.

UNITED KINGDOM

Issue: Digital Platform Regulation

The Digital Markets, Competition and Consumers Act (DMCCA), effective January 2025, establishes a new regulatory framework empowering the UK Competition and Markets Authority (CMA) to oversee digital markets by designating firms with "Strategic Market Status" (SMS) based on their market dominance and revenue thresholds. The Act shifts the CMA's role from traditional post-investigation enforcement to proactive, ongoing oversight, allowing it to impose forward-looking

[327] Begüm Yavuzdogan Okumus & Direnç Bada, Turkish data localization rules in effect for social media companies, IAPP, Oct. 20, 2020, available at https://iapp.org/news/a/turkish-data-localization-rules-in-effect-for-social-media-companies/.

[328] Uganda Revenue Authority, IT-Digital Service Tax Return Form for Non-Resident Service Providers (Nov. 2023), https://ura.go.ug/storage/2023/11/ITDigitalServiceTaxReturnFormforNonResidentServiceProviders.pdf

conduct obligations. In October 2025, the CMA designated Google with SMS in general search and search advertising, and Apple and Google with SMS in their mobile platforms.[329] In 2026, the CMA accepted commitments from Apple and Google on app review, app ranking, use of app data and interoperability requests in place of formal conduct requirements, imposed conduct requirements on Google's search services, and consulted on steering conduct requirements for both mobile platforms.[330] ACT recognizes that the CMA has so far taken a more measured and participative approach than the EU has taken under the DMA. Similar to its concerns noted above regarding the EU DMA, however, ACT is concerned that the DMCCA's broad discretion to impose forward-looking obligations could weaken platform functions that small businesses rely on, such as app review, security and IP enforcement, and we urge USTR to monitor its implementation closely.

Issue: Prohibitions on the Use of Strong Encryption

Media reports suggest that the UK government has issued a technical capability notice (TCN) under Section 253 of the Investigatory Powers Act 2016 compelling Apple to introduce a backdoor into its end-to-end encrypted cloud services. This would embed a systemic security vulnerability into one of the world's largest mobile device providers, endangering the security and privacy of all its users—not just in the UK, but worldwide. Additional reporting indicates that Apple has now discontinued its Advanced Data Protection feature in the UK, an optional service that offers end-to-end encryption for iCloud backups, file storage, and certain other apps.

ACT's small business members know that, in order to compete across consumer and enterprise markets, they must be able to reliably restrict data access to authorized users, ensure data remains accurate and unmodified, and guarantee information is available when needed by authorized users. End-to-end encryption is a primary tool for providing the trust and security of their customers. Attempts by governments—most recently the UK—to mandate backdoors to encryption algorithms significantly undermines these goals.

ACT understands and appreciates the need for policymakers to protect public safety across new and emerging digital modalities. However, the TCN issued by the UK government to Apple does not accomplish this goal. Its implementation will deeply damage security and trust across the digital

[329] Competition and Markets Authority, CMA confirms Google has strategic market status in search services (Oct. 10, 2025), https://www.gov.uk/government/news/cma-confirms-google-has-strategic-market-status-in-search-services; Competition and Markets Authority, Apple's mobile platform (case page, SMS decision Oct. 22, 2025), https://www.gov.uk/cma-cases/sms-investigation-into-apples-mobile-ecosystem; Competition and Markets Authority, Google's mobile platform (case page, SMS decision Oct. 22, 2025), https://www.gov.uk/cma-cases/sms-investigation-into-googles-mobile-platform; ACT, Response to the UK Competition and Markets Authority Strategic Market Status Investigations into Apple's and Google's Mobile Ecosystems (Feb. 12, 2025), https://actonline.org/post/act-the-app-associations-response-to-the-uk-competition-and-markets-authority-strategic-market-status-investigations-into-apples-and-googles-mobile-ecosystems/

[330] Competition and Markets Authority, CMA secures commitments from Apple and Google to improve fairness in app store processes and enhance iOS interoperability (Feb. 10, 2026), https://www.gov.uk/government/news/cma-secures-commitments-from-apple-and-google-to-improve-fairness-in-app-store-processes-and-enhance-ios-interoperability; Competition and Markets Authority, Google's general search and search advertising services (case page), https://www.gov.uk/cma-cases/sms-investigation-into-googles-general-search-and-search-advertising-services

economy by creating flaws in algorithms that can be used to compromise data confidentiality, integrity, and access requisites.

It is impossible to reserve security backdoors for just the "good guys." If a door exists then bad actors can, and will, exploit it. It is fair to assume that other tech firms will be asked to create similar backdoors into encrypted services, further damaging security and trust. The UK's demand also sets a precedent for other countries and regimes to demand similar access to encrypted private data, further reducing citizens' privacy and safety.

The damage that would be caused by the implementation of the UK government's TCN to American small businesses innovating and competing across the global digital economy is not hypothetical. As a prime example, government mandates in the 1990s for broadband internet providers to enable law enforcement agencies access to encrypted communications on their networks has directly led recently to the China-backed hacker group Salt Typhoon gaining unprecedented unauthorized access to swaths of sensitive data. While the magnitude of this breach of U.S. telecommunications carrier networks continues to be investigated, at this time, it appears that Salt Typhoon's access was essentially unlimited. This (ongoing) episode is the strongest evidence that mandating unfettered access via backdoors to encrypted devices or data in transit will result in that access being exploited by unintended actors. The Salt Typhoon experience demonstrates that weakening encryption will expose businesses to more frequent breaches, creating an even greater risk for those already marginalized.

The UK government's issuance of the reported TCN also stands in stark contrast to the U.S. government's efforts to encourage the use of encryption for securing critical infrastructure, businesses, and personal data; promote best practices for encryption in cybersecurity; and for the U.S. government itself to use encryption to protect classified information and communications. With cyber attacks to critical infrastructure continuing to increase in both frequency and severity, the need for security that end-to-end encryption provides has never been more essential. A mandated weakening of encryption will undermine these efforts. In a separate letter,[331] we have explained to the UK Home Office that in compelling a company to covertly compromise the security of its product, the UK undermines its own stated goal of "protect[ing] and promot[ing] its interests as a sovereign nation in a world fundamentally shaped by technology"[332] and raises serious concerns about the security of products from UK firms, leading to investors and consumers questioning whether their products contain hidden security vulnerabilities mandated by the UK government. The precedent the TCN implementation will create may force some of our members to consider withdrawing from the UK market to avoid the reputational risks associated with undermining their own product's security, representing the closing off of a key market to countless U.S. small business innovators. Any government that mandates, or attempts to mandate, backdoors to encryption damages their own standing in global security and innovation policy.

In August 2025, the U.S. Director of National Intelligence stated that the UK had agreed to drop its original TCN,[333] and in October 2025 the UK Home Office reportedly issued a new TCN limited to data of UK users. Apple and civil society groups are challenging the TCN and the TCN regime before the

[331] https://actonline.org/wp-content/uploads/ACT-Ltr-re-UK-Encryption-TCN-24-Feb-2025.pdf.
[332] https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030.
[333] Al Jazeera, UK agrees to drop mandate for Apple 'back door', US spy chief says (Aug. 19, 2025), https://www.aljazeera.com/economy/2025/8/19/uk-drops-mandate-for-apple-back-door-us-spy-chief-says

Investigatory Powers Tribunal, where a substantive hearing is listed for December 2026.[334] We note that ACT's concerns above remain, despite this second attempt.

We strongly support efforts to combat governments' attempts to undermine encryption, which damage and distort the security and competitiveness foundations that our small business innovator community relies on. The U.S. has the power to protect encryption standards, ensuring they remain strong enough to safeguard our digital infrastructure without creating loopholes that compromise security. We request USTR leadership in promoting strong encryption in its engagement with governments around the world to ensure that end-to-end encryption supports U.S. national and economic security. Our community fully commits to supporting policies that enhance security and innovation as well as U.S. global leadership.

Issue: Digital Services Taxation

The UK levies a 2 percent Digital Services Tax (DST) on companies that have worldwide revenues of £500 million and local revenues of £25 million. The UK has kept the DST in place even though, in the May 2025 U.S.-UK Economic Prosperity Deal, both countries agreed to negotiate an ambitious set of digital trade provisions,[335] and the United States reportedly put the September 2025 U.S.-UK Technology Prosperity Deal on hold in December 2025 over the DST.[336] In April 2026, HM Treasury again defended the DST.[337] For reasons discussed above, ACT is significantly concerned with the imposition of DSTs in this key market, and calls for USTR support in securing its repeal through ongoing U.S.-UK negotiations.

Issue: Intellectual Property Rights and Standards

In the case *Unwired Planet v. Huawei*,[338] the United Kingdom Supreme Court upheld an injunction prohibiting the sale of wireless telecommunications products in Britain due to a party's failure to enter a patent license for Unwired Planet's worldwide portfolio of SEPs, even though the party was willing to enter into a license for UK SEPs. If a single patent in a single jurisdiction can be used to obtain an injunction unless the alleged infringer enters a worldwide license, SEP owners will be highly incented to engage in global forum shopping, depressing the ability for American innovators like ACT members to compete abroad.

---

[334] Privacy International, PI Apple TCN Challenge, https://privacyinternational.org/legal-action/pi-apple-tcn-challenge; Bill Goodwin, Home Office challenged on 'farcical' secrecy over Apple 'backdoor' order, Computer Weekly (Sept. 17, 2026), https://www.computerweekly.com/news/366650612/Home-Office-challenged-on-farcical-secrecy-over-Apple-backdoor-order

[335] Government of the United Kingdom, General Terms for the United States of America and the United Kingdom of Great Britain and Northern Ireland Economic Prosperity Deal (May 8, 2025), https://www.gov.uk/government/publications/us-uk-economic-prosperity-deal-epd/general-terms-for-the-united-states-of-america-and-the-united-kingdom-of-great-britain-and-northern-ireland-economic-prosperity-deal-web-accessible-v

[336] The Register, US freezes $42B trade pact with UK over digital tax row (Dec. 16, 2025), https://www.theregister.com/2025/12/16/us_uk_trade_deal/

[337] Ryan Hogg, UK Defends Digital Services Tax as Fair Amid Trump Tariff Threat, Bloomberg Tax (Apr. 24, 2026), https://news.bloombergtax.com/daily-tax-report/uk-defends-digital-services-tax-as-fair-amid-trump-tariff-threat

[338] See https://www.supremecourt.uk/cases/docs/uksc-2018-0214-judgment.pdf.

The Unwired Planet decision continues to present grave risks to those who rely on standards to innovate, presenting a major barrier to trade for American small businesses in the digital economy and IoT that rely on standards to innovate and compete.

UK courts have since moved to support willing licensees, and in *Panasonic v. Xiaomi* and *Lenovo v. Ericsson* the Court of Appeal granted interim license declarations and found that pursuing injunctions in other courts was out of compliance with the ETSI IPR Policy,[339] although the UPC and a German court have since issued anti-interim-license injunctions to stop an implementer from seeking an interim license in the UK.[340]

In July 2026, the UK Supreme Court allowed Tesla, as a prospective licensee, to pursue declarations that it is entitled to a FRAND license to the SEPs on the Avanci 5G platform, rejecting the position that a patent pool has no liability under the FRAND commitments attached to the SEPs it licenses.[341]

The UK Intellectual Property Office (UK IPO) separately consulted on SEPs in 2025 and, on October 13, 2026, published the government's response, which takes constructive first steps on early FRAND determination, licensing guidance, and transparency but expressly declines further action on injunctions as they relate to SEPs.[342] We find this concerning since injunctions are often improperly used in this context and have a direct impact on UK small businesses. In addition, the UK's Competition and Markets Authority (CMA) continues to consider competition-themed mandates for digital platforms that could inhibit some core platform functions, including those that will protect IPR in the digital economy. We therefore urge USTR to track these developments and reflect them in the 2027 NTE report.

Given the impact of the above-described developments in the UK, we strongly recommend that the 2027 NTE report accurately capture and characterize the above concern.

Issue: Online Safety Act Implementation

The Online Safety Act 2023 (OSA) imposes risk assessment, content moderation and age assurance duties on a wide range of user-to-user and search services, including many small apps that let users share content. Ofcom published its register of categorized services in July 2026 and continues to develop guidance on highly effective age assurance.[343] The UK government has also announced plans to restrict social media access for users under 16, with regulations expected by the end of

[339] JUVE Patent, Lenovo and Kirkland take the win in UK interim licence dispute with Ericsson (Feb. 28, 2025), https://www.juve-patent.com/cases/lenovo-and-kirkland-take-the-win-in-uk-interim-licence-dispute-with-ericsson/

[340] JUVE Patent, UPC and Munich court limit UK jurisdiction over interim patent licences (Oct. 6, 2025), https://www.juve-patent.com/cases/upc-and-munich-court-limit-uk-jurisdiction-over-interim-patent-licences/

[341] Supreme Court of the United Kingdom, Tesla, Inc and another v InterDigital Patent Holdings, Inc and others [2026] UKSC 27, Press Summary (July 27, 2026), https://caselaw.nationalarchives.gov.uk/uksc/2026/27/press-summary

[342] UK Intellectual Property Office, Government sets out next steps on Standard Essential Patents (Oct. 13, 2026), https://www.gov.uk/government/news/government-sets-out-next-steps-on-standard-essential-patents

[343] Ofcom, Online Safety industry bulletin, October 2026, https://www.ofcom.org.uk/online-safety/protecting-children/online-safety-industry-bulletin-october-2026

2026 and the first restrictions targeted for spring 2027.[344] ACT supports the goal of protecting children online, but the cost of age assurance, risk assessments and ongoing compliance falls hardest on small developers, and unclear scoping can discourage U.S. small businesses from offering services in the UK. We urge USTR to encourage the UK to apply these rules in proportion to the size and risk of each service and to avoid requirements that weaken the security and privacy protections, such as encryption, that small businesses and their users rely on.

VIETNAM

Issue: Digital Platform Regulation

In June 2025, Vietnam adopted the Law on Digital Technology Industry (DTI Law) that went into effect in January 2026.[345] The law, while designed to set up new legal frameworks governing new technology industries like cryptocurrencies, in-app credits, or digital goods, also aims to rein in companies benefiting from Vietnamese users. This acts similarly to the DMA as a digital tax on U.S. innovation. USTR should remain concerned about how these obligations may disproportionately burden small U.S.-based app developers and digital-services firms operating in Vietnam (or planning to enter) by imposing new oversight, compliance, registration and reporting requirements on larger players.

More recently, Vietnam adopted the Law on Digital Transformation (Law No. 148/2025/QH15) on December 11, 2025, and the law took effect on July 1, 2026.[346] The law, much like the EU's DMA, places significant restrictions on digital platforms, introduces extensive obligations, and imposes other onerous restrictions. The law also designates certain platforms as dominant based on user base thresholds and imposes restrictions similar to the EU Digital Services Act. These measures represent substantial digital trade barriers that limit operational flexibility and raise barriers to market entry for ACT members.

Vietnam's Ministry of Industry and Trade (MOIT) is also drafting a law amending the Law on Commerce, the Competition Law, the Law on Foreign Trade Management, and the Law on Protection of Consumer Rights, under policies the Government approved in June 2026.[347] The bill, which the

[344] IAB UK, Government announces social media restrictions for under-16s, key takeaways (June 16, 2026), https://www.iabuk.com/news-article/government-announces-social-media-restrictions-under-16s-key-takeaways

[345] Government of Viet Nam, Thông qua Luật Công nghiệp Công nghệ số: Tăng tốc "Make in Vietnam", vươn ra toàn cầu [Law on Digital Technology Industry Adopted], BAO CHINH PHU (June 14, 2025), https://baochinhphu.vn/thong-qua-luat-cong-nghiep-cong-nghe-so-tang-toc-make-in-vietnam-vuon-ra-toan-cau-102250614120409337.htm.

[346] Government of Viet Nam, Ban hành Kế hoạch triển khai thi hành Luật Chuyển đổi số [Plan Issued for Implementing the Law on Digital Transformation], BAO CHINH PHU (Feb. 12, 2026), https://baochinhphu.vn/ban-hanh-ke-hoach-trien-khai-thi-hanh-luat-chuyen-doi-so-102260212174749918.htm

[347] Government of Viet Nam, Chính phủ thông qua 2 chính sách của Luật sửa đổi, bổ sung các Luật về thương mại, tiêu dùng [Government Approves Two Policies for the Law Amending Laws on Commerce and Consumers], BAO CHINH PHU (June 2, 2026), https://baochinhphu.vn/chinh-phu-thong-qua-2-chinh-sach-cua-luat-sua-doi-bo-sung-cac-luat-ve-thuong-mai-tieu-dung-102260602111440418.htm

Government submitted to the National Assembly in October 2026,[348] would add a new clause to Article 27 of the Competition Law that, although revised in August 2026 to remove most explicit references to digital platforms,[349] would in practice bar platforms with a dominant position from favoring their own products through rankings or algorithms, imposing unreasonable conditions on payment methods or other transaction terms, and making it difficult to remove preinstalled apps.[350] These prohibitions would import DMA-style ex ante rules into Vietnam's competition law and would restrict platform functions that protect security, privacy, and IP for small developers. ACT submitted comments to MOIT in 2026 asking for an effects-based significant harm threshold and an objective justification defense,[351] and in October 2026 ACT commented on MOIT's draft decree on administrative penalties in the competition sector, which would replace Decree 75/2019.[352] We urge USTR to press Vietnam to withdraw the Article 27 platform prohibitions.

Issue: Artificial Intelligence Regulation

Vietnam's new Law on Artificial Intelligence, which the National Assembly adopted on December 10, 2025 and which took effect on March 1, 2026, also functions as a trade barrier.[353] It mandates strict regulation of AI development and deployment, including requirements for AI-generated content to carry identifying marks and prohibitions on AI use for fraudulent purposes or to spread misinformation.[354] The law and its implementing Decree No. 142/2026/ND-CP impose burdensome compliance and assessment processes, especially for small technology firms wishing to operate in

[348] Ministry of Industry and Trade, Bộ trưởng Lê Mạnh Hùng trình bày tờ trình về sửa đổi, bổ sung một số điều của 4 luật lĩnh vực Công Thương [Minister Presents Bill Amending Four Industry and Trade Laws] (Oct. 20, 2026), https://moit.gov.vn/tin-tuc/bo-truong-le-manh-hung-trinh-bay-du-an-luat-sua-doi-bo-sung-mot-so-dieu-cua-luat-thuong-mai-luat-canh-tranh-luat-quan-ly.html.

[349] Information Technology and Innovation Foundation, Comments to National Assembly of Vietnam Regarding the Draft Law Amending and Supplementing Certain Articles (Sept. 19, 2026), https://itif.org/publications/2026/09/19/comments-national-assembly-vietnam-regarding-draft-law-amending-supplementing-certain-articles/.

[350] Vietnam Chamber of Commerce and Industry, Siết quản lý nền tảng số hạn chế cạnh tranh không lành mạnh [Tightening Management of Digital Platforms to Limit Unfair Competition] (Mar. 19, 2026), https://vcci.com.vn/news/siet-quan-ly-nen-tang-so-han-che-canh-tranh-khong-lanh-manh

[351] ACT, Comments on the Draft Law Amending and Supplementing a Number of Articles of the Law on Commerce, the Competition Law, the Law on Foreign Trade Management, and the Law on Protection of Consumer Rights (June 20, 2026), https://actonline.org/post/comments-of-the-association-for-competitive-technology-act-on-the-draft-law-amending-and-supplementing-a-number-of-articles-of-the-law-on-commerce-the-competition-law-the-law-on-foreign-trade-mana/.

[352] ACT, Comments on the Draft Decree on Administrative Penalties in the Competition Sector (Replacing Decree No. 75/2019/ND-CP) (Oct. 5, 2026), https://actonline.org/post/comments-of-the-association-for-competitive-technology-on-the-draft-decree-on-administrative-penalties-in-the-competition-sector-replacing-decree-no-75-2019-nd-cp-english-vietnamese-versions/.

[353] Government of Viet Nam, Việt Nam chính thức có Luật Trí tuệ nhân tạo (AI) [Viet Nam Officially Has a Law on Artificial Intelligence], BAO CHINH PHU (Dec. 10, 2025), https://baochinhphu.vn/viet-nam-chinh-thuc-co-luat-tri-tue-nhan-tao-ai-102251210164948585.htm

[354] Government of Viet Nam, Nội dung do AI tạo ra phải có dấu hiệu nhận biết [AI-Generated Content Must Carry Identifying Marks], BAO CHINH PHU (Feb. 27, 2026), https://baochinhphu.vn/noi-dung-do-ai-tao-ra-phai-co-dau-hieu-nhan-biet-102260227152118678.htm

Vietnam.[355] These broad, vague provisions threaten to restrict the participation of small AI providers through restrictive standards and transparency requirements, thereby limiting cross-border AI trade and innovation.

Issue: National Cybersecurity Law

Vietnam's broadly scoped Law on Cybersecurity, which the National Assembly amended in December 2025 to merge the 2018 Cybersecurity Law with the 2015 Law on Network Information Security and which took effect on July 1, 2026,[356] applies to onshore and offshore companies/individuals directly involved or related to the management, provision or use of cyberspace; imposes forced localization (specifically, administrators of critical systems must store personal data and critical data within Vietnam); imposes discriminatory licensing requirements; and conflicts with Vietnam's pro-innovation and investment positions at the Asian-Pacific Economic Cooperation. The law also requires domestic and foreign service providers to remove content within 24 hours of a request, or within six hours in urgent cases.[357] Vietnam's Ministry of Public Security continues to tighten censorship and restrictions on social media and online freedom.[358]

Issue: Data Localization and Cross-Border Data Transfer Restrictions

Vietnam's Law on Data, adopted in November 2024, and its implementing Decree No. 165/2025/ND-CP set strict conditions on transferring "core" and "important" data abroad, tied to national security and public interest safeguards.[359] Vietnam's Personal Data Protection Law, which took effect on January 1, 2026, and its implementing Decree No. 356/2025/ND-CP add further obligations on the processing and cross-border transfer of personal data.[360] These overlapping regimes create pressure to localize data and require costly assessments and approvals that U.S. small businesses cannot easily absorb. In its October 2025 framework with the United States, Vietnam agreed to finalize

[355] Government of Viet Nam, Ban hành Nghị định quy định chi tiết một số điều và biện pháp thi hành Luật Trí tuệ nhân tạo [Decree Issued Detailing the Law on Artificial Intelligence], BAO CHINH PHU (May 8, 2026), https://baochinhphu.vn/ban-hanh-nghi-dinh-quy-dinh-chi-tiet-mot-so-dieu-va-bien-phap-thi-hanh-luat-tri-tue-nhan-tao-102260508162952667.htm

[356] Government of Viet Nam, Quốc hội thông qua Luật An ninh mạng (sửa đổi) [National Assembly Passes the Amended Law on Cybersecurity], BAO CHINH PHU (Dec. 10, 2025), https://baochinhphu.vn/quoc-hoi-thong-qua-luat-an-ninh-mang-sua-doi-tang-cuong-bao-ve-khong-gian-mang-va-nhom-yeu-the-102251210125412744.htm

[357] Government of Viet Nam, Luật An ninh mạng 2025: Những điểm mới cần chú ý khi thực thi [Cybersecurity Law 2025: New Points to Note in Implementation], BAO CHINH PHU (Aug. 21, 2026), https://baochinhphu.vn/luat-an-ninh-mang-2025-nhung-diem-moi-can-chu-y-khi-thuc-thi-102260821185122728.htm

[358] Vu Lam, Vietnam's Public Diplomacy and the Peril of Mixed Messages, THE DIPLOMAT, (October 6, 2020), available at https://thediplomat.com/2020/10/vietnams-public-diplomacy-and-the-peril-of-mixed-messages/.

[359] U.S. Department of State, 2025 Investment Climate Statements: Vietnam (2025), https://www.state.gov/reports/2025-investment-climate-statements/vietnam/

[360] Government of Viet Nam, Luật Bảo vệ dữ liệu cá nhân chính thức có hiệu lực từ ngày mai (1/1/2026) [Personal Data Protection Law Officially Takes Effect Tomorrow (Jan. 1, 2026)], BAO CHINH PHU (Dec. 31, 2025), https://baochinhphu.vn/luat-bao-ve-du-lieu-ca-nhan-chinh-thuc-co-hieu-luc-tu-ngay-mai-1-1-2026-102251231155609721.htm

commitments on digital trade,[361] and we urge USTR to use that process to secure commitments on the transfer of data across trusted borders and against data localization requirements.

Issue: Licensing and Local Presence Requirements for Online Services

Decree No. 147/2024/ND-CP on the management, provision, and use of internet services and online information already imposes significant obligations on cross-border services that reach Vietnamese users. In July 2026, the Ministry of Culture, Sports and Tourism released a draft decree amending Decree 147 that would require prior licensing to publish online games, create a new license for platforms that allow users to create and distribute games, and require such platforms to have a local establishment and local operator.[362] ACT submitted comments urging removal of these licensing and local establishment requirements,[363] which conflict with Vietnam's local presence commitments under the Comprehensive and Progressive Agreement for Trans-Pacific Partnership. We urge USTR to press Vietnam to withdraw them.

***

ACT appreciates the opportunity to submit these comments for the 2027 NTE report. We stand ready to work with USTR and other stakeholders to address trade barriers for all of America's businesses and innovators.

Sincerely,



Brian Scarpelli
Senior Global Policy Counsel
Association for Competitive Technology (ACT)

Chapin Gregor
Global Policy Counsel
Association for Competitive Technology (ACT)
1401 K St NW (Ste 501)
Washington, DC 20005

[361] The White House, Joint Statement on United States-Vietnam Framework for an Agreement on Reciprocal, Fair, and Balanced Trade (Oct. 26, 2025), https://www.whitehouse.gov/briefings-statements/2025/10/joint-statement-on-united-states-vietnam-framework-for-an-agreement-on-reciprocal-fair-and-balanced-trade/
[362] Ministry of Culture, Sports and Tourism, Authority of Broadcasting, Television and Electronic Information, Draft Decree Amending and Supplementing Decree No. 147/2024/ND-CP (July 13, 2026)
[363] ACT, Comments on the Draft Decree Amending and Supplementing a Number of Articles of Decree No. 147/2024/ND-CP on the Management, Provision, and Use of Internet Services and Online Information (July 18, 2026), https://actonline.org/post/comments-of-the-association-for-competitive-technology-act-on-the-draft-decree-amending-and-supplementing-a-number-of-articles-of-decree-no-147-2024-nd-cp-on-the-management-provision-and-use-of-i/.